Hands-on Training for Mitigating Web Application Vulnerabilities

2110435 Ngo Van Quyen

Web applications are becoming increasingly complex and interconnected, making them more vulnerable to attack. In 2022, web application attacks accounted for about 56% of all data breaches. This is due to the fact that web applications are often developed using frameworks that contain security vulnerabilities that are known to hackers.

One of the most popular frameworks to build web applications is the Yii2 PHP Framework. Yii2 is a free and open-source framework that is used by millions of developers worldwide. It is also a very secure framework, and it has been penetration tested by a number of security experts. However, there are still some vulnerabilities, such as those caused accidentally or unknowingly by developers, that need to be mitigated.

Mitigating web application vulnerabilities can be approached in several ways. One approach is to use automated tools to scan for vulnerabilities. However, these tools can only find known vulnerabilities, and they often miss new or zero-day vulnerabilities. Another approach is to use manual security testing. This involves having a security expert manually test the application for vulnerabilities. However, manual security testing is a time-consuming and expensive process. A third approach is to use hands-on training. This involves training developers on how to identify and fix vulnerabilities in web applications. Hands-on training should be used as a complement to automated tools or manual security testing, as it teaches developers secure development practices with an attacker perspective.

CyPROM is a scenario progression management system for cybersecurity training that allows instructors to define training scenarios and provide target information. The management module of CyPROM uses a set of processes to drive the execution of those scenarios in the training environment. This enables conducting hands-on training in which trainees can actively engage in simulated cyberattacks, forensic investigations, and defensive measures. Thus, they can actively participate in realistic cyber exercises, gaining practical experience in dealing with cybersecurity challenges. By simulating attack scenarios, trainees can develop skills in identifying vulnerabilities, detecting and responding to threats, and implementing defensive measures.

The research presented in this thesis is an endeavor focused on bolstering the security characteristics of web applications by conducting a meticulous analysis of the Yii2 framework while drawing upon the reputable OWASP Top Ten as a fundamental reference. The OWASP Top Ten, developed and maintained by the Open Web Application Security Project (OWASP) Foundation, plays a crucial role in promoting awareness about the most critical

security risks faced by web applications. By attentively examining the 2021 updates and trends outlined in the OWASP Top Ten, our research ensured a comprehensive approach to addressing the most pressing threats to web application security.

In particular, vulnerabilities within the Yii2 framework were identified and carefully evaluated for their potential impact on web applications, leveraging insights from the OWASP Top Ten. A significant contribution of our research lies in providing a thorough assessment of web applications built on Yii2, aligning the results with industry-accepted security standards, and offering effective strategies to enhance web application security. This was achieved by extending the functionality of CyPROM via a custom module specifically designed for analyzing web applications. Extending CyPROM required a careful understanding of the intricacies of the Yii2 framework and its underlying architecture. We conducted a thorough analysis of the framework's source code, libraries, and dependencies to identify potential areas vulnerable to security threats. The process required reverse engineering and static code analysis to gain comprehensive insights into the framework's security posture.

After gaining a comprehensive understanding of the Yii2 framework, the CyPROM extension development commenced, entailing an in-depth investigation that surpassed mere vulnerability identification. The focus extended to crafting a specialized hands-on training program using CyPROM, tailored explicitly to address the identified vulnerabilities, accompanied by a strategic approach to tackling each security concern. The training program provided a set of systematically implemented actions and scenarios, empowering web developers with practical knowledge to proficiently secure their web applications. This included rules and heuristics inspired by the OWASP Top Ten, targeting prevalent security issues commonly encountered in web applications. Through the incorporation of this extension, CyPROM facilitated automated security assessments, bolstering the security not only of Yii2-based web applications but also laying the groundwork for enhancing the security posture of other frameworks.

The extension of CyPROM was assessed comprehensively via functionality evaluation, comparative analysis of implemented actions and scenarios, and user evaluation. Overall the enhanced CyPROM demonstrated significant coverage in addressing specific vulnerabilities in web applications, with notable strengths in dealing with Broken Access Control (3.36 out of 5), Identification and Authentication Failures (3.27 out of 5), and Cryptographic Failures (3.18 out of 5). The evaluation result, determined based on trainees' feedback obtained during training sessions, estimates the capability of the enhanced CyPROM to handle these critical categories. In addition,

the assessment also revealed areas that need further improvement to increase overall effectiveness in addressing other vulnerabilities. Even so, participants appreciated the clarity and conciseness of the training, which enabled them to apply their newly acquired knowledge in a real-life environment. The positive feedback from users underscored the practical value and real-world relevance of our research findings. Efforts to increase coverage in areas where CyPROM is currently less effective will help improve its capabilities.

This research serves as a valuable resource for developers and security professionals, aiding them in fortifying the integrity of web applications by highlighting vulnerabilities, benchmarking against the OWASP Top Ten, and conducting a comprehensive evaluation of Yii2-based projects.

Keywords: *web application vulnerabilities*, *hands-on training*, *vulnerability mitigation*, *CyPROM*, *Yii2 PHP Framework*, *OWASP Top Ten*.