Chhatrapati Shivaji Maharaj Institute of Technology

COMPUTER ENGINNERING

ACADEMIC YEAR
2023 - 2024

OWASP OS

Group Members :-

Yuvraj Todankar
Om Dhumal
Raj Mhatre
Atharva Patil

COMPUTER ENGINNERING

Guide Name:- Prof. Anup Maurya

Table Of Contents

- Abstract
- Introduction
- Literature Review
- Problem Statement
- Previous System & Gap Analysis
- Proposed System
- Objective
- Tools And Technology
- Conclusion
- References

Abstract

Our engineering major project introduces a specialized operating system designed for seamless web application development and comprehensive penetration testing, following the principles outlined in the OWASP Web Penetration Testing Guide. This unique OS offers an integrated environment with tailored tools for developers and security professionals, ensuring secure coding practices and thorough vulnerability assessments. By merging web development and cybersecurity, our project aims to enhance application security, streamline workflows, and provide an educational resource for students seeking to master both domains.

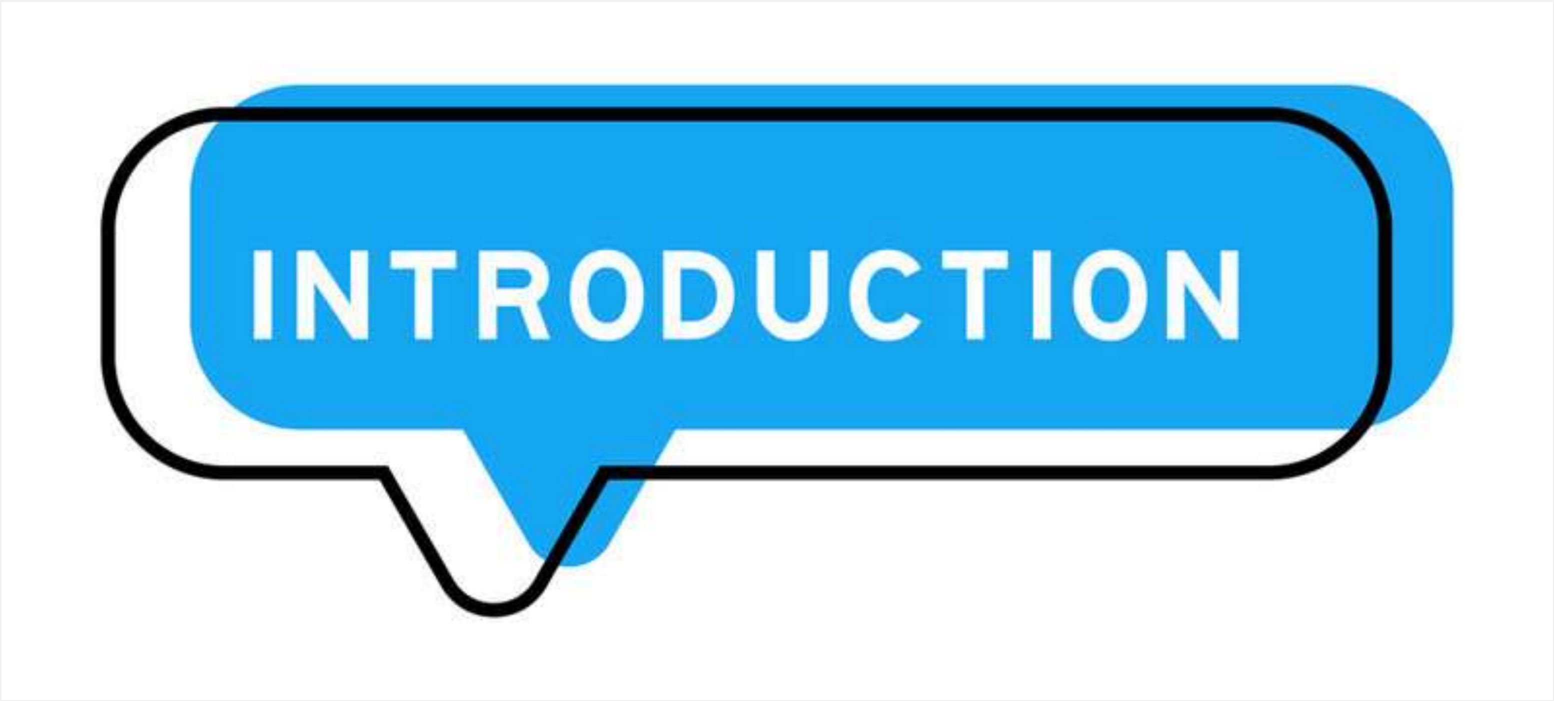
.

Introduction

Web apps now form the foundation of contemporary enterprises and services as a result of the quick expansion of the digital ecosystem.

The need for strong security measures has never been more pressing as businesses rely more and more on web-based platforms to interact with consumers, run operations, and store critical data.

However, the expansion of web applications and the constantly changing world of cyber threats can create a difficult conundrum. We need to adopt a new paradigm for both development and testing processes in order to reconcile functionality and innovation with strict security requirements.



Literature Review

Research paper on Operating system	Anjalee Shau & Rahul chawda	https://ijcrt.org/papers/IJCRT2106251.pdf
Linux based real-time operating system	Michael Barabanov	https://www.yodaiken.com/papers/BarabanovThesis.pdf
Linux operating system	Shahid H. Bokari	https://apps.dtic.mil/sti/pdfs/ADA297953.pdf

Problem Statement

Development of an Integrated Operating System for Streamlined Web Application Development and Penetration Testing, Aligning with OWASP Web Penetration Testing Guide

In the rapidly evolving landscape of web application development and cybersecurity, the need for a comprehensive and specialized operating system has become increasingly evident. The conventional approach of utilizing disparate tools and environments for web application development and penetration testing introduces inefficiencies, complexity, and potential security gaps.

Previous System & Gap Analysis

The previous system was a basic operating environment for web application development and penetration testing. It lacked efficient integration of tools, alignment with OWASP guidelines, and user-friendly features.

While it provided some resources for security testing, it fell short of offering a comprehensive and specialized environment.

The system's documentation might have been limited, and it might not have catered well to the evolving landscape of web application security.

Tool Integration and Streamlining: The previous system lacked efficient integration and management of a comprehensive set of web application development and penetration testing tools.

OWASP Alignment and Documentation: The previous system did not have a strong alignment with OWASP guidelines and the Web Penetration Testing Guide.

User Experience and Customizability: The user experience in the previous system might have been less intuitive, hindering usability for both novice and experienced users.

Proposed System

Integrated Tool Suite: Develop an all-in-one operating system that integrates a comprehensive suite of web application development and penetration testing tools, accessible through a user-friendly interface. This suite will cover various stages of the development lifecycle and offer a seamless experience for users to switch between tasks.

OWASP-Aligned Framework: Design the system architecture and workflows based on the OWASP Web Penetration Testing Guide, ensuring adherence to industry best practices and security standards. The system will facilitate easy access to relevant resources and methodologies, promoting effective web application security testing.

Objectives

Comprehensive Operating Environment

Develop an operating system that provides a comprehensive environment for web application development and penetration testing, integrating tools and resources to cover the complete lifecycle of web application security.

OWASP Web Penetration Testing Guide Integration

Incorporate the OWASP Web Penetration Testing Guide as a central knowledge base and reference, ensuring that the operating system aligns with the best practices and methodologies defined by OWASP for effective web application security testing.

User-Friendly Interface

Create an intuitive and user-friendly graphical user interface (GUI) that allows users, regardless of their level of expertise, to easily access and utilize various tools, scripts, and resources required for web application development and penetration testing.

Objectives

Tool Integration and Management

Integrate a diverse set of open-source and proprietary web application development and penetration testing tools, ensuring seamless installation, updates, and management of these tools within the operating system.

Documentation and Training Materials

Create comprehensive documentation and training materials that explain the operating system's features, functionalities, usage guidelines, and tutorials, empowering users to effectively leverage the system for web application development and security testing.

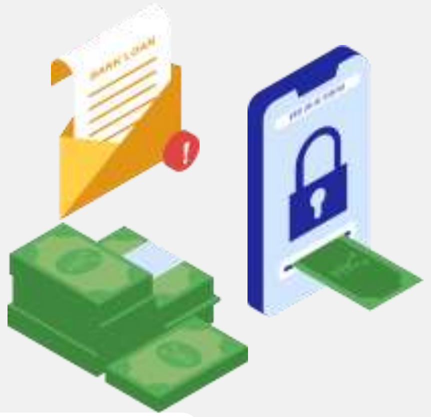
Regular Updates and Maintenance

Establish a process for regular updates and maintenance of the operating system, ensuring that it remains up-to-date with the latest security tools, libraries, and best practices in the dynamic field of web application security.

ethodology

- Debian 11 “Bullseye” upgraded to Debian 12 “Bookworm”
- Transition from GNOME to KDE Plasma
- Optimization for Performance and Security
- Implemented Firewall
- Enhanced Development Environment
- Improved User Interface
- Security Compliance

Tools And Technology



Virtual Box

Debian based linux

Kali linux (Penetration Testing Distribution)

Python, C and Java Language

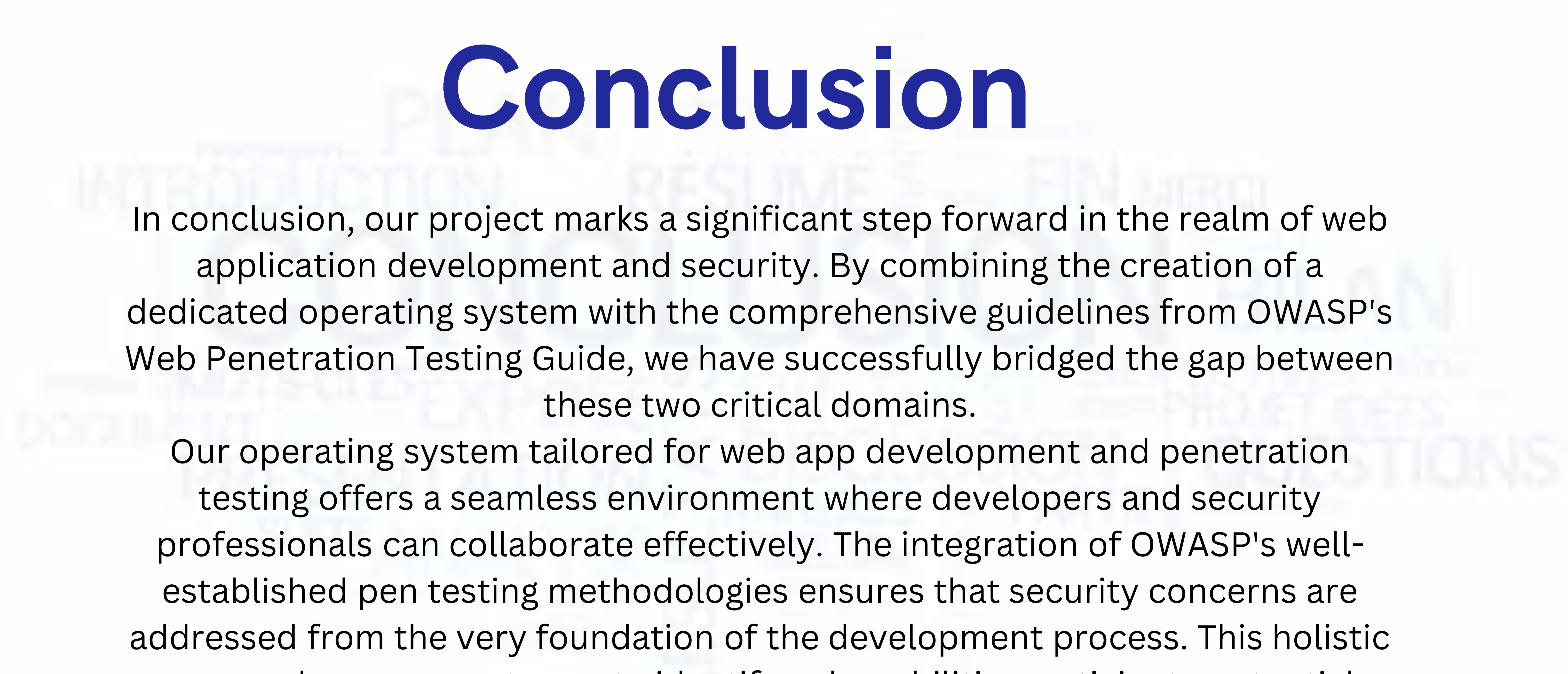
Node.js

Burp Suite

OWASP ZAP, OWASP AMASS

Visual studio code, VIM

Conclusion



In conclusion, our project marks a significant step forward in the realm of web application development and security. By combining the creation of a dedicated operating system with the comprehensive guidelines from OWASP's Web Penetration Testing Guide, we have successfully bridged the gap between these two critical domains.

Our operating system tailored for web app development and penetration testing offers a seamless environment where developers and security professionals can collaborate effectively. The integration of OWASP's well-established pen testing methodologies ensures that security concerns are addressed from the very foundation of the development process. This holistic approach empowers teams to identify vulnerabilities, anticipate potential threats, and implement robust security measures throughout the development lifecycle.

References

https://owasp.org/www-project-web-security-testing-guide/v41/	
https://www.linuxfromscratch.org/	
https://www.debian.org/	
https://nodejs.org/en	

Do you have any questions?

Thank You!