OCT 2023

Graduation Project Proposal: Development of a Web Application Scanner for OWASP Top 10 Vulnerabilities

PRESENTED TO:
D.Mohamed Hassan

PRESENTED BY:
Mohammed Mahmoud

Table of Contents

Introduction

We propose the development of a graduation project that focuses on creating a web application scanner for identifying vulnerabilities from the OWASP Top 10 list. OWASP, the Open Web Application Security Project, identifies the most critical web application security risks, and addressing these vulnerabilities is vital for ensuring the security of web applications.

This graduation project aims to create a web application scanner that automates the process of identifying and reporting vulnerabilities in web applications. The scanner will be designed to help organizations, developers, and security professionals proactively address security issues, reduce the risk of data breaches, and improve the overall security posture of web applications.

Project Team

Mohammed Mahmoud: Project Lead and Developer - Responsible for overall project management, technical development, and ensuring project milestones are met.

Amr Yasser: Quality Assurance and Testing - Responsible for rigorously testing the scanner to validate its accuracy, performance, and security.

Mohammed Mahmoud Morad: UI/UX Designer - In charge of designing an intuitive and user-friendly web-based interface for the scanner.

TEAM MEMBERS

Mohammed Mahmoud

Amr Yasser

Mohammed Mahmoud Morad

Project Objectives

1. Vulnerability Detection: Develop a web application scanner capable of identifying vulnerabilities from the OWASP Top 10 list, including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and others.
2. User-Friendly Interface: Create an intuitive and user-friendly web-based interface to configure scans, view results, and generate detailed reports.
3. Accuracy: Implement techniques to minimize false positives and ensure the accuracy of detected vulnerabilities.
4. Integration: Provide integration options with popular development tools to facilitate seamless security testing within the development process.
5. Scalability: Ensure that the scanner can handle scans of various sizes and complexities while maintaining performance.
6. Customization: Allow users to customize and extend the scanner's functionality to adapt it to their unique needs.

Methodology

To achieve the project objectives, we propose the following methodology:

1. **Requirements Gathering**: Gather and document the specific requirements of the web application scanner, considering user needs and available resources.
2. **Design and Prototyping**: Create a design and prototype of the scanner's user interface and core functionality.
3. **Implementation**: Develop the scanner using suitable programming languages and technologies.
4. **Testing and Validation**: Conduct thorough testing to validate the scanner's accuracy, performance, and security. Address any identified issues.
5. **Documentation**: Prepare comprehensive documentation to guide users on how to use and customize the scanner.
6. **Presentation and Demonstration**: Present the project, demonstrate its functionality, and discuss its significance in web application security.
7. **Final Report**: Compile a final report detailing the project's objectives, methodology, results, and future recommendations.

Timeline and Resources

The project is expected to be completed within (June 1st, 2024), aligning with the graduation requirements. The project can be implemented using commonly available development tools and open-source technologies to minimize costs.

Conclusion

This graduation project offers an excellent opportunity to explore web application security, develop practical skills in software development, and make a meaningful contribution to the field of cybersecurity. By creating a web application scanner for OWASP Top 10 vulnerabilities, this project can help organizations enhance their web application security and protect sensitive data.

I am excited to undertake this project as a graduation endeavor and look forward to the opportunity to learn and develop practical skills in web application security and software development.