

Title	Assessment and Improvement of Security Awareness Training Methodologies [Project Paper]
Author(s)	Yuan, Liangwen
Citation	
Issue Date	2020-03
Type	Thesis or Dissertation
Text version	author
URL	<a href="http://hdl.handle.net/10119/16382">http://hdl.handle.net/10119/16382</a>
Rights	
Description	Supervisor: Beuran Razvan Florin, 先端科学技術研究科, 修士 (情報科学)

Master's Research Project Report

Assessment and Improvement of Security Awareness Training  
Methodologies

1810026 Liangwen Yuan

Supervisor Razvan Beuran  
Main Examiner Razvan Beuran  
Examiners Yasuo Tan  
Shinobu Hasegawa  
Yuto Lim

Graduate School of Advanced Science and Technology  
Japan Advanced Institute of Science and Technology  
(Information Science)

March 2020

## Abstract

IBM 2016 study of the cost of data breach for the USA found that the total cost of data breaches had increased 7% by an average. Some companies affected by a serious security incident lose not only the trust of their customers but also their entire business after a major data breach. The average data breach incidents are 29,611 records, a cost of \$221 each. It means during an accident, there is an estimated loss of \$6,544,000. What's more, not only data breaches, but also other security problems, like Viruses, Worms, Trojan horses and so on, are taking place which cause serious problem. Security awareness training is considered to be one of the main factors in reducing the risks of data breach and other security problems.

Security awareness training approach aims to teach people multiple layers of protection on the computer, network, program or data they intended to protect. There are a lot security awareness training programs and systems nowadays. We want to figure out whether they can be improved or not.

In this report, we introduce the security awareness training programs within four categories. The first category is e-learning training programs. When the interactive whiteboard appeared on the training site, it was big news because it replaced the old chalk and rags as a key tool for education. Today, online learning tools may make traditional classroom training a thing of the past. The second category is video training programs. Traditional training make it difficult to measure the effectiveness of training. With video, the training can be done on the road or at home. The more readily training are available, the more likely they are to be studied. It's safe to say that trainees prefer fast, engaging videos to other time-consuming training tasks. The third category is reading material training programs. When trainees have a chance to select their reading content, they have more ownership in education. Trainees must read at their own reading level and cannot rely on other's support to understand the materials. The fourth category is focus on technology training and practice. Technology training is critical to providing individuals with the computer tools they need to protect themselves from attacks. Common training content in technology training systems points to web security but also includes firewalls, DNS filtering, malware prevention, antivirus software and email security solutions.

For those security awareness training programs/systems categories introduced, we make a questionnaire to evaluate them. The questionnaire includes two parts, one is security knowledge quiz questions and the other is the actual assessment criteria. The main purpose of assessment criteria is to

see whether it meets its objectives or not. Therefore, we gather feedback and data on how participants feel about the training will enable us to identify ways to improve. This applies to any other area. Trainers can contribute to the company by developing the improvements we offer to conduct an effective training. In security knowledge quiz questions, we prepare 8 questions and participants don't know the difficulty and this part is not counted into the evaluation of training programs/systems. Participants can provide feedback on the concept of the question, the level of knowledge required to answer, the range of possible answers. It is the process of informal testing questionnaire for potential respondents. For example, if we find out a strange value for a participant in the assessment criteria, we can use his or her score of the security knowledge quiz questions to help us figure the reason whether the content is too difficult for him or her.

In assessment criteria, we create 9 close-end questions and 3 open-end questions depending on opinions from three experts in cyber security field. The 9 close-end questions are presented by Likert Scale. Some people advocate a 7-point or 9-point scale to add granularity. Sometimes using a 10-point (even number) scale to generate a forced choice measurement in which case there are no unrelated choices. However the most common scale is 5-point which is "Strongly agree", "Agree", "Neutral", "Disagree" and "Strongly Disagree". In our report, we use the common 5-point scale to measure the assessment criteria.

About calculation for the assessment criteria (Likert scale), we found a new method to measure discreteness that is expressed as agreement and disagreement. This measurement based on the recognized Shannon entropy utilizes the probability distribution and the distance between categories to generate a value spanning the unit interval. With this measurement, ordinal scale's data can be assigned a dispersion value which is logically and theoretically reasonable.

We select 6 representative participants among the original 25 participants to conduct our assessment criteria of three e-learning training programs, four video training programs and three advanced training systems. From the outcome, we want to improve the gamification and practicality (be practical or easy to apply) to e-learning training program; the learning environment, gamification, addressing real security threats and engagement to video training program; engagement and practicality (be practical or easy to apply) to advanced training system. Therefore, in the overall proposed improvements, we propose the detailed improvements which seems possible.

With 9 close-end questions and 3 open-end questions in this report, we can easily weed out old and ineffective training methods and find better ones. The more appropriate a safety awareness solution is to the unique needs of social

organization, the more effective it will be in reducing violations, building a strong security culture, and providing positive experiences for trainees.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Background . . . . .	1
1.2	Objectives . . . . .	1
1.3	Originality and Significance . . . . .	2
1.4	How to select the original 23 training programs/systems . . . . .	3
<b>2</b>	<b>E-learning Training Programs</b>	<b>4</b>
2.1	ProProfs . . . . .	4
2.2	Secure Click . . . . .	5
2.3	Marshal Security . . . . .	8
2.4	ECSM . . . . .	9
2.5	DARK Reading . . . . .	10
<b>3</b>	<b>Video Training Programs</b>	<b>13</b>
3.1	SANS . . . . .	13
3.2	ESET . . . . .	16
3.3	Khan Academy . . . . .	18
3.4	INFOSEC Institute . . . . .	19
3.5	Lynda.com . . . . .	23
3.6	MakeUseOf . . . . .	24
3.7	Udemy . . . . .	25
3.8	ENISA . . . . .	27
3.9	CSIAC . . . . .	29
<b>4</b>	<b>Reading Material Training Programs</b>	<b>31</b>
4.1	U.S. Security Awareness . . . . .	31
4.2	UNIVERSITY OF CALIFORNIA (Systemwide Information Security) . . . . .	33
4.3	INFOSEC . . . . .	35

<b>5</b>	<b>Advanced Training Systems</b>	<b>39</b>
5.1	DVWA . . . . .	39
5.1.1	Brute Force . . . . .	40
5.1.2	Command Injection . . . . .	43
5.1.3	CSRF(Cross-site request forgery) . . . . .	44
5.1.4	File Inclusion . . . . .	45
5.1.5	File Upload . . . . .	47
5.2	OWASP Security Shepherd . . . . .	52
5.3	OWASP Mantra . . . . .	55
5.4	GameOver . . . . .	56
5.5	Mutillidae . . . . .	58
5.6	Damn Vulnerable Linux . . . . .	60
<b>6</b>	<b>Assessment Criteria and Results</b>	<b>65</b>
6.1	General rules for writing survey questions . . . . .	65
6.2	Questionnaire in survey . . . . .	67
6.2.1	Part 1: Security Knowledge Quiz . . . . .	67
6.2.2	Part 2: Assessment criteria . . . . .	70
6.3	Likert Scale question . . . . .	74
6.3.1	Use Likert's five choices in the sample questions . . . . .	74
6.3.2	Scoring and analysis . . . . .	75
6.3.3	Scale of measurement . . . . .	76
6.4	Consensus Based Assessment (CBA) . . . . .	76
6.4.1	Consensus and Dissention . . . . .	77
6.4.2	Issues in consensus . . . . .	77
6.4.3	Rules for consensus . . . . .	77
6.4.4	Calculation for Cns . . . . .	78
6.4.5	The measure of consensus and the rules . . . . .	79
6.5	Results . . . . .	81
6.5.1	How to determine participants . . . . .	81
6.5.2	How to determine which training programs to assess . . . . .	82
6.5.3	Outcome . . . . .	82
6.5.4	The state of each training programs/systems . . . . .	85
6.5.5	Participants' answers in open-end questions . . . . .	86
<b>7</b>	<b>Analysis and Proposed Improvements</b>	<b>91</b>
7.1	The outcome comparison and analysis for 3 e-learning training programs . . . . .	91
7.2	The outcome comparison and analysis for 4 video training programs . . . . .	93

7.3	The outcome comparison and analysis for 3 advanced training programs . . . . .	95
7.4	Proposed improvements for each assessment criterion . . . . .	96
7.5	Overall Improvements . . . . .	98
<b>8</b>	<b>Conclusion</b>	<b>101</b>



# List of Figures

2.1	The homepage of ProProfs . . . . .	4
2.2	The homepage of Secure Click . . . . .	5
2.3	The homepage of Marshal Security . . . . .	8
2.4	The homepage of ECSM . . . . .	9
2.5	The homepage of DARK Reading . . . . .	10
3.1	The homepage of SANS . . . . .	13
3.2	The homepage of ESET . . . . .	16
3.3	The homepage of Khan Academy . . . . .	18
3.4	The homepage of INFOSEC . . . . .	19
3.5	The homepage of Lynda . . . . .	23
3.6	The homepage of MakeUseOf . . . . .	24
3.7	The homepage of Udemy . . . . .	25
3.8	The homepage of ENISA . . . . .	27
3.9	The homepage of CSIAC . . . . .	29
4.1	The homepage of U.S Security Awareness . . . . .	31
4.2	The homepage of UC(Systemwide Information Security) . . . . .	33
4.3	UC's TDI service . . . . .	34
4.4	The homepage of INFOSEC . . . . .	35
5.1	The homepage of DVWA . . . . .	39
5.2	Brute Force Login . . . . .	40
5.3	Brute Force intercept . . . . .	41
5.4	Brute Force Position . . . . .	41
5.5	Use built-in dictionary . . . . .	42
5.6	Load external dictionary . . . . .	42
5.7	The three links of File Inclusion . . . . .	46
5.8	File Upload low level . . . . .	48
5.9	File Upload medium level . . . . .	50
5.10	The homepage of OWASP Security Shepherd . . . . .	52
5.11	The homepage of OWASP Mantra . . . . .	55

5.12	The homepage of Mutillidae . . . . .	58
5.13	Successful SQL Injection attack . . . . .	60
5.14	DVL Login . . . . .	61
5.15	Determine to format which disk . . . . .	62
5.16	Select disk to be partitioned . . . . .	62
5.17	View the partition option . . . . .	63
5.18	Add a new partition . . . . .	63
5.19	View the created partition . . . . .	64
5.20	Save the new partition . . . . .	64
5.21	Exit . . . . .	64
6.1	Security Knowledge Quiz . . . . .	68
6.2	Security Knowledge Quiz . . . . .	69
6.3	Assessment Criteria . . . . .	73
6.4	The almost identical reliability of 5-7-11-point scales . . . . .	74
7.1	The outcome of 3 e-learning training programs . . . . .	91
7.2	The outcome of 4 video training programs . . . . .	93
7.3	The outcome of 3 advanced training programs . . . . .	95

# List of Tables

1.1	The criteria for original select of training programs/systems . . . . .	3
6.1	Masha Sedova's opinions and our choice . . . . .	70
6.2	Donald Kirkpatrick's opinions and our choice . . . . .	71
6.3	Jonathan Deller's opinions and our choice . . . . .	72
6.4	Lacking consensus data . . . . .	80
6.5	The movement towards a single category . . . . .	80
6.6	. . . . .	80
6.7	Security Knowledge Quiz results of the 24 participants . . . . .	81
6.8	The results of Proprofs . . . . .	82
6.9	The results of DARK Reading . . . . .	82
6.10	The results of Marshal Security . . . . .	83
6.11	The results of Lynda.com . . . . .	83
6.12	The results of Khan Academy . . . . .	83
6.13	The results of Udemy . . . . .	84
6.14	The results of SCIAC . . . . .	84
6.15	The results of DVWA . . . . .	84
6.16	The results of Security Shepherd . . . . .	85
6.17	The results of GameOver . . . . .	85
6.18	The state of each training programs/systems . . . . .	86
6.19	The answers of Proprofs . . . . .	87
6.20	The answers of Marshal Security . . . . .	87
6.21	The answers of DARKReading . . . . .	87
6.22	The answers of Khan Academy . . . . .	88
6.23	The answers of Lynda.com . . . . .	88
6.24	The answers of Udemy . . . . .	88
6.25	The answers of CSIAC . . . . .	89
6.26	The answers of DVWA . . . . .	89
6.27	The answers of Security Shepherd . . . . .	89
6.28	The answers of GameOver . . . . .	90

# Chapter 1

## Introduction

### 1.1 Background

As WannaCry and NotPetya recently demonstrated, cyber attacks are spreading at an unprecedented rate. The more networks are infected, the greater risk for other networks. Similarly, with the Internet, a decrease in the security of a single network increases the overall threat to other networks. A lack of security awareness training in one organization can leave other organizations vulnerable to attack. It's a bit like leaving a door unlocked – the key next door is waiting inside. Nowadays, as people have realized cyber security is a huge problem, there are many ways to get security awareness training, like books, videos or taking some courses; some authority websites provide professional training programs for companies to train their employees. But we cannot ensure the effectiveness of those training methods. According to an EMA research study, 48% of trainees stated they were measured the effectiveness of the security awareness training program; while 18% were certain that it was not measured and 34% did not have any idea whether the training was effective or not. In order to make sure the training is effective to trainees, the current developers begin to focus on interactive training ways.

### 1.2 Objectives

A good security awareness training is a great way to inform trainees of any kind of malicious activity. The important aspect of focus on is whether the training implemented is effective and really address the needs of the organizations or trainees themselves. Assessment is necessary. Attempts to ignore any assessment reflect a lack of interest and professionalism. The effort involved in designing any assessment pays off handsomely but identifying

the right questions is always the key starting point. In order to analyze and understand which factors have succeeded in achieving their objectives and which have not. When the time and cost of conducting a comprehensive evaluation are limited, we should consider which techniques and methods best suit the intended purpose. It is important to keep in mind the benefits and challenges of the selected tools before applying them to the assessment process. Therefore, in this research we first should do a detailed survey about how security awareness training is being conducted today. Then develop some assessment criteria. At last, considering in what ways current security awareness training could be improved, for example by using interactivity.

### **1.3 Originality and Significance**

Although security awareness training is being promoted energetically today, many trainees who got training before still suffer from phishing attacks in their daily life. If a training method cannot communicate with its trainees, resonate with them, make the training content impressive, then the warning of phishing attacks is likely to go in one ear and out the other.

Security awareness training needs to achieve a specific outcome. Before evaluating any solution, we should get clear on goals. Then search for a solution designed for that outcome, such as a 75% increasing in reporting incident rates, 80% decreasing in user-generated incidents, or 100% completion rate for the training. Another goal is to have trainees to want to take the training instead of being forced to take it.

In this research, we will assess the most used training programs within two categories, online training programs, which can be accessed via the Internet, and open-source training programs, which can be installed locally. Our main goal is to find out what kind of training is most effective and appreciated, such as gamification, competition or something that is straight-to-the-point and can act as a reference guide in the future. Section 2 discusses the online training programs and section 3 discusses the open-source training programs. Then, an assessment and an improvement of those training programs are separately presented in section 4 and section 5. This research ends with conclusions, acknowledgments and appendices.

## 1.4 How to select the original 23 training programs/systems

When we are ready to start security awareness training, we want an interesting approach to appeal our users and give them secure feeling. Therefore, we create those 4 generic assessment criteria to select the original 23 training programs.

Criterion 1	The training content is engaging.
Criterion 2	The training program is optimized for learning and retention of content.
Criterion 3	The training program is easy to undergo.
Criterion 4	The training program can address real security threats.

Table 1.1: The criteria for original select of training programs/systems

# Chapter 2

## E-learning Training Programs

E-learning is a learning system provided via a computer or other digital device, acting in an educational course online. It is lent to every type of training using various techniques like presentations, quizzes, games, simulations, social elements.

### 2.1 ProProfs

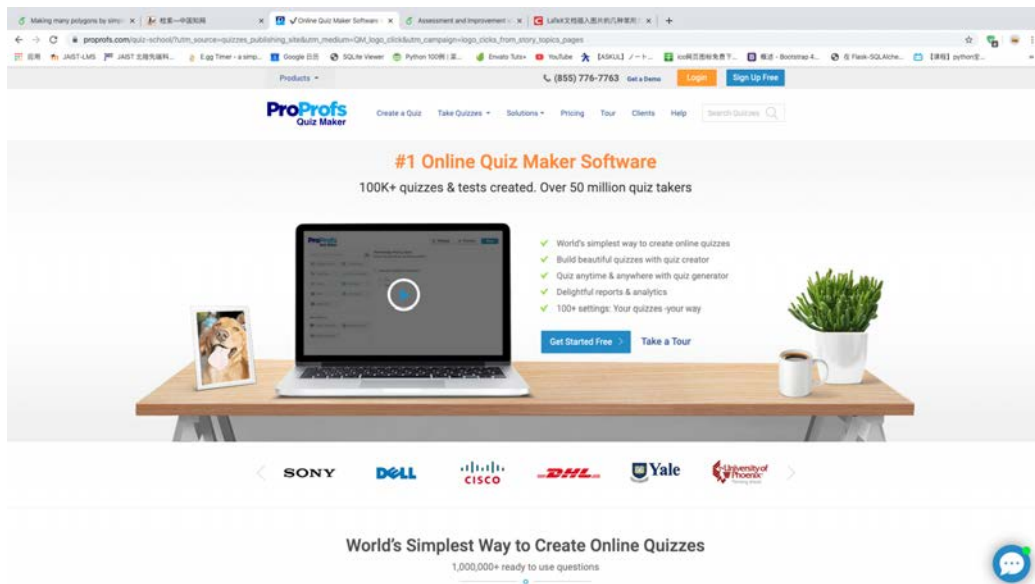


Figure 2.1: The homepage of ProProfs

ProProfs [1] was founded in 2010 by Sameer Bhatia, starting out as a quiz making website freely for users and developing into a full-fledged software provider for companies including SONY, Dell, CISCO, DHL, Yale and University of Phoenix at a fast speed. Look at Figure 2.1, this is the homepage of ProProfs. As of April 2013, there are more than 1 million registered users in ProProfs. In June 2015, HelpIQ was acquired for developing an online help center, user manuals, knowledge base. Until May 2019, ProProfs had more than 7 million website visitors every month and its global Alexa Rating is 4122.

The products line of Proprofs includes: survey and quizzes, knowledge base software and training course creation tools online. Also, for supporting reporting features, ProProfs provides LMS(Learning Management System). The ProProfs's tools are used for corporate training, business, e-learning and some other industries.

## 2.2 Secure Click

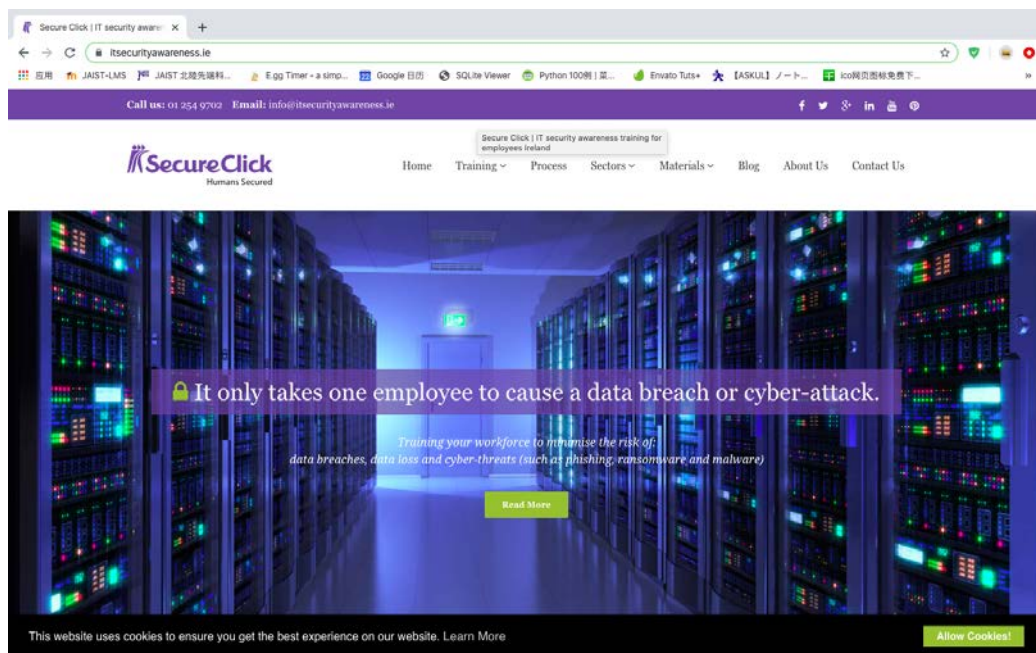


Figure 2.2: The homepage of Secure Click

Secure Click [2] are fervent about IT security and they are also interested in studying and changing human behavior in information security. Because the



most security threats today are designed to make use of poor user security behaviors.

In Secure Click, the following are training modules:

- IT Security is Everybody's Business  
This module lets users understand why IT restrictions are set and explain why failure to comply with them can lead to data leaks and network attacks.
- Cyber-security Awareness Training  
Embed network security practices among users to protect user organization from intrusions, IP theft and malware.
- Anti-Phishing/Spear-Phishing Training  
Spear phishing is the most common form of attack we've seen. It means a well-designed email is most likely to be sent to an unsuspecting trainee, potentially triggering a major data breach.
- Simulated Phishing Training  
At the Electricity Supply Board(ESB) which supplies power to Northern Ireland and the Republic, senior engineers are received a private email containing malware from a group linked to Russia's GRU intelligence agency.
- Ransomware Prevention Training  
Trainees need to be educated about ransomware threats to prevent ransomware infection.
- Information Security Training for Mobile Computing  
79 percent of businesses consider employees are the biggest security threat.
- Data Protection Training  
Human error plays an important role in data breaches. This module describes common data leakage and provides trainees with actionable measures to prevent.
- IT Policy Reinforcement  
82 percent cyber professionals worry about trainees not following cloud security policies.

For many people, Cyber security can be abstract and boring topic. The end-user security awareness training in Secure Click is engaging, interesting and relevant. Like the funny teacher you met in school when content is delivered in an interesting and engaging way, people will remember it. In addition, we try to use relevant examples of good security practices based on job titles of industry sectors or participants. People pay attention to it when they think the topic is related to them.

Cyber attacks can bring your daily operations to a complete standstill. Maersk, the Danish shipping company, ground to a halt globally when IT confirmed that its IT systems had been compromised. When the French television station TV5 suffered a serious cyber attack, their business was immediately shut down.

Stories abound about how cyber attacks forced organisations to stop operating. Cyber attacks not only cause inconvenience to the company's business, but also cause long-term damage to the way the company operates. With the right planning and implementation, you can identify threats before they become risks.

## 2.3 Marshal Security

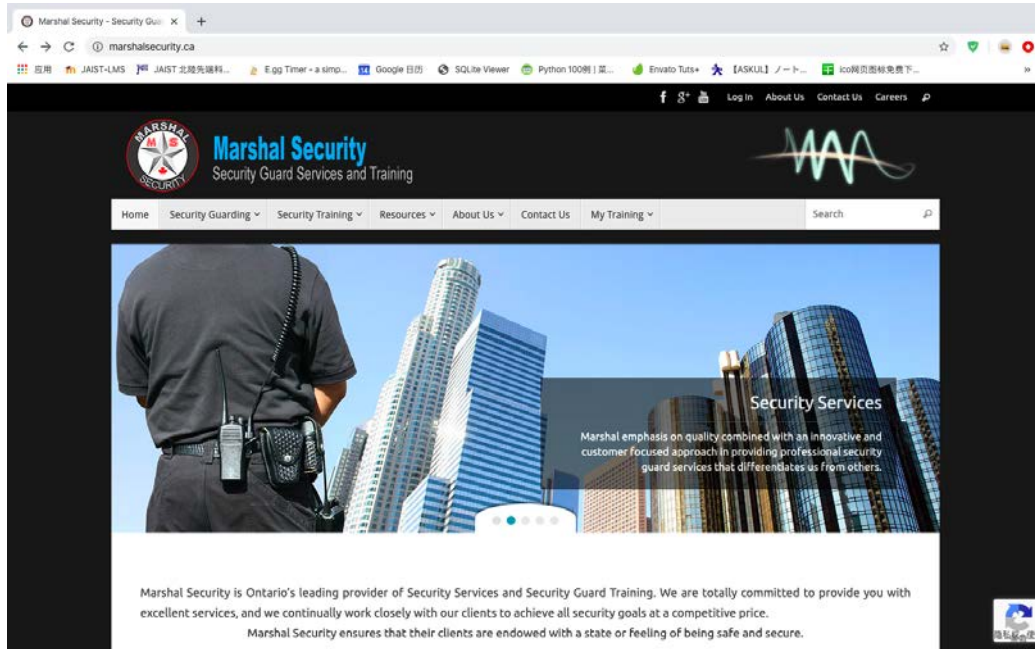


Figure 2.3: The homepage of Marshal Security

Marshal Security [3] is the best Provider of Security Guard Training and Supplier of Security Services. They are contributed to encompassing Security Guarding, Ontario Security Guard Training and CCTV solutions. Totally they are committed to provide users perfect services and work continually with clients to realize all security goals with a competitive price.

Marshal Security is a member of the speediest growing security companies in Canada. It has the expertise to provide professional, high quality, cost-effective and reliable security training and security guarding services by retail, public sector and corporate.

Whatever and whenever are user's needs relevant to security, Marshal Security can be trusted to offer users professional services customized and completely integrated to answer their needs. Marshal Security provides security guarding solutions to shopping centres, retail stores, industries, educational institutions, health care, condominiums, corporate offices, custom events, office complex and so on. Their office building for security are fully trained, licensed and produce the best standards which is required.

The commitment and dedication of Marshal Security enable them to provide an improving service including the very newest technology and ensuring

the professional training programs to satisfy every user's needs. They give prompt and professional response and the piece of mind and satisfaction of knowing to fulfill users' security requirements.

Marshal Security is an approved excellent centre training with the licensing requirements under the Private Security and Investigative Services Act, 2005. They not only provide In-class but also online Ontario Security Guard training to prepare users for achieving their Security Guard Licence.

## 2.4 ECSM

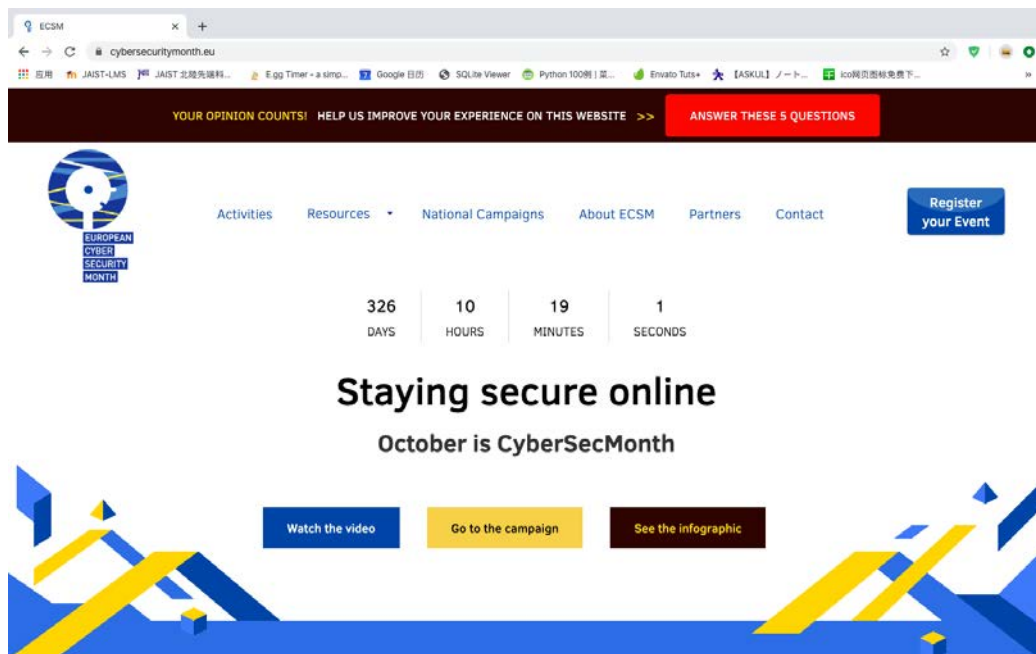


Figure 2.4: The homepage of ECSM

European Cyber Security Month(ECSM) [4] is an European Union awareness campaign. It encourages cyber security to citizens and organizations about the importance of information security and also highlights the simple steps which can be operated to protect their financial, personal or professional data. Raising awareness, changing behaviour and providing resources to all people about how to protect themselves in current cyber environment online is the main goal.

The European Union Agency for ENISA(European Union Agency for Network and Information Security) and the European Commission DG CON-

NECT and Partners are contributed to deployed the European Cyber Security Month(ECSM) every October.

The objectives of the European Cyber Security Month(ECSM): 1.Generate general awareness of cyber security, which is one of the main priorities identified in the European Union Cyber Security Strategy. 2.Generate specific awareness on Network and Information Security(NIS), which is presented in the proposed NIS Directive. 3.Promote more safer use of Internet to all users. 4. Develop a string track record through ECSM to raise people's awareness. 5.Absorb relevant stakeholders. 6.Arouse national media interest through the European and global dimensions of the projects. 7.Increase interest and attention in regard to information security through media and political coordination.

## 2.5 DARK Reading

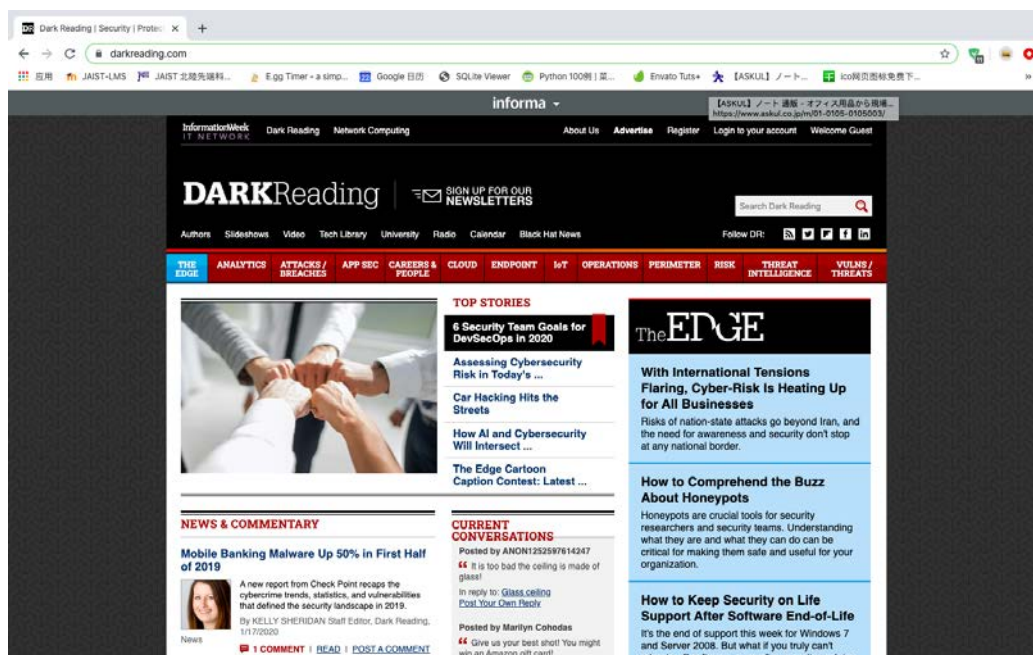


Figure 2.5: The homepage of DARK Reading

As one of the most widely read Internet security sites, DARK Reading [5] is the most popular online community for security professionals. The community includes leading thinking security researches and technologists.

This is where enterprise security personnel and policy makers learn about new cyber threats, vulnerabilities and technology trends. Here, they discuss potential defense against the latest attacks, as well as key technologies and practices that could help protect their sensitive data in the future. They can communicate with each other, embrace new ideas with DARK Reading editors, find answers to their security problems and solve their pressing problems.

DARK Reading includes 13 communities, each of them delves into security challenges: analysis, attack and sabotage, application security, careers and people, cloud security, endpoints, Internet of Things, mobile, operations, perimeter, risk, threat intelligence, vulnerabilities and threats. Editors and subject matter experts lead each community. They collaborate with security researchers, technical experts, industry analysts to provide timely, accurate, informative articles to generate spirited discussions.

DARK Reading is a platform where cyber security researches, consultants and technicians collaborate across industries and regions to build a better defense but not every platform has the same goals. Therefore, DARK Reading has a range of media tools and custom services to allow marketers building a program to meet their needs like:

Lead Generation:

- Custom Research Report
- Research Report
- Technology Digests
- Theme Alignment Program
- Virtual Events
- Web Seminar

Native Advertising:

- Sponsored Article
- Partner Perspective
- Native Content Advertising Unit

Advertising:

- Advertising Targeting

- In-Read Video
- Banner Advertisements
- e-Newsletters

# Chapter 3

## Video Training Programs

A security awareness training video, whether a knowledge training or technology training, is a video focus on educating trainees on a specialized topic. In short, the video based content shows people how to do something.

### 3.1 SANS

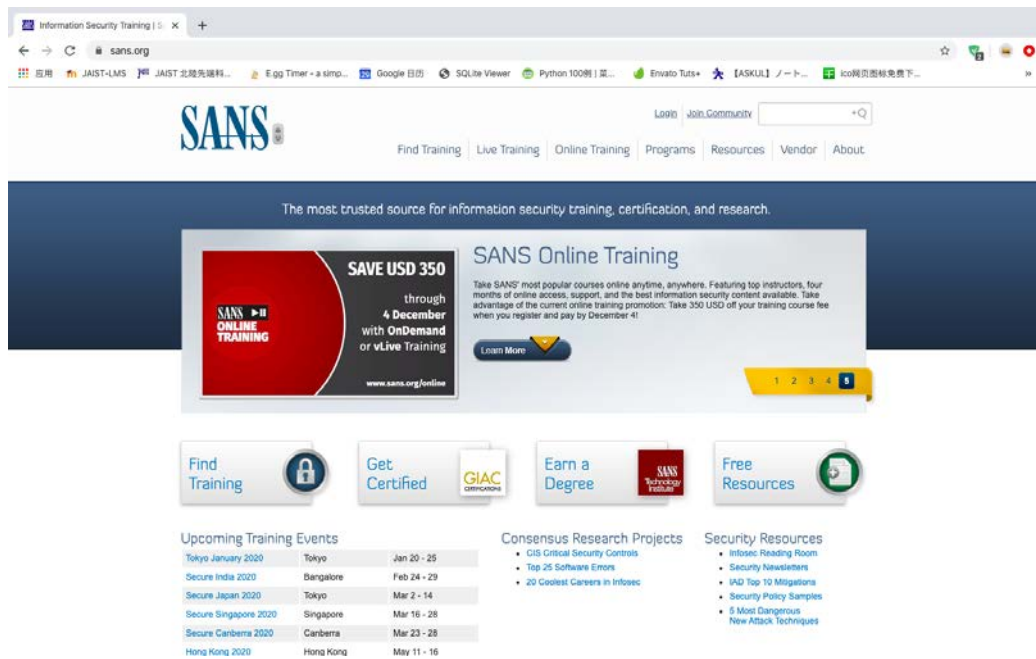


Figure 3.1: The homepage of SANS



In 1989, SANS [6] Institute was built as a cooperative and educational organization. Today, its programs has reached over 165,000 security professions around the world. From network administrators to information security offices, a wide range of individuals are sharing the learnt content and looking for solutions to face their challenges. Various global organizations' security professionals from universities to corporations are the heart of SANS. They are working jointly to help the whole security community.

By far, for information security training and security certification SANS is the most believable and the most rich source in the world. It is free of development, maintenance and available for the largest collection of research about different aspects of information security. The Internet's beginning warning system named Internet Storm Center is operated by SANS.

SANS offers concentrated, immersion training to help users take the practical steps necessary to defending against the most dangerous security threats. The courses include important and useful technical skills you can apply in work as soon as you go back your offices. They were improved by a continued process including many administrators, information security professionals and security managers and deal with security fundamentals and awareness.

From SANS-certified instructors, self-paced in the Internet around the world, SANS training can be taken in class. SANS programs provide education for over 30,000 people internationally every year. In order to look for the perfect instructors in each topic, SANS operates a competition for instructors. More than 90 people participated but only 5 people were passed.

Work Study Program is also provided by SANS acting as a candidate of SANS conference member and coordinators would attend not at a incremental rate. Coordinators are expected to achieve their educational recompense for what they are doing.

- Information Security Training — Over 400 courses in 90 cities around the world
- The GIAC Certification Program — Technical Certification for people to protect systems

Many valuable SANS resources are free to all users including Internet Storm Center, NewsBites(the weekly news report), @RISK(the weekly vulnerability report and original information security research thesis.

- SANS Information Security Reading Room — 3000+ original research thesis in 100 important categories of security

- SANS Weekly Bulletins and Alerts — Authoritative updates on security news and vulnerabilities
- SANS Security Policy Projects — Highlighting the vendors that can help make security more effective
- Vendor Related Resources — Drawing attention to the vendors that can help make security more effective
- Information Security Glossary — Words, acronyms, more
- Internet Storm Center — The Internet's Early Warning System
- S.C.O.R.E — Helping the security community reach agreement on how to secure guard common software and systems
- CIS Critical Security Controls — A consensus ranking of the security controls that are the most effectiveness in declining risk from real world attacks.
- SANS Press Room — Our press room is designed to assist the media in coverage of the information assurance industry

## 3.2 ESET

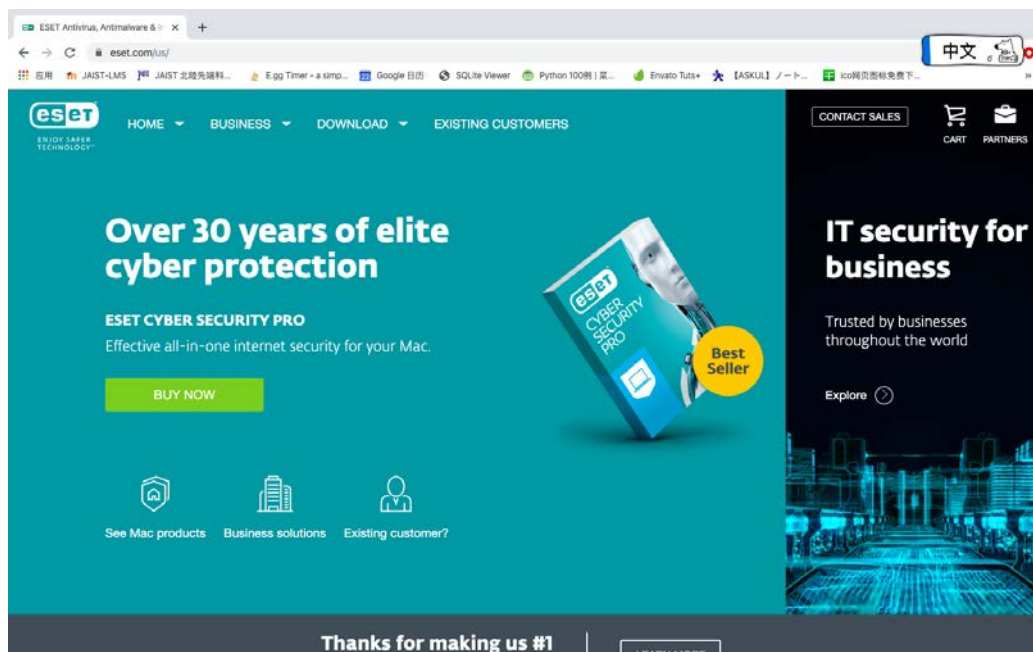


Figure 3.2: The homepage of ESET

ESET [7] is held privately, building its branch company in San Diego,US; Montreal Canada; Buenos Aires, Argentina and some other countries as well as more than 180 countries.

ESET proves it has the fastest worldwide growth rate in the range of the Consumer Security industry for 2011 according to Gartner. And also according to the Gartner report, a fundamental installed base in Europe especially in Eastern Europe has been built by ESET and it has a fast growing business presence. Its Completeness of Vision score is beneficial from malware effectiveness in a lightweight client but suffering from weak expert management capabilities and lacking of investment in market — leading features like virtualization and application control. ESET is a good option for organizations looking for an light, effective, integrated malware solution.

ESET is proud of its rich history and numerous achievements :

In 1987, NOD, ESET's first antivirus code, is developed by ESET's founders.

In 1992, ESET, spol. s r.o. is established; its first AV products go on sale in Czechoslovakia and abroad.

In 1995, a streamlined version of ESET's NOD-iCE antivirus program is released.

In 1995, ESET NOD32 v1.0 wins its first VB100 award for malware detection.

In 1999, ESET, LLC is established in San Diego (USA).

In 2004, ESET's Latin America office opens in Buenos Aires (Argentina).

In 2009, Inc. magazine ranks ESET as one of America's fastest-growing private companies.

In 2010, Our Asia-Pacific office opens in Singapore.

In 2010, ESET becomes the first company to receive 60 VB100 awards for malware detection.

In 2012, ESET exhibits for the first time at the GSMA Mobile World Congress in Barcelona.

In 2012, A new ESET technology hub opens in Montreal(Canada).

In 2013, ESET opens its office in Jena(Germany).

In 2013, ESET marks an unbroken 10-year run of VB100 awards.

In 2013, Launch of dedicated WeLiveSecurity website, covering a vast spectrum of security-related topics.

In 2014, ESET wins the Peter Szor Award for uncovering Operation Windigo.

In 2015, More than 1,000 employees worldwide now work for ESET.

In 2016, ESET opens its office in Toronto.

### 3.3 Khan Academy

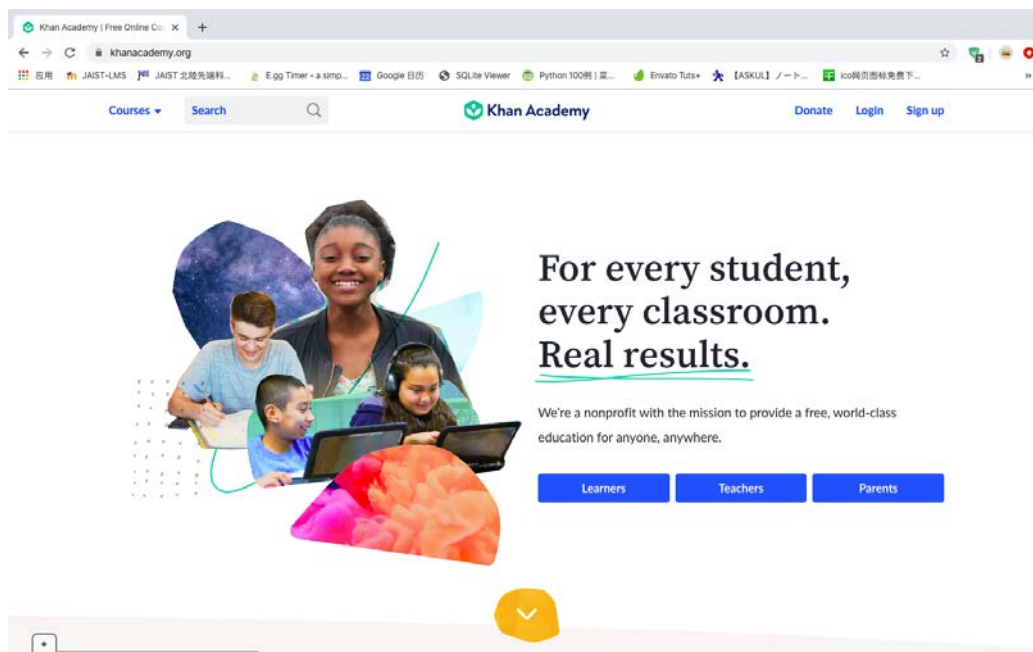


Figure 3.3: The homepage of Khan Academy

Khan Academy [8] is created in 2008 as a non-profit educational organization aiming at helping educate students with online tools. It generates lessons in the form of videos. Khan Academy's website includes supplementing exercises and learning materials to educators. All resources are free to website users. The website and the content are mainly provided in English and other languages including Armenian, Bulgarian, Chinese, Danish, French, Dutch, Czech, Bengali, Georgian, German, Gujarati, Hindi, Indonesian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Serbian, Spanish, Swedish, Tamil and Turkish.

Khan Academy provides exercises, a personal learning board and instructional videos to encourage learners study at pace on their own at any place. The videos are displayed on an blackboard similar to a teacher giving a lecture. The teacher describes every drawing and the relation to material which is taught. In Latin America, Asia, Africa, the groups with no profit distributes the videos which are not connected to Internet. The videos cover all subjects and range from kindergarten to high school.

## 3.4 INFOSEC Institute

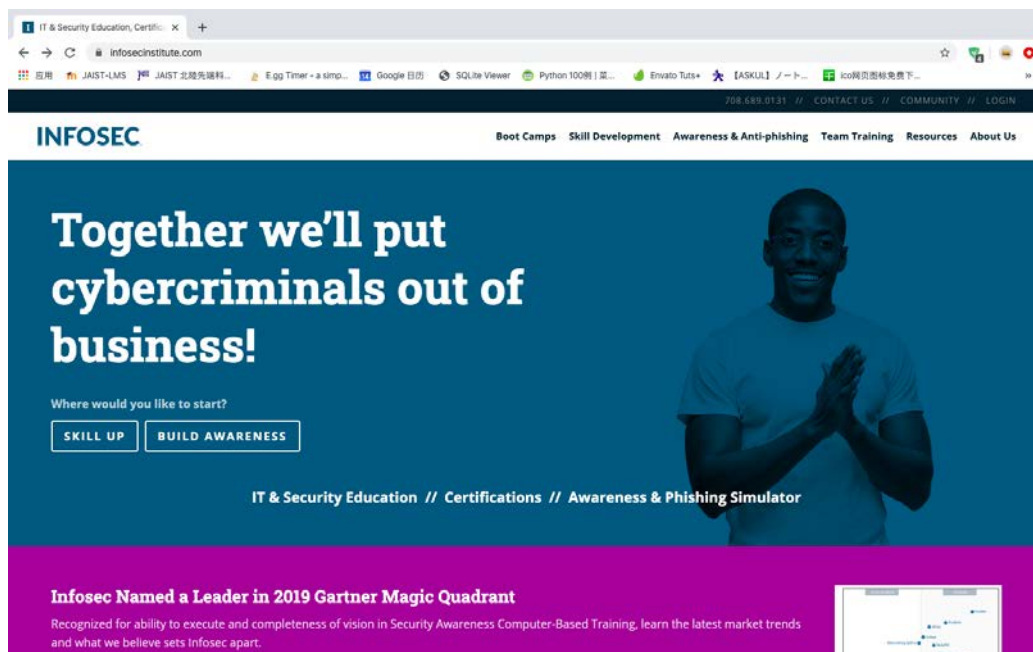


Figure 3.4: The homepage of INFOSEC

Infosec [[infosecinstitute](https://infosecinstitute.com)] believes that knowledge is the most powerful tool in fighting against cybercrime. IT and security professionals careers are advanced with skills development training and a full regimen of certifications. All employees are also empowered with security awareness and training to remain secure at work or home.

Established by smart users wanting to do better, Infosec educates how to defend from cybercrime to entire organizations and equipping everyone with the newest security skills is what Infosec is doing every day so that the good guys win.

Tools to help users outmart the bad guys:

### 1. INFOSEC IQ

With the knowledge and skills to remain cybersecure at work or home empowering users, more than 2,000 security awareness resources and phishing simulations are helped to change users behaviour and culture.

- Infosec IQ content library. Its massive library about role based training resources and industry is updated weekly to help users deliver relevant and fresh training whatever the style they need.

- Security awareness resource center. From here starting security awareness program. Users can download their cybersecurity tips to share with their friends and they can explore Infosec security awareness webinar library.
- Funny situations, real security training. Users will learn to love and connect with the office security through watching and learning as characters and they can still manage to keep themselves in-office behaviors.

## 2. INFOSEC Skills

Keeping users skills updated year-round. Over 50+ security certification studying paths and more than 400 courses are opened to the National Initiative for Cybersecurity Education's Cyberseek model.

When users are growing in their cybersecurity career, Infosec Skills takes the role as the platform to make sure their skills are able to defeat the latest attracts. According to courses are directly mapped to the NICE Cybersecurity Workforce Framework, users can control their career and get ahead of criminals and learn building defenses to future threats.

### **Cybersecurity roles :**

- Cybersecurity specialist / technician
- Cybercrime analyst / investigator
- Incident analyst / responder
- IT auditor
- Cybersecurity analyst
- Cybersecurity consultant
- Penetration and vulnerability tester
- Cybersecurity manager / administrator
- Cybersecurity engineer
- Cybersecurity architect

### **Featured learning paths**

Skill paths:

- Ethical Hacking
- Information Security Fundamentals

- Networking Fundamentals
- Computer Forensics
- Mobile Forensics
- Computer Incident Response
- Web Application Pentesting
- Malware Analysis & Reverse Engineering
- ICS / SCADA Security Fundamentals
- Information Security Auditing

Certification paths :

- $(ISC)^2$  CISSP
- CompTIA Security+
- CompTIA PenTest+
- CompTIA CySA+
- EC-Council Certified Ethical Hacker(CEH)
- Cisco Certified Network Associate R&S(CCNA)
- Project Management Professional(PMP)
- ISACA Certified Information Systems Auditor(CISA)
- ISACA Certified Information Security Manager(CISM)
- Certified Computer Forensics Examiner(CCFE)

**Featured courses :**

- Security Technologies and Tools
- Threats and Threat Actors
- Common Malware Behavior
- Introduction to Cryptography
- Introduction to Reverse Engineering
- Computer Forensics Investigations
- Digital Evidence and Legal Issues
- Fundamentals of Exploitation
- Post-Exploitation Techniques
- Obfuscation, Encoding and Encryption



**Featured courses :**

- Security Technologies and Tools
- Threats and Threat Actors
- Common Malware Behavior
- Introduction to Cryptography
- Introduction to Reverse Engineering
- Computer Forensics Investigations
- Digital Evidence and Legal Issues
- Fundamentals of Exploitation
- Post-Exploitation Techniques
- Obfuscation, Encoding and Encryption

3. INFOSEC Flex

Designing boot camps for advancing users career to help them pass their first certification exam and guaranteed. Users can take from any location on their favourite.

## 3.5 Lynda.com

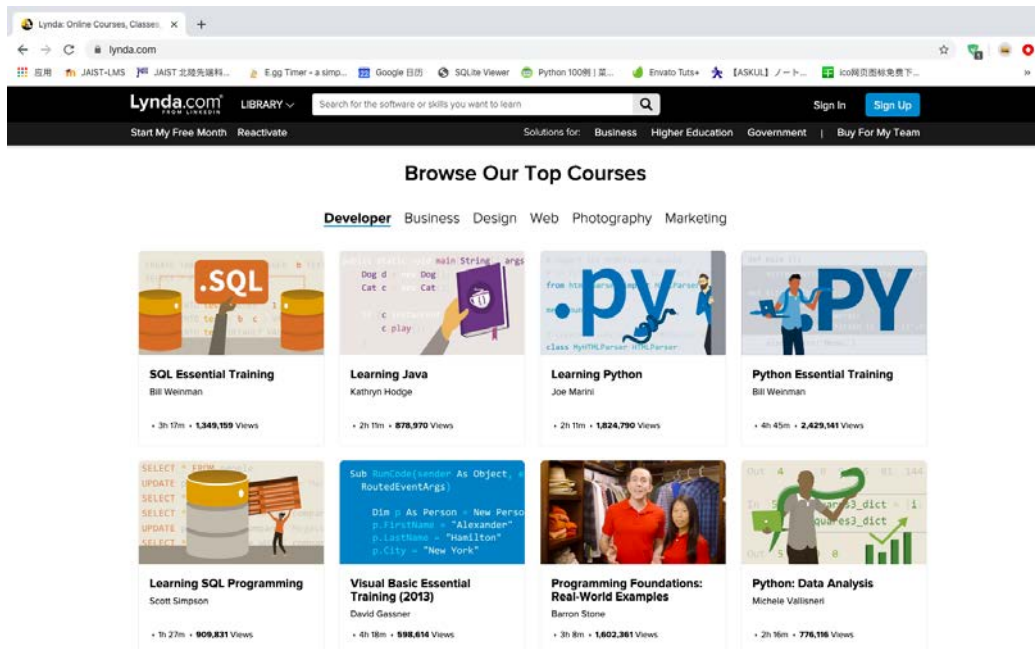


Figure 3.5: The homepage of Lynda

Lynda.com [9] is a leading learning online platform helping people study business, software, technology and skills to reach their goals. Learning by individual, corporate, academic, users are able to access to Lynda's video library of qualitative, attractive courses taught by recognized experts. Lynda has given learning to students, leaders, IT design professors, project managers. software developers. More than 10,000 organizations are severed in Lynda with five languages, Lynda is a global successful platform. For Developer Training and Tutorials course, learning how to code how to create applications in Java those object-oriented functional programming. At Lynda's developer tutorials, users can learn developing and creating mobile apps and work with PHP, MySQL databases, start with the statistical processing language R and so on.

## 3.6 MakeUseOf

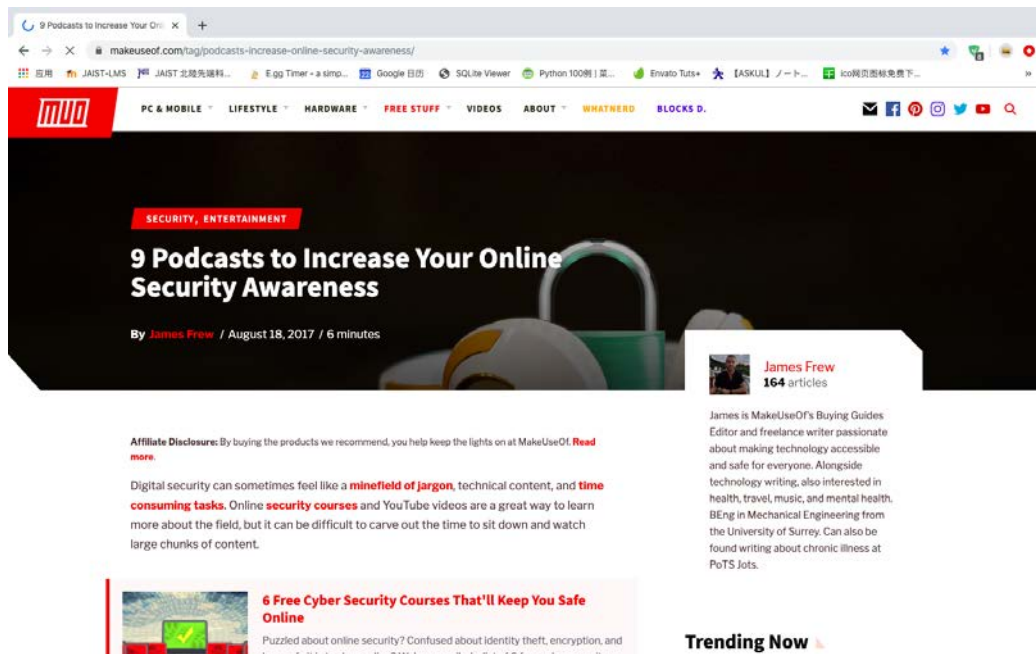


Figure 3.6: The homepage of MakeUseOf

MakeUseOf [10] was founded in 2007 as an online publication releasing tips and guides on how to take the most advantage of Internet, computer software and mobile applications.

In PC & Mobile modules, there are 6 fields:

1. Windows

Know your Windows operating system inside. Get tips, tricks and find out the best Windows software and modern applications.

2. Mac

If you have different ideas, please read this field carefully. You'll find the best software to do almost anything on your Mac, some of Apple's less known guides and hints to speed up Mac OS workflow.

3. Linux

Take advantage of the best open source operating systems on the planet. We'll focus on the best Linux distributions, software, games and share useful tips for users switching operating system.

#### 4. Android

A tutorial that teaches you how to best customize and use your Android smartphone, tablet, or other device.

#### 5. Security

It is vital to keep your personal online data and private source. With the beat firewall and antivirus, you will learn how to manage your passwords and identify fraud and security risks.

#### 6. Programming

Whether you are a novice or an expert programmer, you can find everything from Python and SQL.

### 3.7 Udemy

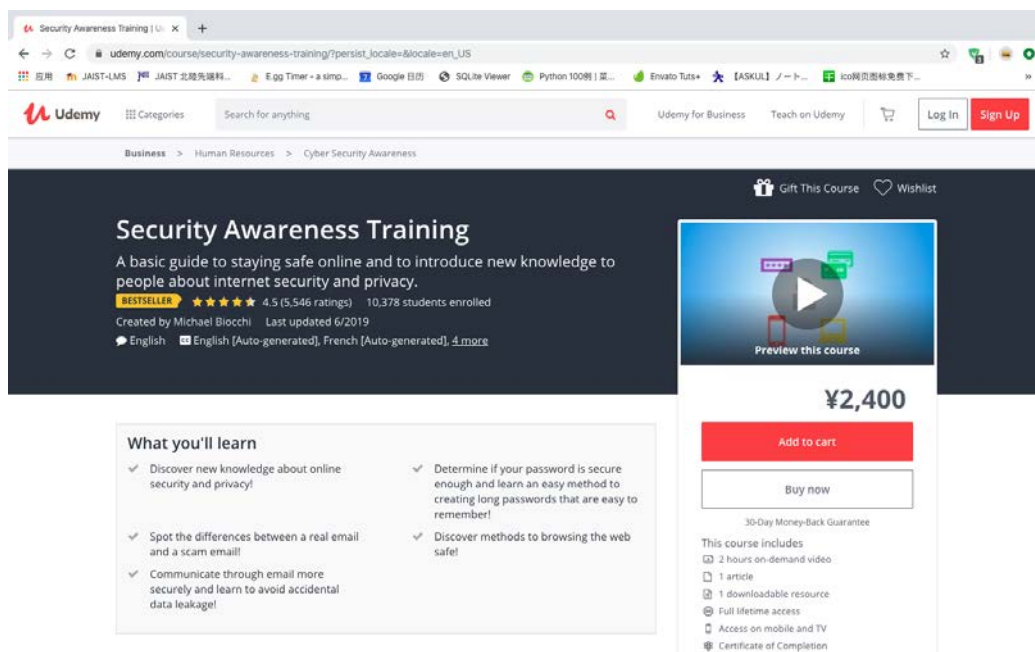


Figure 3.7: The homepage of Udemy

Udemy [11] is providing a learning platform for students and professional adults. It is a portmanteau of YOU + ACADEMY, has 50,000 instructors

teaching a wide variety of courses(over 4,000 million course enrollments) in over 60 kinds of languages and more than 30 million students.

Instructors and students come from over 190 countries and 2/3 of the students are not located the U.S. Udemy also owns more than 4,000 enterprise customers and 80% of Fortune 100 companies using Udemy for improving employee skills through Udemy for Business. Most students take courses as for improving job-related skills and some courses are generated toward achieving technical certification. Udemy has done a special effort to appeal corporate trainers seeking to design coursework for employees in their company.

Until 2019, Udemy has more than 130,000 courses online. Furthermore, Udemy allows instructors to create online courses freely on topics of their choosing as a serving platform. In Udemy, they can upload PowerPoint, presentations, PDFs, audio, zip files and live classes by using course development tools to create courses. Instructors can also engage or be interactive with uses through online discussion.

Courses are offered in each category including the arts, business and entrepreneurship, health and fitness, language, music and technology. Most classes such as Excel or using an iPhone camera are in practical subjects.

Udemy for Business is also offered in Udemy, building business access to the targeted over 3,000 training courses from the topics of digital marketing to design, programming, office productivity and more. For corporate training, organization users they can develop custom learning portals.

Udemy has been worthy of note for the various courses provided, and is part of the developing Massive Open Online Course(MOOC) moving available among the traditional university system.

## 3.8 ENISA

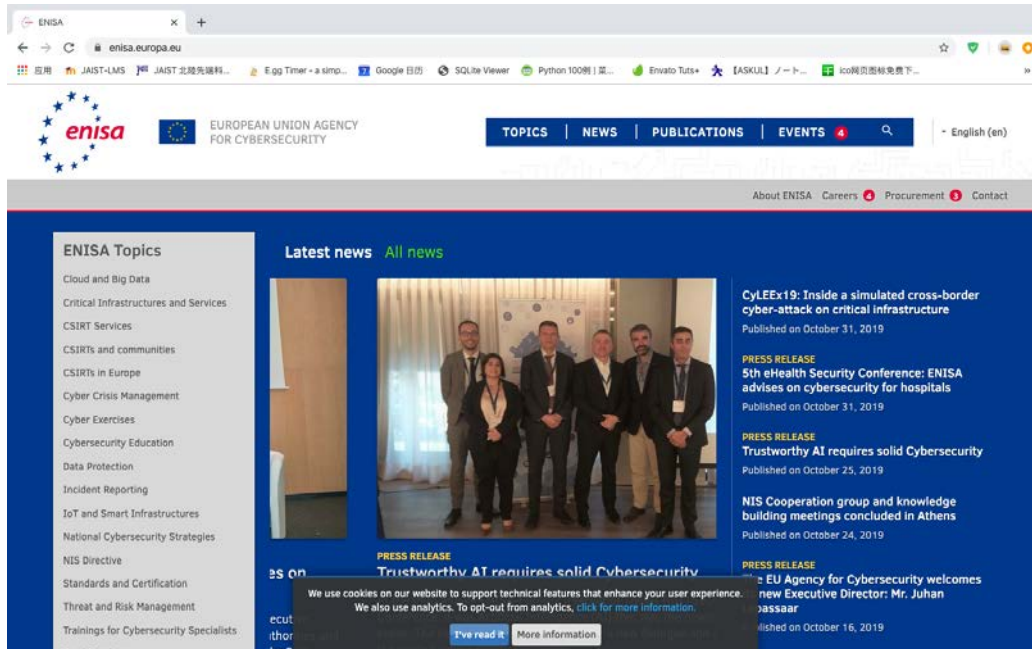


Figure 3.8: The homepage of ENISA

The abbreviation ENISA's [12] original name is the European Union Agency for Cybersecurity, created by EU Regulation No 460/2004 in 2004 under the name of European Network and Information Security Agency. Since September 1, 2005 it is in full operation. The Agency is in Athens, Greece and owns a second office in Heraklion, Greece.

The Agency works as a partner with the EU Member States and other stakeholders to provide suggestions and solutions and improve their capabilities in cybersecurity. This support includes:

- the pan-European Cybersecurity Exercises;
- the development and evaluation of National Cybersecurity Strategies;
- CSIRT's cooperation and capacity building;
- studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, and others.

Since 2019 it gives support to develop a cooperative response for large scale and cross-border cybersecurity incidents, it has been in process in drawing up cybersecurity certification.

ENISA cooperates the Member States, the Commission and the business community in satisfying the requirements of information security and network, whatever present and future EU legislation. Ultimately ENISA tries to operate as a centre of expertise for EU Institutions and Member States to find advice on incidents relevant to information security and network.

ENISA's approach is presented below by its activities:

- Suggestions on cybersecurity and independent suggestions;
- Activities which provide assistance to policy making and implementation;
- According to hand-on work, ENISA collaborates with operational teams throughout EU directly;
- Drawing up cybersecurity certification;
- Linking with each EU Community and coordinating the reaction to large cross-border incidents in cybersecurity.

## 3.9 CSIAC

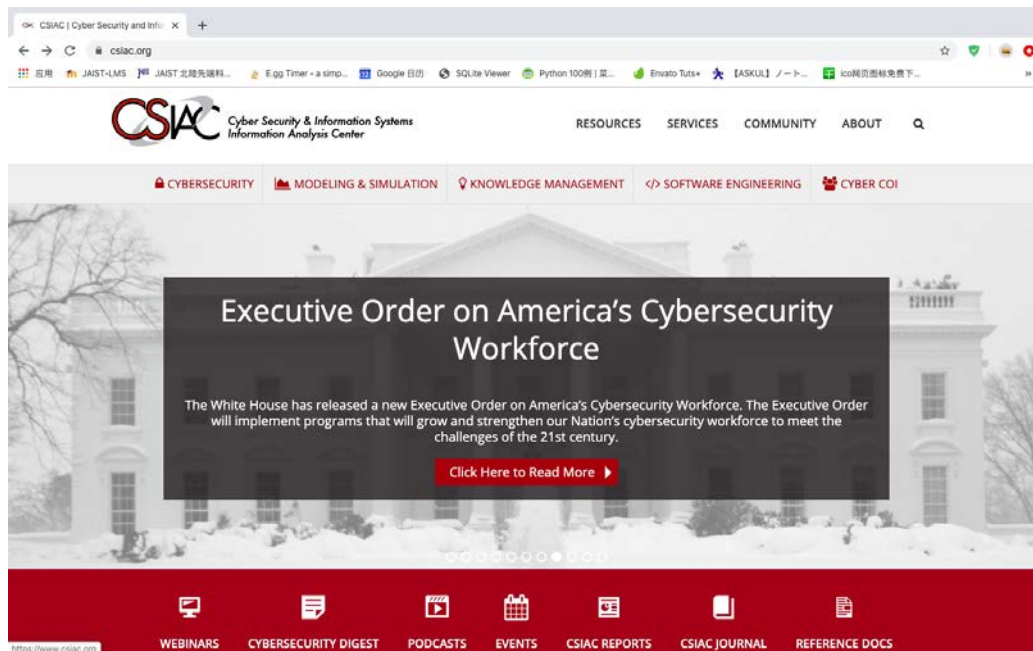


Figure 3.9: The homepage of CSIAC

The Cyber Security and Information Systems Information Analysis Center [13] is a Department of Defense(DoD) Information Analysis Center(IAC) supported by the Defense Technical Information Center. The three names used before are: Data and Analysis Center for Software(DACS), Information Assurance Technology IAC(IATAC) and Modeling & Simulation IAC(MSIAC), with the technical area of Knowledge Management and Information Sharing. The Cyber Security and Information Systems Information Analysis Center is sponsored by DTIC, performing the Basic Center of Operations functions and it is necessary to realize the objectives and missions which is applicable to the needs of DoD Research, Development, Test and Evaluation and Acquisition communities. The collection, synthesizing/processing, analysis and dissemination of Scientific and Technical Information(STI).

The Basic Center of Operations functions, explicitly the collection and dissemination of Scientific and Technical Information, produce some worthy resources in the core technology areas of Cyber Security and Information Systems Information Analysis Center like Software Engineering, Knowledge Management/Information Sharing, Modeling & Simulation and Cybersecurity. Beside offering access to resource we have mentioned before, the Cyber



Security and Information Systems Information Analysis Center performs towards 4 hours support reponensing to Technical Inquiries. Another service Core Analysis Tasks(CATs) provided by the CSIAC are funded by the issuance of Delivery Orders.

CSIAC provides the following types of produce :

- State-of-the-Art Reports
- Technology Assessments/ Critical Reviews
- Handbooks/ Data Books
- Technical Journals
- Webinars&Podcasts

CSIAC provides the following types of service :

- Free Technical Inquiry Services
- Core Analysis Tasks
- Subject Matter Expert Referrals
- Training Classes

The Cyber Security and Information Systems Information Analysis Center is contributed to give people best practices and skills from industry, government in information technology and cyber security. The assignment is to supply DoD with a central point of approach to Cybersecurity and Information Assurance for emerging technologies in vulnerabilities, models and analysis to develop and implement the effective defense against information attacks.

# Chapter 4

## Reading Material Training Programs

### 4.1 U.S. Security Awareness

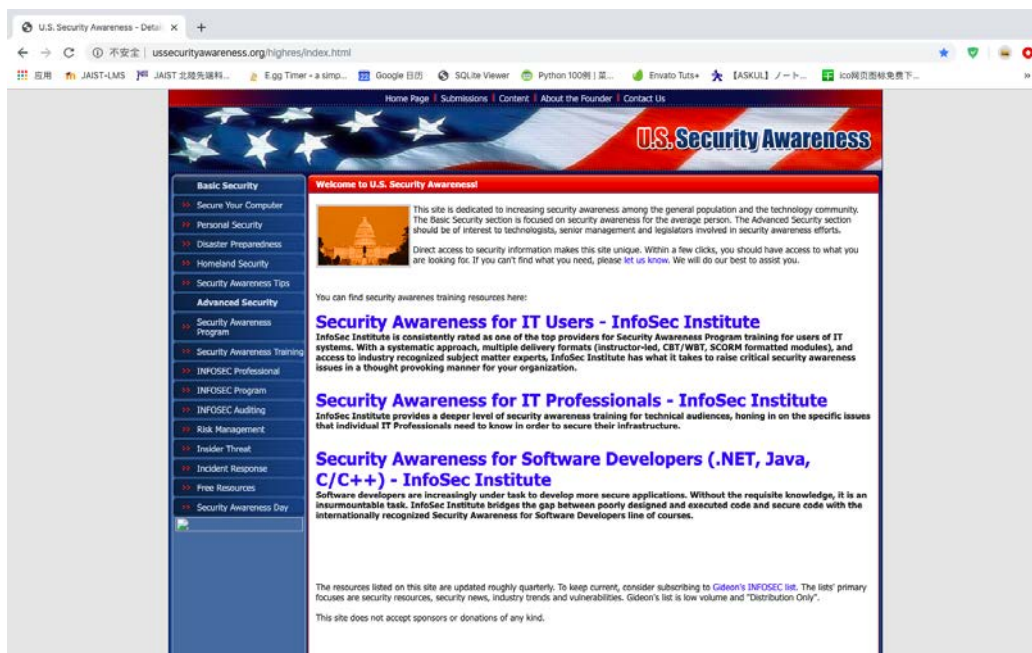


Figure 4.1: The homepage of U.S Security Awareness

The site [14] is dedicated to raising safety awareness among the public and the technology community. The basic safety section focuses on the safety

awareness of ordinary people. Senior security departments should be interested in technicians, senior managers, and legislators involved in security awareness.

U.S. Security Awareness has been rated as one of the top providers of IT system user security awareness training. With a systematic approach, multiple delivery formats (including instructor-guided, CBT/WBT, SCORM modules), and access to industry-recognized subject matter experts. It can raise key security awareness issues for your organization in a thought-provoking manner.

U.S. Security Awareness provides a deeper level of security awareness training for technical personnel on specific issues that IT professionals need to understand in order to protect their infrastructure.

Software developers increasingly need to develop more secure applications. It is an impossible task without the necessary knowledge. The InfoSec institute provides software developers with a bridge between poorly designed and executed code and secure code, and provides them with an internationally recognized sense of security.

There are two sections in U.S. Security Awareness:

#### 1. Basic Security

- Secure Your Computer
- Personal Security
- Disaster Preparedness
- Homeland Security
- Security Awareness Tips

#### 2. Advanced Security

- Security Awareness Program
- Security Awareness Training
- INFOSEC Professional
- INFOSEC Program
- INFOSEC Auditing
- Risk Management
- Insider Threats
- Incident Response
- Free Resources
- Security Awareness Day

## 4.2 UNIVERSITY OF CALIFORNIA (Systemwide Information Security)

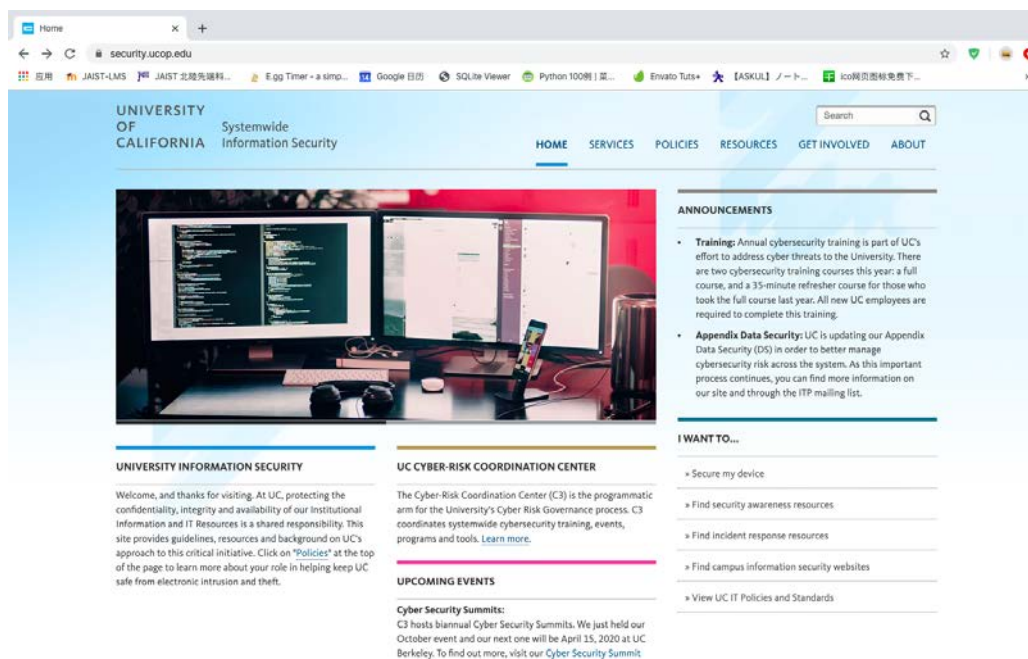


Figure 4.2: The homepage of UC(Systemwide Information Security)

The University of California Office [15] of the President tries to establish a secure environment for technology development which can protect information in University of California and cyber resources and reduces disruption to research mission and academic mission. Nevertheless, technology alone is not able to protect Institutional Information at all times. Every person at UC has an obligation to guard Institutional Information and IT resources. The Cyber-Risk Coordination Center(C3) is the programmatic support for the Cyber-Risk Governance process at UC. Systemwide cybersecurity training, events, programs are coordinated with C3.

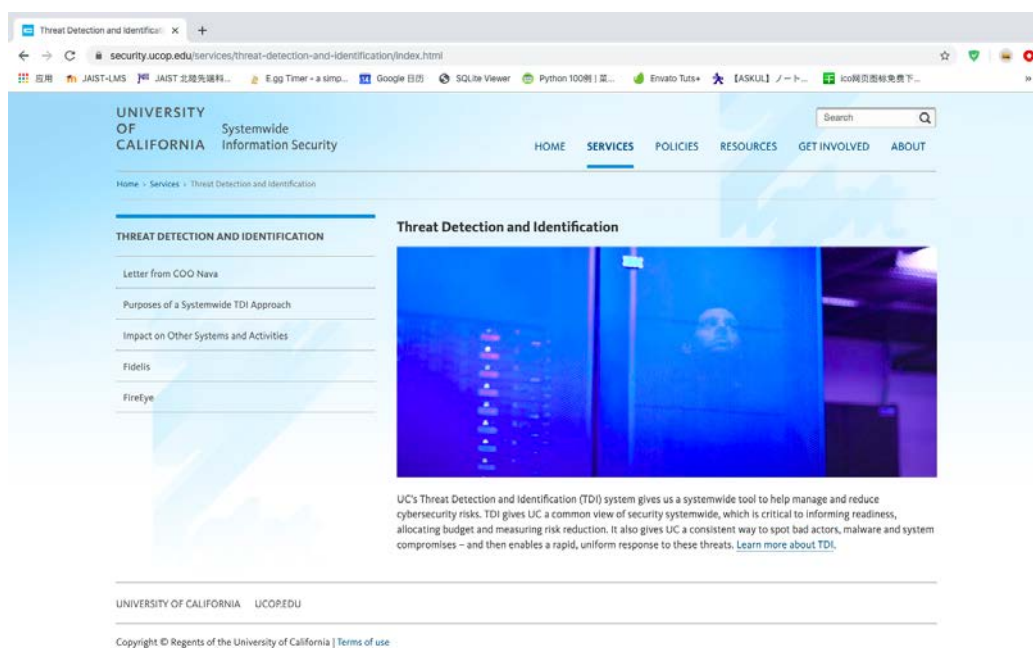


Figure 4.3: UC's TDI service

Threat Detection and Identification(TDI) system takes the role of a systemwide tool to assistant management and reduction of cybersecurity risks and gives a common view of security which is critical to notifying readiness, measuring reduction of risk and budget. Also giving a consistent way to UC to identify malware and system compromises and enables a rapid response to any risks.

## 4.3 INFOSEC

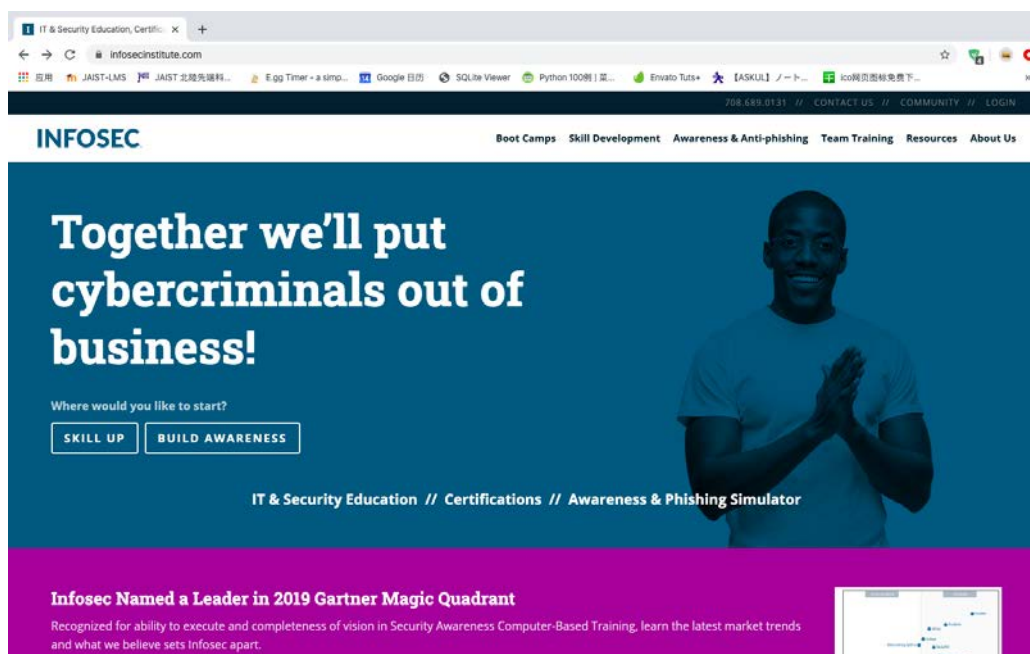


Figure 4.4: The homepage of INFOSEC

Infosec [[infosecinstitute](https://infosecinstitute.com)] believes that knowledge is the most powerful tool in fighting against cybercrime. IT and security professionals careers are advanced with skills development training and a full regimen of certifications. All employees are also empowered with security awareness and training to remain secure at work or home.

Established by smart users wanting to do better, Infosec educates how to defend from cybercrime to entire organizations and equipping everyone with the newest security skills is what Infosec is doing every day so that the good guys win.

Tools to help users outmart the bad guys:

### 1. INFOSEC IQ

With the knowledge and skills to remain cybersecure at work or home empowering users, more than 2,000 security awareness resources and phishing simulations are helped to change users behaviour and culture.

- Infosec IQ content library. Its massive library about role based training resources and industry is updated weekly to help users deliver relevant and fresh training whatever the style they need.

- Security awareness resource center. From here starting security awareness program. Users can download their cybersecurity tips to share with their friends and they can explore Infosec security awareness webinar library.
- Funny situations, real security training. Users will learn to love and connect with the office security through watching and learning as characters and they can still manage to keep themselves in-office behaviors.

## 2. INFOSEC Skills

Keeping users skills updated year-round. Over 50+ security certification studying paths and more than 400 courses are opened to the National Initiative for Cybersecurity Education's Cyberseek model.

When users are growing in their cybersecurity career, Infosec Skills takes the role as the platform to make sure their skills are able to defeat the latest attracts. According to courses are directly mapped to the NICE Cybersecurity Workforce Framework, users can control their career and get ahead of criminals and learn building defenses to future threats.

Cybersecurity roles :

- Cybersecurity specialist / technician
- Cybercrime analyst / investigator
- Incident analyst / responder
- IT auditor
- Cybersecurity analyst
- Cybersecurity consultant
- Penetration and vulnerability tester
- Cybersecurity manager / administrator
- Cybersecurity engineer
- Cybersecurity architect

Featured learning paths

Skill paths:

- Ethical Hacking
- Information Security Fundamentals

- Networking Fundamentals
- Computer Forensics
- Mobile Forensics
- Computer Incident Response
- Web Application Pentesting
- Malware Analysis & Reverse Engineering
- ICS / SCADA Security Fundamentals
- Information Security Auditing

Certification paths :

- $(ISC)^2$  CISSP
- CompTIA Security+
- CompTIA PenTest+
- CompTIA CySA+
- EC-Council Certified Ethical Hacker(CEH)
- Cisco Certified Network Associate R&S(CCNA)
- Project Management Professional(PMP)
- ISACA Certified Information Systems Auditor(CISA)
- ISACA Certified Information Security Manager(CISM)
- Certified Computer Forensics Examiner(CCFE)

Featured courses :

- Security Technologies and Tools
- Threats and Threat Actors
- Common Malware Behavior
- Introduction to Cryptography
- Introduction to Reverse Engineering
- Computer Forensics Investigations
- Digital Evidence and Legal Issues
- Fundamentals of Exploitation
- Post-Exploitation Techniques
- Obfuscation, Encoding and Encryption



### 3. INFOSEC Flex

Designing boot camps for advancing users career to help them pass their first certification exam and guaranteed. Users can take from any location on their favourite.

# Chapter 5

## Advanced Training Systems

If you want to have a deep understanding of cyber security, you can't talk on paper, you need to try and practice. It is only through trial and error that your skills improve substantially.

### 5.1 DVWA

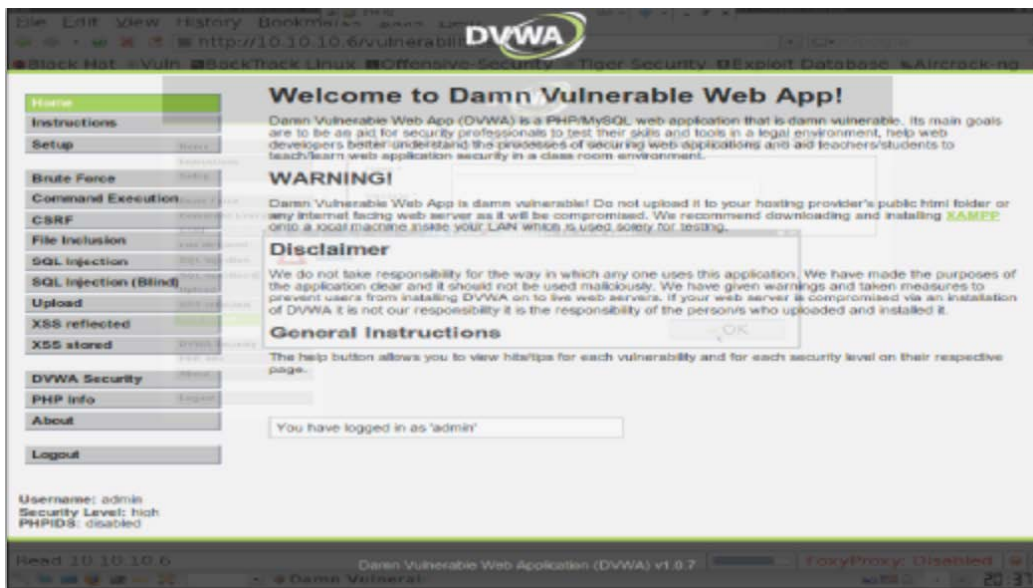


Figure 5.1: The homepage of DVWA

DVWA(Damn Vulnerable Web Application) is a PHP/MySQL web application for security vulnerability identification. It aims to provide a legal envi-

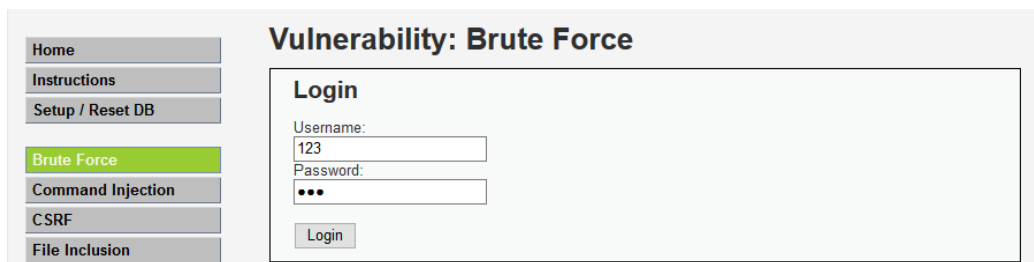
ronment for security professionals to test their professional skills and tools, and help web developers better understand the process of web application security prevention.

DVWA has 10 modules, which are:

### 5.1.1 Brute Force

Brute force cracking generally refers to the exhaustive method. The basic idea of exhaustive method is to determine the approximate range of the answer according to the partial conditions of the question and verify all possible cases one by one within this range until all the cases are verified. If a situation is verified to meet all the conditions of the problem, then is a solution of the problem; There is no solution to the problem if all the conditions are not met after verification. The exhaustive method is also known as enumeration.

1. We first configured the local agent for burp suite
  - Enter your username and password in Login. See Figure 5.2.



The screenshot shows a web application interface for a Brute Force attack. On the left, there is a vertical navigation menu with buttons for 'Home', 'Instructions', 'Setup / Reset DB', 'Brute Force' (which is highlighted in green), 'Command Injection', 'CSRF', and 'File Inclusion'. The main content area is titled 'Vulnerability: Brute Force' and contains a 'Login' form. The form has two input fields: 'Username:' with the value '123' and 'Password:' with masked characters '•••'. Below the input fields is a 'Login' button.

Figure 5.2: Brute Force Login

- Then intercept with burp suite. See Figure 5.3.

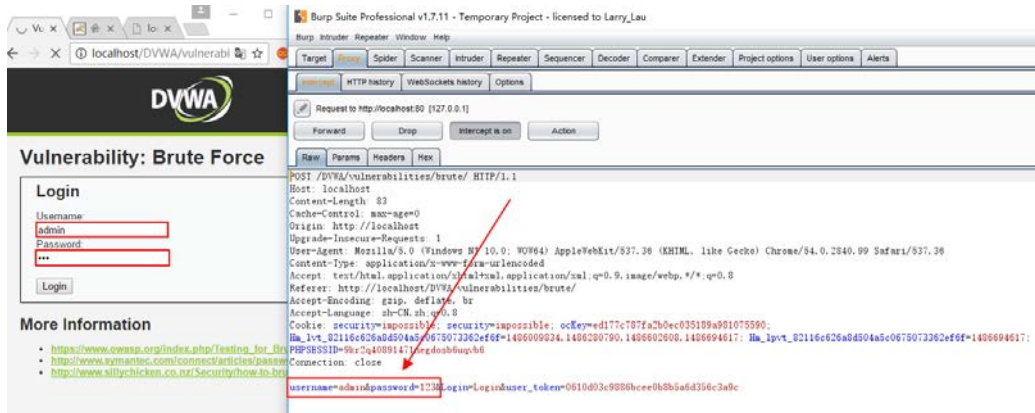


Figure 5.3: Brute Force intercept

2. Submit the form to the intruder module and set the password as the payload cracked
  - Then set the variables which is needed to cracked in the Position option. Burpsuite automatically sets a number of variables. Click the "Clear" button to clear all default variables, select the password 123 and click the "Add" button to set it to the variable need to be cracked. See Figure 5.4.

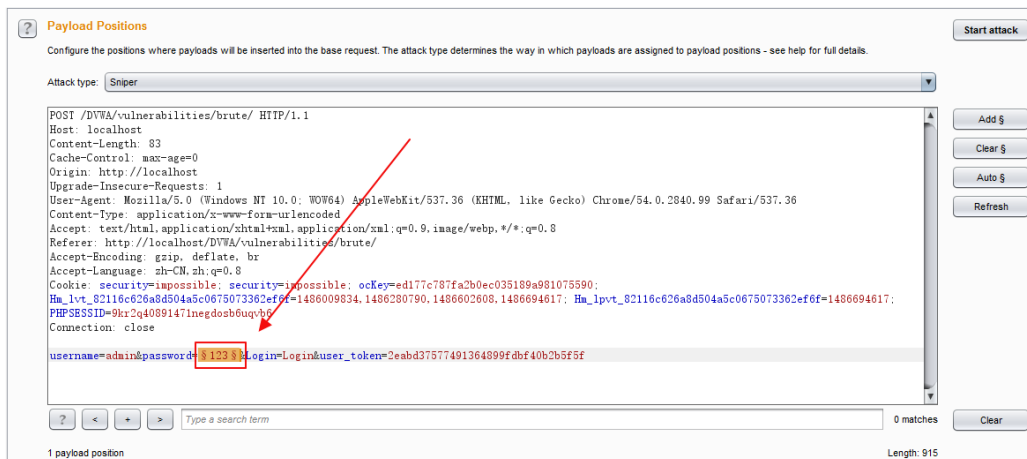


Figure 5.4: Brute Force Position

3. Set dictionary file

- Use built-in dictionary. See Figure 5.5.

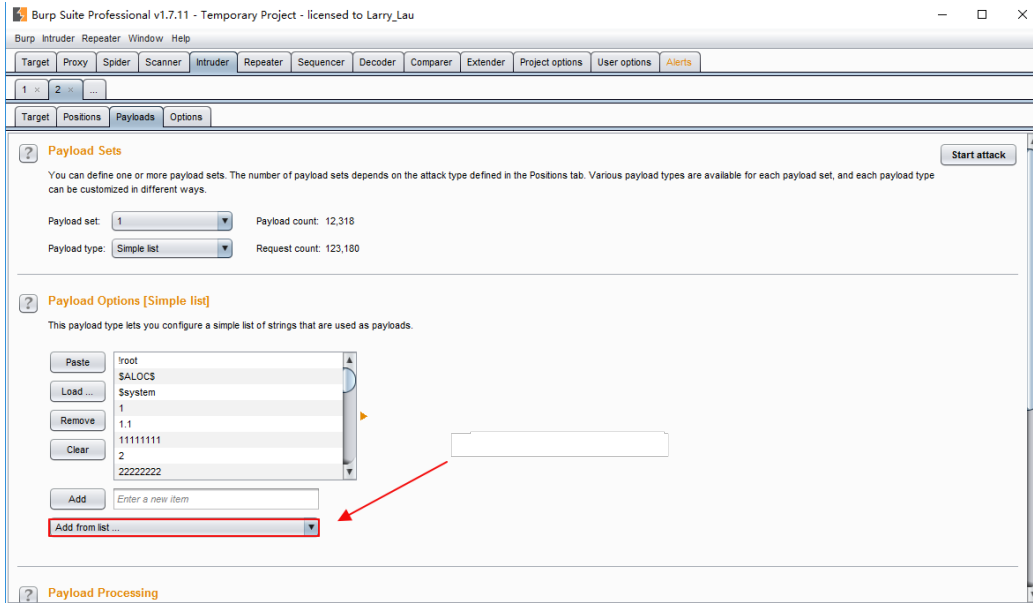


Figure 5.5: Use built-in dictionary

- Load external dictionary. See Figure 5.6.

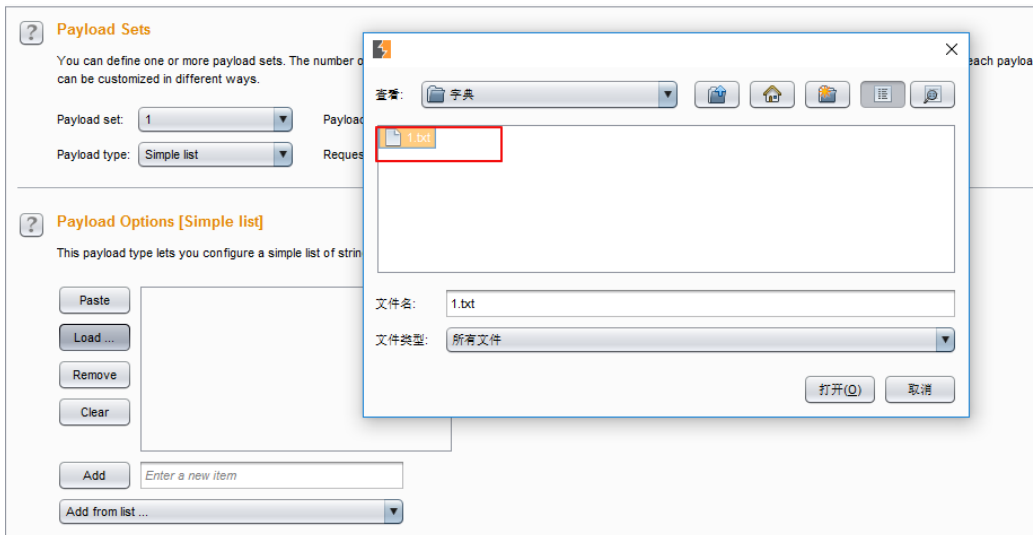


Figure 5.6: Load external dictionary

4. Start the enumeration to get the password.

- Sniper
- Battering ram
- Pitchfork
- Cluster bomb

### 5.1.2 Command Injection

A common pattern of command injection attacks is that when only data is required to enter, malicious code is entered along with the data and the system which loads the data doesn't have a well-designed filtering process. Finally resulting in the execution of the malicious code and information leakage or the destruction of normal data.

#### Low level

As can be seen from the source code, the server directly gets the IP input from the user, splicing the ping command before IP and running it in the shell without any filtering.

Windows and Linux have many command concatenates that spline the commands attackers want to run with previous ping commands, allowing arbitrary code execution.

```
if isset( $_POST[ 'Submit' ] ) then 1
    $target = $_REQUEST[ 'ip' ]; 2
    if striistr( php_uname( 's' ), 'Windows NT' ) then 3
        $cmd = shell_exec( 'ping'. $target ); 4
    else 5
        $cmd = shell_exec( 'ping -c 4'. $target ); 6
    end 7
end 8
```

**Algorithm 1:** Low level

#### Medium level

Compared with Low level source code, only '&&' and ';' two command linker are filtered but the command linker also has '||' and '|', which is unfiltered.

```

if isset( $_POST[ 'Submit' ] ) then                                1
    $target = $_REQUEST[ 'ip' ];                                    2
    $substitutions = array('&&'=' ', ';' = ' ', '|' = ' ', '-' = ' ', 3
        '$' = ' ', '(' = ' ', ')' = ' ', '`' = ' ', '|' = ' ');
    $target = str_replace(array_keys( $substitutions                    4
        ),$substitutions,$target);
    if stristr( php_uname('s', 'Windows NT') ) then                5
        | $cmd = shell_exec('ping'.$target);                        6
    else                                                            7
        | $cmd = shell_exec('ping -c 4'.$target);                    8
    end                                                            9
end                                                                10

```

**Algorithm 2:** Medium level

### High level

If you look at the source code, it looks like all connectors were filtered out but if you're a little more careful, you'll notice that there is a space after the pipe where has a picture description. So you can still use the pipe character for command injection without a space after the pipe character.

```

if isset( $_POST[ 'Submit' ] ) then                                1
    $target = trim(REQUEST[ 'ip' ]);                                2
    $substitutions = array('&&'=' ', ';' = ' ', '|' = ' ', '-' = ' ', 3
        '$' = ' ', '(' = ' ', ')' = ' ', '`' = ' ', '|' = ' ');
    $target = str_replace(array_keys( $substitutions                    4
        ),$substitutions,$target);
    if stristr( php_uname('s', 'Windows NT') ) then                5
        | $cmd = shell_exec('ping'.$target);                        6
    else                                                            7
        | $cmd = shell_exec('ping -c 4'.$target);                    8
    end                                                            9
end                                                                10

```

**Algorithm 3:** High level

### 5.1.3 CSRF(Cross-site request forgery)

Cross-site request forgery is also known as "One Click Attack" or "Session Riding", often abbreviated as CSRF or XSRF. It is a malicious exploitation of a website.

Attackers stealing your identify and sending malicious request in the name of you. For server the request is perfectly legal but it finished the attacker's

expected operation such as sending emails, messages, stealing your account, adding a system administrator or even buying goods in the name of you.

If the spam messages sent by CSRF are accompanied by worm links, those who received harmful messages will also become the dissemination when they open the connection in the private message. Thus thousands of users are stolen information planted Trojan.

CSRF defense:

1. Verification code

Requiring customer in interaction to operate.

2. Referer check

Referer Check one of the most common application is to prevent hotlinking images, by looking at the source of the request to determine whether a request is reasonable, such as embedded from the attacker's web site access blog address, the Referer is an attacker website address, so much can tell this is a CSRF attacks, but the defects of this method is: the server is not to take to the Referer information every time.

3. Construct an unpredictability URL

CSRF can attack successfully, the essence of the reason is that the requested URL is guessed by the attacker, if the requested URL is unpredictable, then the attacker has no way to start. The most common way to do this now is to include a token parameter in the URL. The token can be stored in the user's cookie, and the server also holds the token value for that customer. Because CSRF attacks only use login cookies and cannot obtain the specific values of cookies (unless the user is also attacked by XSS and the cookie is compromised, it is useless).

#### **5.1.4 File Inclusion**

File Inclusion, which means that when the server opens the `allow_url_include` option, it can dynamically include files through some PHP feature functions (`include()`, `require()`, `include_once()`, and `require_once()`) by using urls. At this point, any File reading or arbitrary command execution will result if the File source is not strictly checked. File containing vulnerability is divided into local file containing vulnerability and remote file containing vulnerability, which is caused by the `allow_url_fopen` option in the PHP configuration (after the option is enabled, the server is allowed to include a remote file).



## Low level

Sever-side core code is:

```
$file = $_GET['page']; 1
```

As you can see, the page parameter is not filtered or checked on the server side.

What the server expects the user to do is click on the three links Figure 5.7, the server will contain the appropriate file, and the result will be returned. Need of special note is that the server contains files, regardless of whether file suffix is PHP, will try to perform as a PHP file, if the file content for PHP, for sure will be normal execution and returns the results, if not, will print the file content intact, so the file contain bugs often leads to read arbitrary files with arbitrary command execution.

### Vulnerability: File Inclusion

```
[file1.php] - [file2.php] - [file3.php]
```

Figure 5.7: The three links of File Inclusion

## Medium level

Sever-side core code is:

```
$file = $_GET['page']; 1
$file = str_replace(array("http://", "https://"), "", $file); 2
$file = str_replace(array("../", "..\\"), "", $file); 3
```

As you can see, the medium-level code adds the `str_replace` function and deals with the page parameter taking "Http: //" , "https://", "../" and "..\\" replaced by a null character.

## High level

Sever-side core code is:

```
$file = $_GET['page']; 1
if !fnmatch("file*", $file) && $file != "include.php" then 2
    echo "ERROR: File not found!"; 3
    exit; 4
end 5
```

As you can see, the high-level code uses the `fnmatch` function to check the page parameter, requiring the page parameter to start with a file so that the server will include the corresponding file.

## Impossible

Sever-side core code is:

```
$file = $_GET['page'];
if $file != "include.php" || $file != "file1.php" || $file !=
    "file2.php" || $file != "file3.php" then
    | echo"ERROR: Filenotfound!";
    | exit;
end
```

As you can see, the code at the impossible-level is protected by the white list mechanism which is very simple and rough. The page parameter must be one of "include.php", "file1.php", "file2.php", "file3.php".

### 5.1.5 File Upload

File upload is one way to quickly gain server privileges during penetration testing.

If the developer is not strict in filtering uploaded content, then there will be any vulnerability in file upload. Even if it can not be resolved, it also can hang a black page. If used by fghk, it will cause a very bad impact.

If the uploaded file can also be parsed or if the file contains vulnerabilities, then you can gain access to the server.

## Low level

Sever-side core code is:

```

1  if isset( $_POST[ 'Upload' ] ) then
2      $target_path =
3          DVWA_WEB_PAGE_TO_POOT."hackable/uploads/";
4      $target_path = basename($_FILES['uploaded']['name']);
5      if !move_upload_file($_FILES['uploaded']['tmp_name'], $target_path)
6      then
7          echo '<pre>Your image was not uploaded. </pre> ';
8      else
9          echo '<pre> $target_path successfully uploaded! </pre> ';
10     end
11 end

```

Taking the file, uploading it to hack-able/uploads/ and echoing the path, this is the simplest file upload. Figure 5.8.

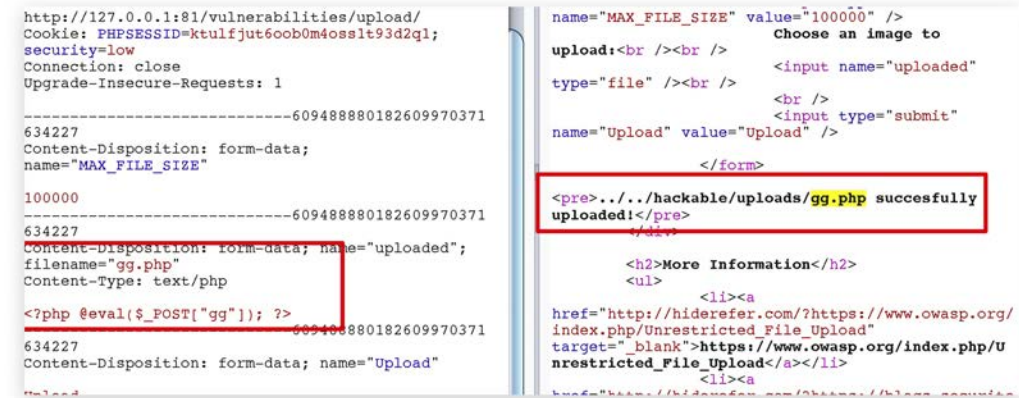


Figure 5.8: File Upload low level

**Medium level**

Sever-side core code is:

```

if isset( $_POST[ 'Upload' ] ) then                                1
|   $target_path =                                                2
|   DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
|   $target_path .= basename($_FILES['uploaded']['name']);        3
|   $uploaded_name = $_FILES['uploaded']['name'];                 4
|   $uploaded_type = $_FILES['uploaded']['type'];                 5
|   $uploaded_size = $_FILES['uploaded']['size'];                 6
|   if ( $uploaded_type == "image/jpeg" ) || ( $uploaded_type ==  7
|       "image/png" ) &&& ( $uploaded_size < 100000 ) then
|   |   if !move_uploaded_file($_FILES['uploaded']['tmp_name'],    8
|       $target_path) then
|   |   |   echo '<pre>Your omage was not uploaded.</pre>';        9
|   |   else                                                       10
|   |   |   echo '<pre>$target_path successfully uploaded! </pre>'; 11
|   |   end                                                       12
|   else                                                           13
|   |   echo '<pre>Your image was not uploaded. We can only accept 14
|       JPEG or PNG images. </pre>';
|   end                                                           15
end                                                               16

```

**Algorithm 4:** Medium level

The point is that the following code restricts the content-type of uploads. You can upload a picture directly and then add a sentence at the end to upload successfully. Figure 5.9

```

$uploaded_type = $_FILES['uploaded']['type'];                      1
$uploaded_type == "image/jpeg" || $uploaded_type == "image/png"; 2

```



```

if isset( $_POST[ 'Upload' ]) then 1
    $target_path = 2
        DVWA_WEB_PAGE_TO_ROOT."hackable/uploads/";
    $target_path .= basename($_FILES['uploaded']['name']); 3
    $uploaded_name = $_FILES['uploaded']['name']; 4
    $target_ext = substr($uploaded_name, strrpos($uploaded_name, 5
        '.' ) + 1);
    $uploaded_tmp = $_FILES['uploaded']['tmp_name']; 6
    $uploaded_size = $_FILES['uploaded']['size']; 7
    if (strtolower($uploaded_ext) == "jpg" )|| 8
        (strtolower($uploaded_ext) == "jpeg" )|| (strtolower($uploaded_ext)
        == "png")9 and ($uploaded_size<100000) then
        if !move_uploaded_file($uploaded_tmp, $target_path) then 9
            | echo '<pre>Your omage was not uploaded.</pre>'; 10
        else 11
            | echo '<pre>$target_path successfully uploaded! </pre>'; 12
        end 13
    else 14
        | echo '<pre>Your image was not uploaded. We can only accept 15
        | JPEG or PNG images. </pre>';
    end 16
end 17

```

**Algorithm 5:** High level

The specific situation is related to the version of PHP and the version of middle ware, which cannot be practiced directly in DVWA.

Upload the picture with the suffix.png and then use the file containing vulnerability to match.

Upload with %00 truncation vulnerability requires PHP version less than 5.3.4.

Resolve vulnerabilities using.htaccess.

## 5.2 OWASP Security Shepherd

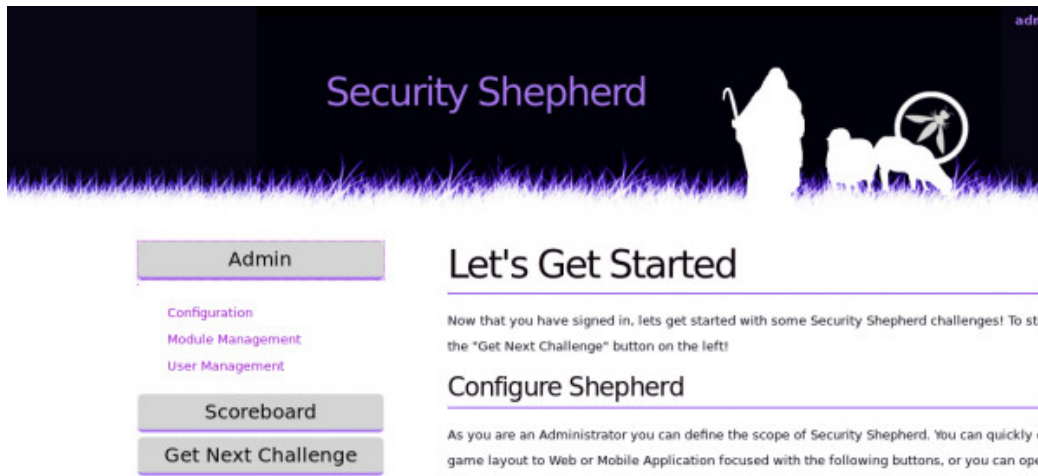


Figure 5.10: The homepage of OWASP Security Shepherd

The OWASP Security Shepherd is a security training platform specialized in web and mobile application. It is aimed at educating and improving security awareness in various skilled demographic. Taking APP Security beginners or experienced engineers and making their penetration testing skill sharper are the OWASP Security Shepherd's goals.

The OWASP Security Shepherd project gives users opportunity to improve their existent manual penetration testing skills. By presenting security risk concepts accomplishes this to users in challenging lessons, which provides users help about a specific security risk and a text version of the issue. Insufficient security mitigation to vulnerabilities are included in challenges.

The OWASP top ten — Injection, Broken Authentication and Session Management, Sensitive Data Exposure, XML External Entity, Broken Access Control, Security Misconfiguration, Cross-Site Scripting, Insecure deserialization, Using Components With Known Vulnerabilities, Insufficient Logging and Monitoring as a challenging test bed. Most security vulnerabilities can be solved and their impact on systems is worked. The necessary skill of this challenge game is by product to make a user's own environment serious among OWASP top ten security risks. The modules provide a challenging chance for security and also for professionals.

So the reasons for why we use Security Shepherd are:

1. Wide Topic Coverage

Security Shepherd covers 70+ levels from the whole spectrum of web to mobile application security in the form of a single project.

2. Gentle Learning Curve

Security Shepherd is a good entry for the user who is new to security field with increasing difficulty.

3. Layman Write Ups

Every security concept is shown using plain language when first acted.

4. Real World Examples

In Security Shepherd, risks are real vulnerabilities. The attack vectors used are how they would act in the real world.

5. Scalability

A single user or a server for a great deal of users can use Security Shepherd locally.

6. Highly Customisable

Admins can set the suitable levels and the way they are presented(Open, CTF and Tournament Layouts).

7. Perfect for Classrooms

Security Shepherd supplies users specific keys in order to stop them sharing their keys.

8. Scoreboard

For encouraging a competitive environment, Security Shepherd adopts a scoreboard.

9. User Management

It's available for Security Shepherd admins to create users, suspend, unsuspend, add bonus points. Students can segmented into specific class by admins.

10. Localisation Support

Even though from a single instance, Security Shepherd material is presented in many languages.



### 11. Robust Service

There are online CTFs such as the OWASP Global CTF and OWASP LATAM Tour CTF 2015 run in Security Shepherd, both of them exceeding 200 users.

### 12. Configurable Feedback

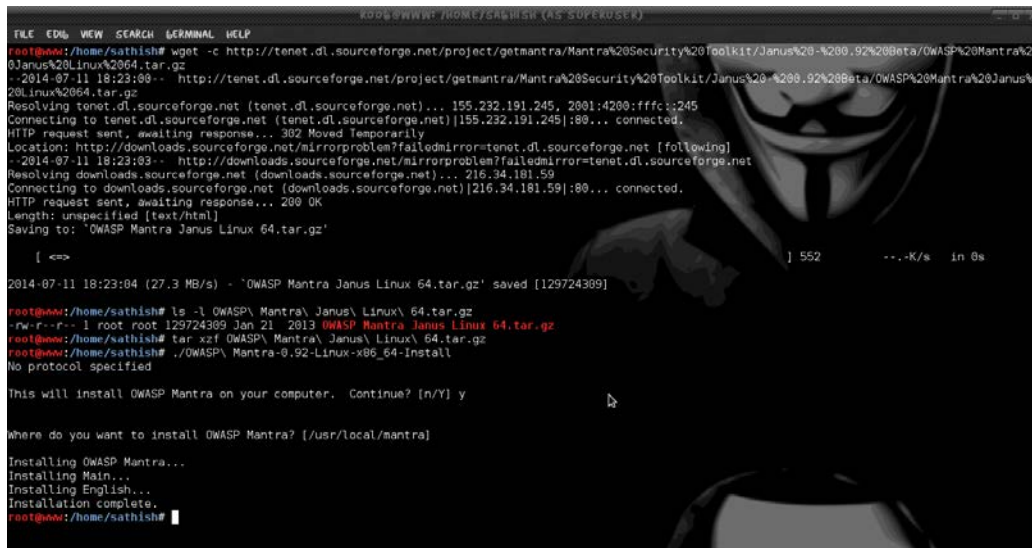
Before a project is marked as complete, an admin can enable a feedback process. This function not only promotes project improvement but for system admins to gather whether understanding or not from their students.

### 13. Granular Logging

The log reports by Security Shepherd is detailed.

The Security Shepherd covers the following security topics about web and mobile application: Lack Of Binary Protections, Client Side Injection, Broken crypto, Poor Authentication and Authorisation, Unintended Data Leakage, Insecure Data Storage, Poor Data Validation, Invalidated Redirects and Forwards, Cross Site Request Forgery, Missing Function Level Access Control, Sensitive Data Exposure, Security Misconfiguration, Insecure Direct Object Reference, Cross Site Scripting, Broken Authentication and Session Management, SQL Injection

## 5.3 OWASP Mantra



```
FILE EDIT VIEW SEARCH BROWSER HELP
root@hws: /home/sathish# wget -c http://tenet.dl.sourceforge.net/project/getmantra/Mantra%20Security%20Toolkit/Janus%20-%200.92%20Beta/OWASP%20Mantra%20Janus%20Linux%2064.tar.gz
--2014-07-11 18:23:00-- http://tenet.dl.sourceforge.net/project/getmantra/Mantra%20Security%20Toolkit/Janus%20-%200.92%20Beta/OWASP%20Mantra%20Janus%20Linux%2064.tar.gz
Resolving tenet.dl.sourceforge.net (tenet.dl.sourceforge.net)... 155.232.191.245, 2001:4200:ffff::245
Connecting to tenet.dl.sourceforge.net (tenet.dl.sourceforge.net)[155.232.191.245]:80... connected.
HTTP request sent, awaiting response... 302 Moved temporarily
Location: http://downloads.sourceforge.net/mirrorproblem?failedmirror=tenet.dl.sourceforge.net [following]
--2014-07-11 18:23:03-- http://downloads.sourceforge.net/mirrorproblem?failedmirror=tenet.dl.sourceforge.net
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 216.34.181.59
Connecting to downloads.sourceforge.net (downloads.sourceforge.net)[216.34.181.59]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'OWASP Mantra Janus Linux 64.tar.gz'

[ <=> ] 552 --.-K/s in 0s

2014-07-11 18:23:04 (27.3 MB/s) - 'OWASP Mantra Janus Linux 64.tar.gz' saved [129724309]

root@hws: /home/sathish# ls -l OWASP\ Mantra\ Janus\ Linux\ 64.tar.gz
-rw-r--r-- 1 root root 129724309 Jan 21 2013 OWASP Mantra Janus Linux 64.tar.gz
root@hws: /home/sathish# tar xzf OWASP\ Mantra\ Janus\ Linux\ 64.tar.gz
root@hws: /home/sathish# ./OWASP\ Mantra-0.92-Linux-x86_64-Install
No protocol specified

This will install OWASP Mantra on your computer. Continue? [n/Y] y

Where do you want to install OWASP Mantra? [/usr/local/mantra]

Installing OWASP Mantra...
Installing Main...
Installing English...
Installation complete.
root@hws: /home/sathish#
```

Figure 5.11: The homepage of OWASP Mantra

Mantra is special browser for web application security test. A large number of people will come to know how easy and flexible being able to take basic testing procedures by this product. Having such a sufficient and effective platform is helpful for the industry development.

Mantra builds many tools to modify headers, input strings, GET/POST requests, edit, switch between proxies, etc. Thus, Mantra can be acted to handle basic levels of different web CTFs.

Abhi M. Balakrishnan and Gokul C. Gopinath started Mantra in October 2010.

OWASP Mantra features:

- Many security and proxy tools
- FireCAT/KromCAT menu structure
- Quick access to tools
- Cookies, cache and proxy management tools
- FTP, SSH, REST and SQLite clients
- Open penetration test bookmarks

- URL operate buttons for changing URL
- Portable version

OWASP Mantra tools:

- Information gathering
- Editors
- Network utilities
- Misc
- Application auditing
- Proxy

## 5.4 GameOver

The objective of GameOver is offering training and education to beginners about the basics of web security and the common web attacks.

GameOver is made up of two sections.

**Section 1** is designed to teach the basics of Web Security covering:

- XSS
- CSRF
- RFI&LFI
- Brute Force Authentication
- Directory/Path traversal
- Command execution
- SQL injection

**Section 2** is gathering insecure web applications, acting as a legal platform in order to test user's skills and exploiting the vulnerabilities to sharpen user's skills before pen-test.

### **System Requirements:**

To run the virtual machine image, it's necessary for users to have a VM Player 4.0.2 or higher. Users need to allocate 265MB or higher RAM in this situation. By any chance if users don't install a VM Player or prefer another virtualization software, they can install the .iso and run it in a 'Live' mode.

### **Getting Started:**

If you chose the Live CD, select 'Live' from the menu and Enter;

Login with the following information:

username: root

password: gameover

### **Web Applications(Section 1):**

1. Damn Vulneable Web Application
2. OWASP WebGoat
3. Ghost
4. Mutillidae
5. Zap-Wave

### **Web Applications(Section 2):**

1. Owasp Hacademic Challenges
2. Owasp Vicnum
3. WackoPicko
4. Owasp Insecure Web App
5. BodgeIT
6. PuzzleMall
7. WAVSEP

## 5.5 Mutillidae



Figure 5.12: The homepage of Mutillidae

Mutillidae is a free, open source web application that allows security enthusiasts to hand-test and hack web applications. It can be installed on Linux, Windows XP, and Windows 7 using XAMPP, making it easy for users who don't want to install or manage their own web servers. It has been installed on Samurai WTF, simply replacing the existing version with the latest Samurai. It contains dozens of bugs and tips to help users take advantage of them; provides an easy-to-use network hacking environment specifically designed to be targeted as a hacker lab for security hobbyists, classroom LABS, and vulnerability assessment tools.

It has been tested/attacked by Cenizic Hailstorm ARC, W3AF, SQLMAP, Samurai WTF, Backtrack, HP Web Inspect, burp-suite, NetSparker Community Edition and other tools. If you want to practice pen testing/cracking web applications by using cross-site scripting, SQL injection, response splitting, HTML injection, javascript injection, clickjacking, cross-framework scripting, form caching, authentication bypassing, or many other vulnerabilities, you can use Mutillidae.

## Features

- There are over 40 vulnerabilities and challenges, containing at least one vulnerability of the OWASP top ten in 2007, 2010, 2013, 2017.
- Actual vulnerability (user is not required to enter "magic" statement).
- It can be installed on Linux or Windows \*AMP stacks for users who don't want to install or manage their own web servers. What is certain is that you will work on XAMPP, WAMP, and LAMP.
- Pre-installed on Rapid7 Metasploitable 2, Samurai Web testing framework (WTF), and OWASP Broken Web Apps (BWA).
- Just click the Settings button and the system can be restored to its default state.
- Users can switch between secure and insecure modes.
- Used in graduate security courses, corporate web SEC training courses, and as "evaluator" targets for vulnerability software.
- Updated frequently.



Figure 5.13: Successful SQL Injection attack

## 5.6 Damn Vulnerable Linux

### Background information

- Damn Vulnerable Linux’s developers spent much time stuffing it with ill-configured, outdated and exploit that makes it easy to attacks.
- Damn Vulnerable Linux is not designed to run on desktop cause it is a learning platform for students who want study security.
- Damn Vulnerable Linux based on the widely enjoyed Linux system Damn Small Linux which has very small size and 2.4 kernel. It makes easier to provide vulnerable stuffs not work under 2.6 kernel.
- It includes old, more breakable version of PHP, MySQL, Apache, SSH and some tools which can assist you compiling, debugging and breaking applications like GCC, GDB, NASM, DDD and so on.

## Prerequisite

Virtualization software is needed to allow to create OS images which uses an ISO or installation CD. However, you can use something popular such as VirtualBox.

## Login to DVL

Credentials (See Below)

- Login: root
- Password: toor

```
Login as "root", with password "toor", both without quotes, lowercase.

After you login, try the following commands:

startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz (KDE)
flux .... to run Xwindow system in VESA mode 1024x768 at 75Hz (FluxBox)
xconf ... to autoconfigure your graphics card for better performance
ati .... to autoconfigure ati drivers (download ati.lzm required)
Other commands you may find useful (for experts only!):

configsave/configrestore ... to save and restore all filesystem changes
fileswap .... to create special file for swapping RAM to your harddisk

When finished, use "poweroff" or "reboot" command and wait until it completes
=====
This distro is based on BackTrack 2.0 Final
=====
bt login:
```

Figure 5.14: DVL Login

## Partition the disk

1. Determine to format which disk. See Figure 5.15.
  - Command: fdisk -l
  - Notice: in this case, the disk is /dev/sda



```
bt ~ # fdisk -l
Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Disk /dev/sda doesn't contain a valid partition table
bt ~ # _
```

Figure 5.15: Determine to format which disk

2. Select disk to be partitioned. See Figure5.16.

- Command: `fdisk /dev/sda`
- Input: `m`

```
bt ~ # fdisk /dev/sda Press Enter
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.

The number of cylinders for this disk is set to 1044.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
(e.g., DOS FDISK, OS/2 FDISK)
Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): m Press Enter
```

Figure 5.16: Select disk to be partitioned

3. View the partition option

- Select "p". See Figure5.17.

```
Command action
a  toggle a bootable flag
b  edit bsd disklabel
c  toggle the dos compatibility flag
d  delete a partition
l  list known partition types
m  print this menu
n  add a new partition
o  create a new empty DOS partition table
p  print the partition table
q  quit without saving changes
s  create a new empty Sun disklabel
t  change a partition's system id
u  change display/entry units
v  verify the partition table
w  write table to disk and exit
x  extra functionality (experts only)

Command (m for help): p_ Press Enter
```

Figure 5.17: View the partition option

4. Add a new partition. See Figure5.18.

- Select "n"
- Select "p"
- Select "l"
- Select 1044

```
Command (m for help): n
Invalid partition number for type `1'
Command action
  e  extended
  p  primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1044, default 1): 1044
```

Figure 5.18: Add a new partition

5. View the created partition. See Figure5.19.

- Select "p"

```
Command (m for help): p
Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		1044	1044	8032+	83	Linux

Figure 5.19: View the created partition

6. Save the new partition

- Select "w". See Figure5.20.

```
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

Figure 5.20: Save the new partition

7. Exit

- Select "q". See Figure5.20.

```
Command (m for help): q
bt ~ #
```

Figure 5.21: Exit

# Chapter 6

## Assessment Criteria and Results

The main objective of assessment is to determine whether they are attaching specific training goals which correct people's security behaviour or not.

The second is to make sure that any changes happening in trainees' capabilities are thanks to the training program/system and not thanks to any other conditions.

The third is to evaluate the training program/system for its cost-effectiveness. Assessment is useful to explain the credibility of training programs/systems. If specific performance can measure the trainees' performance after the training which can be compared with the objectives of the training. If the training objectives have been met then we can say the training is successful.

There are several kinds of assessment criteria: internal, external, participants' reaction and so on. Many experts agree that using multiple criteria to evaluate is more effective. In this report, we combine quiz questions and assessment questionnaire.

### 6.1 General rules for writing survey questions

The suitable question achieves three goals:

1. It measures the potential concept which is intended to tap.
2. It doesn't measure other irrelevant concepts.
3. It points same thing to all participants.

The following rules [16] [19] [23] [24] are useful to accomplish this:

- Avoid technical terms and jargon
 

Every word used in survey questions should be easily grasped meaning for anyone taking the survey.
- Avoid vague or imprecise terms
 

Generally, it would be better to use terms because they will give the same specific meaning to participants. For instance, it is confused what you want to get when you say "Do you think it is important that a candidate shares your values?" If you change the other way to say like "Do you think it is important that a candidate shares your religious values?" You might get a more consistent answer.
- Define things very specifically
 

An example, it prefers asking "What's your income?" rather than ask "What's your total household after taxes per year?"
- Avoid complex sentences
 

Sentences including many clauses or strange constructions usually confuse participants. Requiring participants to make complex calculation is easily causing problems.
- Provide reference frames
 

Ensure all participants are answering questions at the same place and same time. For instance, if you ask someone "How often do you feel happy?" some people might share about their life's experience while some people might only think about today. Generally, it's best to give a reference frame "How often do you feel happy during the past year?"
- Make sure scales are ordinal
 

When using a rating scale, make each point clear suitable for all people such as "How many hotels are available in your town: A lot, some, only a few, or none at all."
- Avoid double-barreled questions
 

Questions should focus on one thing. Two things or more might be measured in double-barreled questions.
- Answer choices should anticipate all possibilities
 

It's best to provide multiple choices in case a participant has more than one answer to a question. If the choices you provided do not anticipate all possibilities, it will need to prepare another specify choices.

- If you want a single answer, make sure your answer choices are unique and include all possible responses

Putting your categories as a range when you measure something pointing to a continuum. For example: Where should this pig put: No place, Five years in the zoo, Ten years in the zoo, Twenty years in the zoo, Life in the zoo, or Death. A better scale might be like: Where should this pig put: No place, Up to five years in the zoo, From five years to ten years in the zoo, From ten years to twenty years in the zoo, More than twenty years but less than life in the zoo, Life in the zoo, or Death.

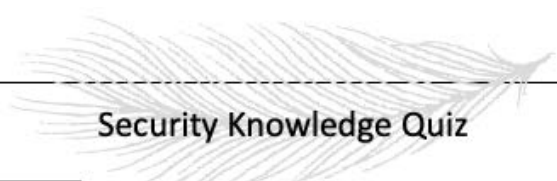
- Avoid questions using leading, emotional, or evocative language

## **6.2 Questionnaire in survey**

### **6.2.1 Part 1: Security Knowledge Quiz**

When participants fill in the part of assessment criteria, they need to finish the 8 security knowledge quiz questions before.

We extract quiz questions from ECSM [4]. Question 1-6 are carried from Level 1(starter) and Question 7-8 are carried from Level 2(advanced). But we don't require participants to know which question is which level because we don't want to give them unnecessary stress.



---

## Security Knowledge Quiz

Your name: \_\_\_\_\_

Before the assessment of security awareness training programs/systems, we want you to do the 8-question quiz below to test your knowledge on security. The quiz will take maximum 10 minutes and we hope you'll enjoy the it. Good luck!

### **Question 1**

Passwords are strings of characters used to access online services, such as your email or social networks profile. They are mainly meant to help prevent other people from accessing your personal accounts. Unfortunately, because we use so many services, it is difficult to remember each password that we have.

**In this situation, what could be a good strategy?**

- I save all my different passwords in a file: when I need one, I can easily retrieve it.
  - I still prefer to use a different password each time by employing a password manager.
  - I use the same password for each service that I use.
- 

### **Question 2**

While opening the email, you got an interesting but suspicious message from a company. The message said that "you've won the lottery" and the company was asking you specific personal and banking details so that they could lodge a large sum of money in your bank account.

**These emails are a common type of cyber-attack that goes by the name of...**

- Phishing
  - Spyware
  - Spoofing
- 

### **Question 3**

How many times a week do you read an article on cyber security and hacking?  
Although both are popular buzzwords they are also of paramount importance in our daily life at work or during our spare time.

**Generally, who are hackers?**

- They are benign computer experts.
  - They are malicious computer criminals.
  - Hackers could be both benign computer experts and malicious computer criminals.
- 

### **Question 4**

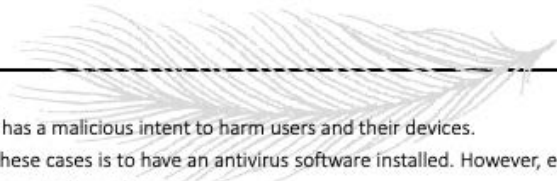
One day you were listening to the evening news while preparing your dinner at home. On the TV show the journalist was interviewing a computer industry expert talking about the importance of regularly updating and **patching computer operating systems** for security reasons. However you were distracted by cooking and could not understand why he was insisting on that.

**When thinking about it the day after, you think that patching the operating system...**

- Fixes problems and makes the operating system more secure.
  - Allows you to continue using your software without paying.
  - Improves the working functions of my operating system.
- 

Figure 6.1: Security Knowledge Quiz

---



### **Question 5**

Malware is software that has a malicious intent to harm users and their devices.

A relevant protection in these cases is to have an antivirus software installed. However, even this is not sufficient as the antivirus needs to be constantly updated.

**What is your perspective about the need for updating the antivirus?**

- Updating of my antivirus should be performed only if I don't regularly patch my operating system.
  - The antivirus update protects my computer from newly created malware.
  - The antivirus updates ensure the correct performance of my computer.
- 

### **Question 6**

One day on the evening news you heard the presenter talking about the Internet threat called 'botnets'.

Despite this name looking like something coming from a science fiction book, this is a serious problem for many users.

**How can botnets affect you?**

- Botnets are a form of malicious software.
  - Someone could take control of my computer and use it for illegal activities, whilst I am not aware that my system has been compromised.
  - I might not be able to use an on-line service if it is affected by a botnet.
- 

### **Question 7**

Cookies are small information items (text files) stored in users' PCs and used widely by online service providers for several purposes, such as to capture user preferences (language, background colors, etc.), to identify the user when he/she uses a shopping list etc. By these means, cookies have indeed positive functions (e.g. they help avoiding the need to repeatedly have to identify yourself).

**However cookies also raise some security and privacy concerns, for example...**

- They could contain a virus which then infects my computer.
  - The collection of data stored in my device.
  - The collection of personal data as well as the risk that someone could impersonate me.
- 

### **Question 8**

When you travel for work you often need to use open Wi-Fi networks, e.g. at train stations or coffee shops.

However, you are aware that there might be dangers with such open networks.

**In order to protect your communication over these public networks you always...**

- Use the private browsing function of your browser.
- Use a Virtual Private Network or VPN.
- Turn off your device's file sharing function.

Figure 6.2: Security Knowledge Quiz



## 6.2.2 Part 2: Assessment criteria

### Basis 1

Masha Sedova, an industry recognized security expert, speaker and trainer focus on engaging people to be key elements of secure organizations. She proposes 8 criteria [22] to let us learn how to select a solution which is right for evaluating a program. The following table we will show her criteria and our choice for close-end questions.

No.	Criteria	Our choice
1	Define the impact of training.	×
2	Is the content engaging ?	✓
3	Is it optimized for learning and retention of content ?	✓
4	Can the training be customized for various groups and use cases ?	×
5	Is the training respectful of employees' intelligence ?	✓
6	Is the training actionable ?	✓
7	Does the training Make You Look Good ?	×
8	Does it address real security threats ?	✓

Table 6.1: Masha Sedova's opinions and our choice

We don't choose criterion 1 because it is mainly about what you need to prepare before evaluating any program.

We choose criterion 2 because engaging content makes trainees to be motivated.

We might choose criterion 3 because it's important for trainees keeping a good memory after learning.

We don't choose criterion 4 as close-end questions because it belongs to improvement.

We might choose criterion 5 because training content should be suitable for trainees.

We might choose criterion 6 because implementing quickly and easily is a factor for a successful training program.

We don't choose criterion 7 because it is about branding and advertising.

We choose criterion 8 because this is one goal of the training.

### Basis 2

Donald Kirkpatrick, former university of Wisconsin professor emeritus, first published his model in 1959. He updated them in 1975 and published his most famous module, "Evaluating Training Programs" , in 1993[20] . The following table we will show his criteria and our choice for close-end questions

In his Level 1: Reaction, questions to trainees include:

No.	Criteria	Our choice
1	Did you feel that the training was worth your time ?	×
2	Did you think that it was successful ?	×
3	What were the biggest strengths and weaknesses of the training ?	×
4	Did you like the venue and presentation style ?	✓
5	Did the training session accommodate your personal learning styles ?	✓
6	Were the training activities engaging ?	✓
7	What are the three most important things that you learned from this training ?	×
8	From what you learned, what do you plan to apply in your job ?	×
9	What support might you need to apply what you learned ?	×

Table 6.2: Donald Kirkpatrick's opinions and our choice

We don't choose criterion 1, criterion 2, criterion 3 and criterion 7 as close-end questions because we want to excavate potential information from participants the reason why this training is successful.

We choose criterion 4 because venue and presentation are affected for trainees' experience.

We choose criterion 5 because training content should be suitable for trainees.

We choose criterion 6 because engaging content makes trainees to be motivated.

We don't choose criterion 8 and criterion 9 as close-end questions because it aims at getting trainees' advice for improvement.

### Basis 3

Jonathan Deller, in his mind [17] , each question should be clear so that trainees know how to deal with each answer. The following table we will show his criteria and our choice for close-end questions.

No.	Criteria	Our choice
1	Did the training content meet your expectations ?	✓
2	Was the size of your training group appropriate ?	×
3	How would you rate the quality of the training ?	×
4	Was the mix of presentations and activities suitable ?	×
5	How would you rate the quality of the instructor ?	×
6	Did you learn anything new ?	✓
7	Was the training relevant to your needs ?	✓
8	Was the course practical and/or easy to apply ?	✓
9	Would participants recommend the training to colleagues ?	×
10	Do you have any suggestions to improve this course ?	×

Table 6.3: Jonathan Deller's opinions and our choice

We choose criterion 1 because it identifies whether the training content matched the trainees' expectations or not.

We don't choose criterion 2 because what we conduct is individual training not group training.

We might not choose criterion 3 and criterion 4 as close-end questions because it seems belong to improvement.

We don't choose criterion 5 because we want to evaluate towards the training itself.

We choose criterion 6 because it makes trainees feel valuable.

We choose criterion 7 because training content should be suitable for trainees.

We choose criterion 8 because implementing quickly and easily is a factor for a successful training program.

We don't choose criterion 9 and criterion 10 as close-end questions because it aims at getting trainees' advice for improvement.

### Actual questions

From the above three experts' ideas, some ideas are similar to another ideas, therefore we summarize them and gain the following 9 close-end assessment questions & 3 open-end assessment questions.

## Assessment of Security Awareness Training Programs/Systems

Training program/system name: \_\_\_\_\_

Thank you for answering the security knowledge quiz. Next is a list of statements for you to use for assessing security awareness training programs/systems, so that we can determine how to improve security awareness training.

The assessment form should take you approximately 15 minutes to complete for each program or system that you will evaluate.

////////////////////////////////////  
 Please rate the statements below referring to aspects such as the training platform, training content and training outcome.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1 The training platform was suitable for learning.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2 The training platform has a clear user interface.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3 You noticed problems with the training platform (dead links, etc.).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4 The training content is sufficiently in-depth.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5 You enjoyed the gamification features in the training (choose the "Neutral" if there were not any).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6 The training content addresses real security threats.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7 You felt that the training was engaging.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8 You felt that your knowledge/skills improved by taking the training.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9 The training was practical and/or easy to apply.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

////////////////////////////////////  
 Please provide additional feedback by answering the three questions below.

① What are the three most important things that you learned?

---

② What were the biggest strengths and weaknesses of the training?

---

③ Do you have any suggestions for improving this training program/system?

---

Figure 6.3: Assessment Criteria

## 6.3 Likert Scale question

Likert scale is a psychological response scale, which is often used in questionnaire and most widely used in survey research. When participants answered the questions, they specify how much they agree with the statement. This scale was established by Lencis Likert.

### 6.3.1 Use Likert's five choices in the sample questions

It is important to clarify the difference between Likert Scale and a Likert item. [18]

Likert Scale is a generic term for using a variety of Likert items. Because Likert items are often a visual scale(for example, a horizontal line on a question that subjects answer in circles or by clicking) and sometimes these items are called scales. However, that is easy to cause confusion. Therefore, the good idea is that Likert items refer to a single item.

A Likert item is a statement. The participant is asked to indicate how much he/her agree with the statement or any form of subjective and objective assessment. Five response levels are usually used but many psychometricians advocate seven-point or nine-point.

**Table 4. Mean Quality, Reliability, and Validity by Number of Response Categories.**

No. of Points	Mean $q^2$	Mean $r^2$	Mean $v^2$
5	0.533	0.717	0.753
7	0.394	0.716	0.555
11	0.383	0.709	0.531

Figure 6.4: The almost identical reliability of 5-7-11-point scales

A recent empirical study [21] has shown that the mean, variance, skewness and kurtosis of data for 5-point, 7-point, 11-point are similar after simple data transformations. See Figure 6.4.

Likert five items:

1. Strongly Disagree
2. Disagree
3. Neutral(Neither agree nor object)

4. Agree

5. Strongly Agree

Likert Scale has two extreme quantitative methods for measuring positive or negative responses to a statement. When the intermediate item "Neutral" is not available, a four-point rating scale(a method of forced selection) is sometimes used. Likert Scale may be distorted by several factors. Participants may avoid checking extreme items(bias toward the middle) and this is habitual acceptance of statements(inertia bias) or try to figure out and match the outcome themselves or their organization wants(social approval bias).

### 6.3.2 Scoring and analysis

After the questionnaire is completed, each item may be individually analyzed or some groups of items may be summed up to form a scale. Therefore, Likert Scale is often called summative scale.

As for the individual Likert items, they can be treated as interval data or only be treated as sequential data, that is a contentious issue. Many people think such items as data of sequential data especially when only five levels are used, there is no way for the participants to perceive that the adjacent items are equidistant. On the other hand, usually(as in the example above) the wording of their response levels clearly implies the symmetry of the middle category of response levels. At a minimum, such a project would become somewhere between order and interval scale. In addition, if the item is accompanied by a visual analog scale, the gap in the degree of response clearly indicates that the argument is stronger as an interval data.

When regarded as sequential data, Likert data can be arranged as bar charts to show central tendency in median or mode(but not mean), or dispersion in quartile(but not standard deviation), or analysis by nonparametric tests such as the chi-square test, the man-whitney test, the wilkerson test, or the kraska-wallis test.

Data from several Likert questions may be aggregated and if all questions use the same Likert Scale, the scale effectively approximates the interval scale which can be considered as interval data to measure potential variables. If the sums satisfy these assumptions, they can be tested by parametric statistics such as anova but only the items are more than five.

Data obtained by Likert Scale sometimes combine all the responses of agree and disagree into the categories of "accept" and "don't accept" which becomes nominal scales. Chi-square test, cochran's theorem, or myne's test are all commonly used statistical methods after these data transformed.

### 6.3.3 Scale of measurement

The five Scale items are often referred to interval measure variables. However, if the interval at each point of scale is consistent with the empirical observation in metric sense, this is an individual case. In fact, it's possible to have sequential scales.

## 6.4 Consensus Based Assessment (CBA)

Consensus Based Assessment, which extends the theoretical observation that expertise can be approached by a large number of novices or skilled workers. Shared knowledge which forms cultural consensus can be interpreted as expertise. According to this, if individual samples of different abilities rate a related scenario, they will provide similar averages for each project. Therefore, from the perspective of the CBA framework, the key cultural criteria for scoring can be obtained from the same people being evaluated.

For many performance domains, expertise reflects knowledge derived from experience is one way to understand this expectation. Because novices tend to be less experienced, their opinions can go wrong in different directions and the errors may not be very consistent. However, with the accumulation of experience, the opinions of experts and even skilled workers will become more and more consistent. According to this view, the error is random. The score data collected from a large number of respondents whose knowledge and skills cover a wide range of expertise can be used to approximate the score. Since the standard deviation of the mean will approach to zero, when the observed value  $N$  becomes very large, estimates based on different capability groups will provide convergent estimates of the maximum performance. These groups responses can be used to create effective scoring rules to evaluate performance. This method is particularly applicable to the use of Likert response scale to score the subjective domain of knowledge which has been applied to development of criteria for several fields lacking experts.

CBA is calculated by using the Pearson  $R$  correlation between the Likert Scale of each person in a set of items and the mean value of all persons' judgements of the same items. This correlation is a measure of how close a person is to consensus. It is also sometimes calculated as a standardized deviation score from the group consensus average. The two processes are mathematically isomorphic. If culture is thought as Shared Knowledge, the mean score of a group for a particular knowledge area is considered as a measure of cultural consensus in that area. Both of them use CBA as a measure of someone's understanding.

### 6.4.1 Consensus and Dissention

We believe that consensus and dissention [25] are distinct concepts. A consensus is a group of people as a whole reached an opinion or position. Dissention is defined as a difference of an opinion like conflicts arise within the group which makes the decision. Consensus is also defined as complement to dissention.

In studying the various meaning of consensus, it is clear that there is plenty of contents in a modest Internet search, generating 6.6m hits. When we begin to investigate the consensus, the repetition and variation of the word "consensus" leads us to a place that provides a fairly complete definition of consensus.

### 6.4.2 Issues in consensus

Consensus has two common meanings. The first is a general consensus among group members or community members. The second is to reach such a consensus as a theory and practice. Many discussions focus on the need for consensus and even dictionaries have different definitions of consensus. This discussions deviate from the point of consensus which is not a voting system but taking everyone's opinion seriously. In the consensus, those who want to take some action want to hear from those who oppose it because they do not want to impose it and they believe that the following dialogue will benefit everyone.

### 6.4.3 Rules for consensus

Consensus is the collective feeling of a group about an issue. This feeling can be measured by Likert Scale to know how much a person agrees or disagrees with a question.

For instance

*The software is easy to download...*

1. Strongly Disagree
2. Disagree
3. Neutral
4. Agree
5. Strongly Agree



We have established a set of rules and before any measure can be considered as a solution to Likert Scale consensus problem, the following rules should be satisfied.

1. For a given (even numbers) individuals involved in discussing an issue of interest, if an equal number of individuals divide themselves into two groups ( $n/2$ ), each focusing on the categories of Strongly Disagree and Strongly Agree. Therefore, the group is considered to have no consensus.
2. Regardless of the category, if all participants placed themselves in the same category on the Likert Scale, the consensus of the group is complete.
3. If assign the mix of participants ( $n/2+1$ ) to any of categories, the degree of consensus must be greater than 0 because in the extreme, the intra-group balance is no longer equal.

#### 6.4.4 Calculation for Cns

We assign ordinal values to these categories

- Strongly Disagree = 1
- Disagree = 2
- Neutral = 3
- Agree = 4
- Strongly Agree = 5

Let us assume the numbers of people in each category

- Strongly Disagree 25
- Disagree 16
- Neutral 22
- Agree 23
- Strongly Agree 14

The mean is:

$$\mu_X = \sum_{i=1}^n p_i X_i = \frac{25}{100} \times 1 + \frac{16}{100} \times 2 + \frac{22}{100} \times 3 + \frac{23}{100} \times 4 + \frac{14}{100} \times 5 = 2.85 \quad (6.1)$$

The Shannon entropy is:

$$Ent(X) = - \sum_{i=1}^n p_i \log_2(p_i) \quad (6.2)$$

$$= - \frac{25}{100} \log_2\left(\frac{25}{100}\right) - \frac{16}{100} \log_2\left(\frac{16}{100}\right) - \frac{22}{100} \log_2\left(\frac{22}{100}\right) \quad (6.3)$$

$$- \frac{23}{100} \log_2\left(\frac{23}{100}\right) - \frac{14}{100} \log_2\left(\frac{14}{100}\right) \quad (6.4)$$

$$= 2.29 \quad (6.5)$$

William J. Tastle et.al. [25] define the consensus to be:

$$Cns(X) = 1 + \sum_{i=1}^n p_i \log_2 \left( 1 - \frac{|X_i - \mu_X|}{d_X} \right) \quad (6.6)$$

We calculate the Consensus as:

$$Cns(X) = 1 + \frac{25}{100} \log_2 \left( 1 - \frac{|1 - 2.85|}{5 - 1} \right) + \frac{16}{100} \log_2 \left( 1 - \frac{|2 - 2.85|}{5 - 1} \right) \quad (6.7)$$

$$+ \frac{22}{100} \log_2 \left( 1 - \frac{|3 - 2.85|}{5 - 1} \right) + \frac{23}{100} \log_2 \left( 1 - \frac{|4 - 2.85|}{5 - 1} \right) \quad (6.8)$$

$$+ \frac{14}{100} \log_2 \left( 1 - \frac{|5 - 2.85|}{5 - 1} \right) \quad (6.9)$$

$$= 0.44 \quad (6.10)$$

### 6.4.5 The measure of consensus and the rules

We see the Cns for each row in Table 6.4, 50% SD(Strongly Disagree) and 50% SA(Strongly Agree) is 0. The number of participants in the group has no effect on the value of consensus and Rule 1 in Section 6.3.3 is satisfied. Notice that the last row in table 6.4 shows one participant's transition from SD(Strongly Disagree) to SA(Strongly Agree). This change tips the scales

slightly towards the SD(Strongly Disagree) side, resulting in a slight increase in the degree of consensus. This is Rule 2 of Section 6.3.3.

SD	D	N	A	SA	Cns
5	0	0	0	5	0
50	0	0	0	50	0
500	0	0	0	500	0
5000	0	0	0	5000	0
51	0	0	0	49	0.0003

Table 6.4: Lacking consensus data

Table 6.5 shows the movement from total opposition to full agreement. Note that the last row represents the total number of members of all groups.

SD	D	N	A	SA	Cns
5	0	0	0	5	0
50	0	0	5	0	0.30
5	0	5	0	0	0.51
5	5	0	0	0	0.81
10	0	0	0	0	1

Table 6.5: The movement towards a single category

See Table 6.6, as the number of participants increasing, consensus measure shouldn't be affected. Whatever the number of participants, in each category the proportion of participants is constant and the consensus measure remains unchanged.

SD	D	N	A	SA	Cns
0	1	0	3	0	0.57
0	10	0	30	0	0.57
0	20	0	60	0	0.57
0	30	0	90	0	0.57
0	300	0	900	0	0.57

Table 6.6

## 6.5 Results

### 6.5.1 How to determine participants

#### Step 1

In the previous Security Knowledge Quiz test, we invite 24 participants to do 8 quiz questions.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	correct rate
Pa	✓	✓	✓	✓	✓	✓	✓	×	7/8
Pb	✓	✓	✓	✓	✓	✓	✓	✓	1
Pc	×	✓	×	✓	✓	✓	✓	×	5/8
Pd	✓	✓	✓	✓	✓	✓	✓	×	7/8
Pe	✓	✓	✓	✓	✓	✓	✓	×	7/8
Pf	✓	✓	✓	✓	✓	✓	✓	×	7/8
Pg	×	✓	×	✓	✓	✓	✓	×	5/8
Ph	×	✓	×	✓	✓	✓	✓	×	5/8
Pi	✓	✓	✓	✓	✓	✓	✓	✓	1
Pj	✓	✓	✓	✓	✓	✓	✓	✓	1
Pk	✓	✓	✓	✓	✓	✓	✓	×	7/8
Pl	×	✓	×	✓	✓	✓	✓	×	5/8
Pm	✓	✓	✓	✓	✓	✓	✓	×	7/8
Pn	×	✓	×	✓	✓	✓	✓	×	5/8
Po	✓	✓	✓	✓	✓	✓	✓	×	7/8
Pp	×	✓	×	✓	✓	✓	✓	×	5/8
Pq	✓	✓	✓	✓	✓	✓	✓	✓	1
Pr	✓	✓	✓	✓	✓	✓	✓	×	7/8
Ps	✓	✓	✓	✓	✓	✓	✓	✓	1
Pt	✓	✓	✓	✓	✓	✓	✓	✓	1
Pu	×	✓	×	✓	✓	✓	✓	×	5/8
Pv	✓	✓	✓	✓	✓	✓	✓	✓	1
Pw	✓	✓	✓	✓	✓	✓	✓	✓	1
Px	×	✓	×	✓	✓	✓	✓	×	5/8

Table 6.7: Security Knowledge Quiz results of the 24 participants

#### Step 2

From the Table 6.7, we can see the correct rates are focus on 5/8, 7/8 and 1 those three kinds. And the number of evaluating training programs is not less, therefore we select each two participants from each kind of correct rates to

do the training programs assessment by Dice(writing each two participants' name with correct rate 5/8, 7/8, 1 in the broken paper then throw the papers and chose one).

### 6.5.2 How to determine which training programs to assess

When the training program which is not satisfied with the second item and the third item in our Assessment of Security Awareness Training Programs/Systems, it will be kicked out.

### 6.5.3 Outcome

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	A	SA	A	A	A	SA	4.33	0.92	0.83
A2	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A3	SD	D	SD	SD	SD	SD	1.17	0.65	0.89
A4	SA	A	A	SA	SA	SA	4.67	0.92	0.83
A5	D	N	D	N	N	N	2.67	0.92	0.83
A6	SA	A	A	SA	A	A	4.33	0.92	0.83
A7	A	SA	A	A	A	SA	4.33	0.92	0.83
A8	A	A	SA	SA	SA	A	4.50	1.00	0.81
A9	SA	SA	SA	A	SA	A	4.67	0.92	0.83

Table 6.8: The results of Proprofs

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	A	SA	A	A	SA	A	4.33	0.92	0.83
A2	A	A	SA	A	A	SA	4.33	0.92	0.83
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	A	A	SA	A	A	A	4.17	0.65	0.89
A5	N	A	N	D	A	N	3.17	1.46	0.77
A6	SA	SA	SA	SA	A	A	4.67	0.92	0.83
A7	A	A	A	A	SA	SA	4.33	0.92	0.83
A8	A	SA	A	SA	A	A	4.33	0.92	0.83
A9	A	A	A	A	A	A	4.00	0.00	1.00

Table 6.9: The results of DARK Reading

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	A	A	SA	SA	SA	SA	4.67	0.92	0.83
A2	SA	N	A	SA	A	SA	4.33	1.46	0.73
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	A	A	SA	A	A	A	4.17	0.65	0.89
A5	A	N	N	SA	A	A	3.83	1.46	0.77
A6	A	A	SA	A	A	A	4.17	0.65	0.89
A7	A	A	A	A	SA	A	4.17	0.65	0.89
A8	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A9	SA	A	A	SA	SA	SA	4.67	0.92	0.83

Table 6.10: The results of Marshal Security

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	A	SA	SA	A	A	SA	4.50	1.00	0.81
A2	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	A	A	A	SA	SA	A	4.33	0.92	0.83
A5	N	N	N	N	N	N	3.00	0.00	1.00
A6	A	SA	SA	A	SA	A	4.50	1.00	0.81
A7	N	A	N	A	SA	A	3.83	1.46	0.77
A8	A	N	SA	A	SA	SA	4.33	1.46	0.73
A9	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00

Table 6.11: The results of Lynda.com

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A2	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	D	D	A	A	N	A	3.17	1.46	0.66
A5	A	A	A	A	SA	A	4.17	0.65	0.89
A6	D	N	A	A	A	N	3.33	1.46	0.73
A7	SA	SA	SA	SA	A	A	4.67	0.92	0.83
A8	D	D	D	A	A	N	2.83	1.46	0.66
A9	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00

Table 6.12: The results of Khan Academy

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	A	A	A	A	A	A	4.00	0.00	1.00
A2	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	A	A	N	N	SA	A	3.83	1.46	0.77
A5	A	A	A	A	N	N	3.67	0.92	0.83
A6	A	A	SA	A	SA	SA	4.60	1.00	0.81
A7	A	A	A	N	A	A	3.83	0.65	0.89
A8	A	A	SA	SA	SA	A	4.60	1.00	0.81
A9	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00

Table 6.13: The results of Udemy

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	A	A	N	A	SA	SA	4.17	1.46	0.77
A2	SA	SA	SA	A	A	A	4.60	1.00	0.81
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	N	A	SA	A	N	SA	4.00	1.58	0.72
A5	A	A	A	N	A	N	3.67	0.92	0.83
A6	SA	A	SA	A	A	A	4.33	0.92	0.83
A7	N	N	N	A	A	A	3.50	1.00	0.81
A8	A	A	A	SA	SA	A	4.33	0.92	0.83
A9	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00

Table 6.14: The results of SCIAC

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A2	SA	SA	SA	SA	A	SA	4.83	0.65	0.89
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A5	SA	SA	SA	SA	A	SA	4.83	0.65	0.89
A6	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A7	A	A	SA	SA	SA	SA	4.67	0.92	0.83
A8	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A9	SA	SA	A	A	A	N	4.17	1.46	0.77

Table 6.15: The results of DVWA

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A2	A	A	A	A	A	A	4.00	0.00	1.00
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	A	A	A	SA	A	A	4.17	0.65	0.89
A5	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A6	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A7	N	A	SA	A	A	A	4.00	1.25	0.86
A8	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A9	SA	A	N	N	SA	N	3.83	1.46	0.66

Table 6.16: The results of Security Shepherd

	P1	P2	P3	P4	P5	P6	mean	Shannon entropy	Cns
A1	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A2	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A3	SD	SD	SD	SD	SD	SD	1.00	0.00	1.00
A4	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A5	SA	A	A	SA	SA	SA	4.67	0.92	0.83
A6	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A7	SA	SA	SA	SA	SA	SA	5.00	0.00	1.00
A8	SA	SA	A	A	SA	A	4.50	1.00	0.81
A9	SA	SA	SA	A	A	D	4.17	1.46	0.62

Table 6.17: The results of GameOver

#### 6.5.4 The state of each training programs/systems

According to the section 6.5.3, we pick up the worst one in each assessment criterion in the following table and consider out some improvements referring to suggestions from participants.



Category	Program name	A1*	A2	A3	A4	A5	A6	A7	A8	A9
E-learning Training Program	Proprofs	↑**		↑		↑				↑
	Marshal Security DARKReading	↑	↑		↑		↑	↑		
Video Training Program	Khan Academy				↑		↑		↑	
	Lynda.com					↑				
	Udemy CSIAC	↑	↑					↑		
Advanced Training System	DVWA Security Shepherd GameOver		↑		↑	↑		↑	↑	↑

- \* A1: The training platform was suitable for learning.  
A2: The training platform has a clear user interface.  
A3: You noticed problems with the training platform (dead links, etc.).  
A4: The training content is sufficiently in-depth.  
A5: You enjoyed the gamification features in the training (choose the “Neutral” if there were not any).  
A6: The training content addresses real security threats.  
A7: You felt that the training was engaging.  
A8: You felt that your knowledge/skills improved by taking the training.  
A9: The training was practical and/or easy to apply.
- \*\* ↑ means this criterion needs to be improved.

Table 6.18: The state of each training programs/systems

### 6.5.5 Participants’ answers in open-end questions

We sort out participants’ answers in the three open-end questions. Listing the different ideas and rewriting the similar ideas.

1. Proprofs

Important learning things	know current threats create quizzes learn responses to attacks
Strengths	assess frequently and extensively user friendly and affordable feedback data is ideal automation of training verification records have explanation text to a question
Weaknesses	a slow internet connection in some areas free trial is too limited
Suggestions	send links and certificates directly and instantly to a cell phone add a video to a question

Table 6.19: The answers of Proprofs

## 2. Marshal Security

Important learning things	learn current security threats know some famous experts empower the knowledge and skills
Strengths	useful training content a lot of current news
Weaknesses	not too much videos
Suggestions	ensure minimum security awareness training videos

Table 6.20: The answers of Marshal Security

## 3. DARKReading

Important learning things	learn current threats learn the newest security activities security campaigns are also important
Strengths	quiz answers with explanations useful training content
Weaknesses	lack challenges limited answering time
Suggestions	add a little difficulty as gamification feature

Table 6.21: The answers of DARKReading

#### 4. Khan Academy

Important learning things	pick up the newest information and videos about cyber security have more perspective to a security topic feel confident to learn other fields
Strengths	enough useful courses to reality threats wide training range a clear interface
Weaknesses	different authors in the series of videos lack a little engaging
Suggestions	need official authors

Table 6.22: The answers of Khan Academy

#### 5. Lynda.com

Important learning things	learn not only security know the expert teams clear know what is cyber security
Strengths	each video has the corresponding quiz practice easy to understand personalized learning
Weaknesses	a small number of quiz questions
Suggestions	add more quiz questions after each section

Table 6.23: The answers of Lynda.com

#### 6. Udemy

Important learning things	current security threats responses to attacks expand knowledge
Strengths	quizzes at the end of each section learning depending on trainees' schedule
Weaknesses	not enough quiz questions
Suggestions	for each section, add more corresponding quiz questions

Table 6.24: The answers of Udemy

#### 7. CSIAC

Important learning things	effective IT security awareness training with different modules multi-stage, continuous learning current security activities
Strengths	release a new video content each month free technical inquiry active groups can be joined in
Weaknesses	no practice
Suggestions	incorporate simulation tests to practice

Table 6.25: The answers of CSIAC

## 8. DVWA

Important learning things	practice the most common web vulnerabilities various levels of difficulty learn something about PHP/MySQL
Strengths	better understand the process of securing web applications learn in a controlled environment a simple straightforward interface
Weaknesses	for technology ones
Suggestions	add easy mode for someone not IT amateur

Table 6.26: The answers of DVWA

## 9. Security Shepherd

Important learning things	safe to practice AppSec techniques see real security risk examples practice the most common web vulnerabilities
Strengths	more comprehensive
Weaknesses	the interface not funny difficult
Suggestions	add easy mode for someone not IT amateur

Table 6.27: The answers of Security Shepherd

## 10. GameOver

Important learning things	teach the basics of web security with XSS, CSRF, RFI&LFI and so on provide a legal platform for testing and exploiting improve knowledge and skills
Strengths	can select the appropriate one among them directional
Weaknesses	a part of practicing platforms lack hints
Suggestions	create a clear hint link between training and practice

Table 6.28: The answers of GameOver

# Chapter 7

## Analysis and Proposed Improvements

### 7.1 The outcome comparison and analysis for 3 e-learning training programs

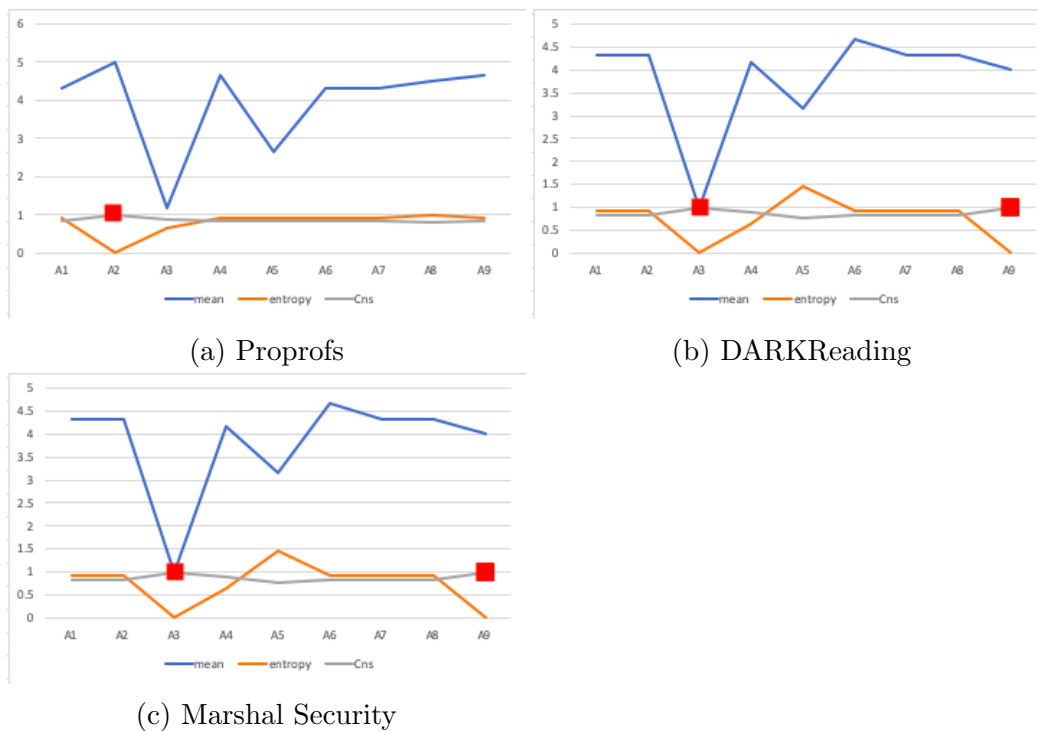


Figure 7.1: The outcome of 3 e-learning training programs

About criterion 1, Marshal Security has the highest mean. According to the value of Cns, as we can say 83% people strongly agree that Marshal Security is a suitable platform for learning.

About criterion 2, Proprofs has the highest mean. According to the Cns, as we can say all people strongly agree that Proprofs has a clear user interface. On the other hand, even though DARKReading and Marshal Security have the same mean, comparing with their Cns, the responses are more clutter in Marshal Security.

About criterion 3, DARKReading and Marshal Security has the same lowest mean. According to the Cns, as we can say all people agree that Proprofs has no problems like dead link,etc.

About criterion 4, Proprofs has the highest mean. According to the Cns, as we can say 83% people strongly agree that Proprofs has sufficiently in-depth training content. On the other hand, DARKReading and Marshal Security are not sufficient enough in training content.

About criterion 5, Marshal Security has the highest mean. According to the value of Cns, as we can say 77% people agree that Marshal Security let trainees enjoy its gamification. On the other hand, comparing with the other two Cns, 83% people disagree with Proprofs's gamification.

About criterion 6, DARKReading has the highest mean. According to the value of Cns, as we can say 83% strongly agree that DARKReading can address real security threats. On the other hand, comparing with the other two Cns, Proprofs are more agreed in addressing real security threats than Marshal Security.

About criterion 7, Proprofs and DARKReading have the same mean and same Cns. They are agreed in engagement by %83 people.

About criterion 8, Marshal Security has the highest mean. According to the value of Cns, as we can say all people strongly agree that Proprofs can improve trainees' skills.

About criterion 9, Proprofs and Marshal Security have the same mean and same Cns. They are more agreed in practical(or easy) applying than DARKReading.

Therefore, the possible point for improving e-learning training program are:

- gamification(Criterion 5: You enjoyed the gamification features in the training.)
- practicality(Criterion 9: The training was practical and/or easy to apply.)

## 7.2 The outcome comparison and analysis for 4 video training programs

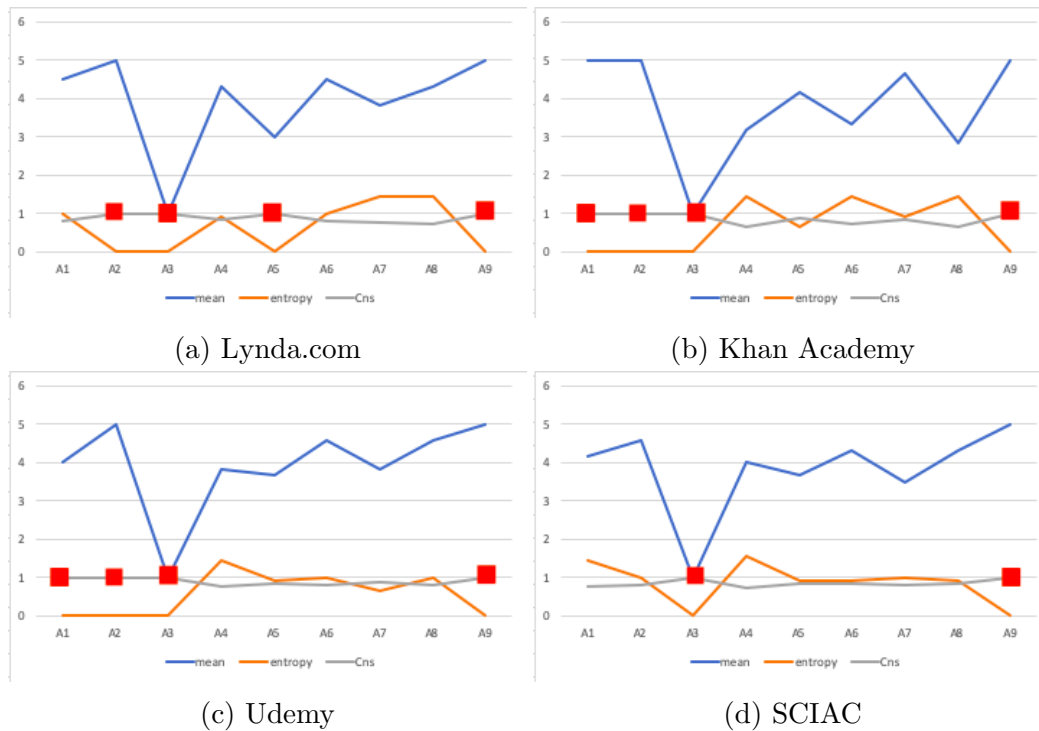


Figure 7.2: The outcome of 4 video training programs

About criterion 1, Khan Academy has the highest mean. According to the Cns, as we can say all people strongly agree that Khan Academy is suitable for learning.

About criterion 2, Lynda.com, Khan Academy and Udemy have the same highest mean and Cns, as we can those three training programs are successful in user interface.

About criterion 3, the four video training programs are not fail in platform problems like dead link, etc.

About criterion 4, Lynda.com has the highest mean. According to the Cns, as we can say %83 people agree that Lynda.com has sufficiently in-depth training content. On the other hand, comparing with the other three Cns, even though Khan Academy is successful in interface, the content may not satisfy most people.

About criterion 5, Khan Academy has the highest mean. According to the Cns, as we can say %89 people agree that Khan Academy makes people



enjoy gamification. On the other hand, Lynda.com seems not giving people the feeling of gamification.

About criterion 6, Udemy has the highest mean. According to the Cns, as we can say %81 people strongly agree that Udemy can address real security threats. Furthermore the mean and Cns of Lynda.com are very close to Udemy so we can consider that Lynda.com is as same as Udemy in addressing real security threats.

About criterion 7, Khan Academy has the highest mean. According to the Cns, as we can say %83 people agreed in Khan Academy's engagement.

About criterion 8, Khan Academy has the lowest mean. According to the Cns, as we can say 66% people disagree that Khan Academy can improve people's skills.

About criterion 9, the four video training programs have the same highest mean and same Cns.

Therefore, the possible point for improving video training program are:

- learning environment(Criterion 1: The training platform was suitable for learning.)
- training content's depth(Criterion 4: The training content is sufficiently in-depth.)
- gamification(Criterion 5: You enjoyed the gamification features in the training.)
- address realistic security threats(Criterion 6: The training content addresses real security threats.)

### 7.3 The outcome comparison and analysis for 3 advanced training programs

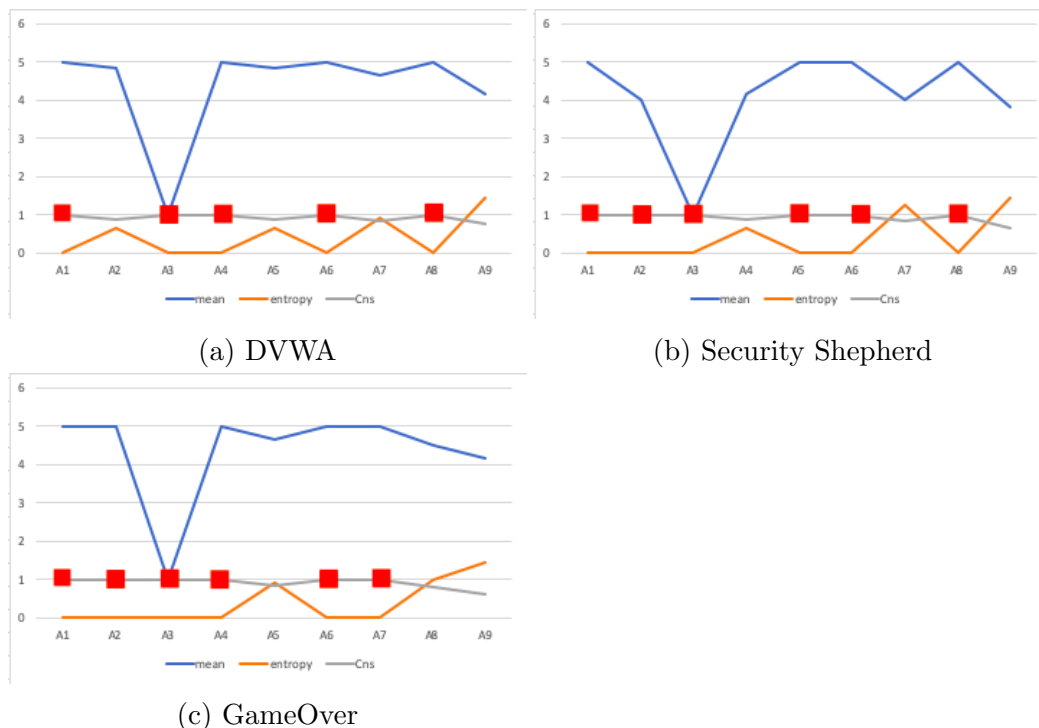


Figure 7.3: The outcome of 3 advanced training programs

About criterion 1, the three advanced training programs have the same highest mean and same Cns, as we can say they are all good at suitable learning environment.

About criterion 2, GameOver has the highest mean. The mean and Cns value of DVWA is very close to GameOver, so we can say that both DVWA and GameOver have clear user interface.

About criterion 3, the three advanced training programs are consensus in platform problems — they have no platform problems.

About criterion 4, DVWA and GameOver have the same highest mean and same Cns, as we can say those two systems are sufficiently in-depth in training content.

About criterion 5, Security Shepherd has the highest mean and Cns, as we can say all people strongly agree that Security Shepherd has more gamification features. Comparing with the other two systems, they have

almost same mean but according to Cns, people have more consensus in DVWA than GameOver.

About criterion 6, the three advanced training programs have the same highest mean and same Cns, as we can say they are all successful in addressing real security threats.

About criterion 7, GameOver has the highest mean. According to the Cns, as we can say all people strongly agree that GameOver is engaging.

About criterion 8, DVWA and Security Shepherd have the same highest mean and same Cns, as we can say those two systems can better improve people's skills than GameOver.

About criterion 9, according to the mean and Cns, Security Shepherd may be not practical(or easy) to apply even though it is good at gamification because it is a little difficult to someone who is not IT amateur.

Therefore, the possible point for improving advanced training system are:

- engagement(Criterion 7: You felt that the training was engaging.)
- practicality(Criterion 9: The training was practical and/or easy to apply.)

## 7.4 Proposed improvements for each assessment criterion

**For "A1: The training platform was suitable for learning"**

- 1) Ensure smooth communication
- 2) Give trainees time to feel comfortable
- 3) Let trainees control their training
- 4) Make learning fun — gamification
- 5) Provide trainees with easily accessible resources repository

**For "A2: The training platform has a clear user interface"**

- 1) Create a short tutorial for trainees when they first log in
- 2) Never design user interface with a surprise
- 3) Make the next step obvious

- 4) Give interface clues training platform interfaces
- 5) Break up the monotony and improve scannability
- 6) Learn from other training platform interfaces.

**For "A3: You noticed problems with the training platform (dead links, etc.)"**

No discussion.

**For "A4: The training content is sufficiently in-depth"**

- 1) Use blended learning
- 2) Take trainee's analytic seriously
- 3) Create learning paths
- 4) Have a mission statement
- 5) Ask trainees what they need

**For "A5: You enjoyed the gamification features in the training"**

- 1) Scenario-based learning
- 2) Interactive video-based approach

**For "A6: The training content addresses real security threats"**

No discussion.

**For "A7: You felt that the training was engaging"**

- 1) Personalization
- 2) High-Quality Content
- 3) Keep texts short
- 4) Embrace new technologies
- 5) Go live (with Instructor-led training)
- 6) Go mobile
- 7) Get the typography right

**For "A8: You felt that your knowledge/skills improved by taking the training"**

No discussion.

**For "A9: The training was practical and/or easy to apply"**

- 1) Make systems and processes as simple and user-friendly as possible
- 2) Don't simply give orders to trainees

## 7.5 Overall Improvements

According to the comments from our participants, we conclude the following points as the improvements.

**For training platform(A1&A2&A3)**

- Create a clear link between training section and outcome evaluation  
For example, a phishing test. If the training program sent a phishing test in January and then sent your training evaluation in February, the logical connection between those two activities is lost.  
We make a clear link between training section and outcome evaluation so that those two types of activities will work most useful in conjunction with each other.
- Keep frequent security training  
Training is not a one-time event like many aspects of security. We need to integrate it into all aspects of the daily life until it becomes a part of your awareness. Regular security awareness training will help put it first.  
Security training is an ongoing process that we need to modify with the changes of trainees. This is to ensure our security awareness state is as measure as possible.
- Use interactive exercises  
For example, desktop exercises; phishing campaigns.

### **For training content(A4&A5&A6)**

- Use real and current phishing examples

Despite computer users becoming smarter and threat tools they used to protect themselves more accurate than ever, the scammers have succeeded. People were cheated out of thousands of dollars with promises of monetary gain or threats of financial or physical danger.

Telling users to be more careful and not to open information from unknown sources which doesn't provide enough insight to protect them from today's complex threats.

- Ensure minimum security awareness training

Security awareness training can be delivered in many ways including computer-based training, formal training, e-mails, memos, notices, posters etc. Whatever the way it is, the training should fit the overall culture of trainees.

The depth of security awareness training could be divided into 3 levels:

1. General security awareness (all personal)
2. Intermediate security awareness(not IT worker but having basic knowledge)
3. In-depth security awareness(IT workers)

### **For training outcome(A7&A8&A9)**

- Customize training by role

A good security training may not localize its education based on culture or language, but it customize security awareness training by job role.

The most effective security awareness training provide the right people at the right time. This means training for your organization and the roles of your trainees, training them when most needed.

- Arrange phishing simulation at random intervals

Whether trying to lower phishing rate or keep trainees on phishing defense, phishing simulation strategy is important. Consider the effectiveness of simulation strategically not just the number of phishing simulations.

Arranging phishing simulations at random intervals to eliminate the ability of trainees to predict phishing email frequency and track changes in behaviour.

- Promote user engagement

Getting users actively involved in the prevention process is a critical component of an effective program, and several studies show that gamification is the best way to increase user engagement. Like Leaderboard/User leveling systems.

# Chapter 8

## Conclusion

At least some current security awareness training platforms recognize the value of security culture and try to measure it from the start. The Cns metrics will be useful over time.

Even though there is a lack of research on behavioral security and theoretical models to explain how consciousness training affects behavior, an advanced security awareness training platform enables security professionals to monitor, nurture and develop a security culture by paying attention to cultural indicators.

In this report, we describe the objectives first. Then introduce five e-learning training programs, 9 video training programs and 3 reading materials training programs as basic security awareness training and the other 6 training systems which are focus on technology as advanced security awareness training. In chapter 6, according to the general rules for writing survey questions and the 3 experts' opinions, we create 9 close-end questions and 3 open-end questions to assessment our selected 10 training programs/systems. At last, using CBA theory as the calculation method of those assessment criteria.

For evaluated training programs/systems, each of them has strengths and weaknesses. We analyze the outcome and give possible improving suggestions for each category of them. Of cause, whatever which category the training program/system belongs to, all of them can be seen as an representative security awareness training project in cyber security world, so we propose the overall actionable improvements in the end of chapter 7. The first possible improvements we proposed is arranging attack simulation at random time to keep the security awareness always in the best state. Or we can offer frequent security training to trainees so that it's difficult to forget what they learn in their training lessons. With respect to security awareness training programs, the threat examples should use real and newest ones to give trainees fresh security knowledge. And also, the training should be suitable to trainee's



experience and intelligence. Only in this way, the security training is most effective to defend the threats in daily life.

Furthermore, there are still some regrets in this report. For example, the number of participants and the identification of participants. If the number could be more larger and a part of participants could be from society not just in school, the outcome will be more accurate.

And in our outcome analysis part, there is no denying that "gamification" is mentioned many times in our possible points for improvement but we have nothing to do with this point. Gamification is essentially using game mechanics and game thinking to engage users to solve problems and by introducing competition and reward elements to motivate them. The strategies we can think of are using rewards, or keeping the training short, or using visual aids and so on with no detailed solutions. We hope someone can consider out a better security awareness training program within gamification to motivate trainees to defeat and protect themselves from cyber threats.

# Bibliography

- [1] URL: <https://www.proprofs.com/>.
- [2] URL: <https://www.itsecurityawareness.ie/cyber-attack-or-data-breach-impact-on-business>.
- [3] URL: <https://www.marshalsecurity.ca/>.
- [4] URL: <https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz/>.
- [5] URL: <https://tech.informa.com/brands/dark-reading>.
- [6] URL: <https://www.sans.org/>.
- [7] URL: <https://www.eset.com/us/cybertraining/>.
- [8] URL: <https://www.khanacademy.org/>.
- [9] URL: <https://www.lynda.com/>.
- [10] URL: <https://www.makeuseof.com/>.
- [11] URL: <https://www.udemy.com/course/security-awareness-training/>.
- [12] URL: <https://www.enisa.europa.eu/media/multimedia/videos>.
- [13] URL: <https://www.csiac.org/series/cyber-awareness-videos/>.
- [14] URL: <http://www.ussecurityawareness.org/highres/index.html>.
- [15] URL: <https://security.ucop.edu/resources/security-awareness/articles.html>.
- [16] Presser S. Converse J. M. *Survey Questions: Handcrafting the Standardized Questionnaire*. Sage University Paper series on Quantitative Applications in the Social Sciences. Thousand Oaks, 1986.
- [17] Jonathan Deller. “10 Training Effectiveness Survey Questions to Ask”. In: (2019).
- [18] James Hartley. “Some thoughts on Likert-type scales”. In: *International Journal of Clinical and Health Psychology* ().

- [19] Fowler F.J. Jr. *Improving Survey Questions: Design and Evaluation*. Applied Social Research Methods Series. Thousand Oaks, 1995.
- [20] Donald Kirkpatrick. ““Evaluating Training Programs” Four Levels”. In: (1993).
- [21] Jon A. Krosnick Melanie A. Revilla Willem E. Saris. “Choosing the Number of Categories in Agree-Disagree Scales”. In: *Structural Equation Modeling A Multidisciplinary Journal* (2014).
- [22] Masha Sedova. “How to Choose the Right Security Awareness Training Solution”. In: (2018).
- [23] Payne Stanley. “The Art of Asking Questions.” In: *Princeton University* (1980).
- [24] Bradburn N. Sudman S. *Asking questions: A practical guide to questionnaire design*. San Francisco, 1982.
- [25] Mark J. Wierman William J. Tastle. “Consensus and dissention: A measure of ordinal dispersion”. In: *International Journal of Approximate Reasoning* 45.8 (), pp. 531–545.