Title: Comparative Analysis of OWASP ZAP and Burp Suite Professional: Evaluating Web Application Security using Juice Shop against the OWASP Benchmark

Abstract: The rapid expansion of web applications has brought forth increased concerns regarding their security vulnerabilities, necessitating the use of robust web application security testing tools. This thesis presents a comparative analysis of two leading web application vulnerability scanners: Burp Suite Professional and OWASP ZAP. The study focuses on evaluating their efficacy in identifying vulnerabilities within the intentionally vulnerable web application, Juice Shop, while benchmarking their performance against the OWASP Benchmark.

The research methodology involves conducting systematic scans of Juice Shop using both Burp Suite Professional and OWASP ZAP. The OWASP Benchmark is employed as a standardized evaluation framework to assess the scanners' abilities to identify a diverse range of security flaws, namely SQL injection, Cross-Site Scripting (XSS), and more. The key aspects analyzed include scan accuracy, True positives and false positives.

The results obtained from the benchmark comparison offer valuable insights into the strengths and weaknesses of each tool. Additionally, the study highlights the areas where one tool outperforms the other and vice versa. Practical implications are drawn from the findings to aid security practitioners in selecting the most suitable tool for their web application security assessments.

Moreover, the research contributes to the field of web application security testing, as it helps shed light on the effectiveness of popular scanners in identifying vulnerabilities. The knowledge gained from this study can assist security professionals and developers in making informed decisions to bolster their web application security posture.

In conclusion, this thesis serves as a comprehensive analysis of OWASP ZAP and Burp Suite Professional's capabilities in detecting security flaws in Juice Shop. The findings contribute to the ongoing discussions surrounding web application security tools and lay the groundwork for future research and advancements in the domain of web application security testing.