CS491 AutoPen AI Project Scope

# // Product Vision Statement:

The AutoPen Project is designed to revolutionize penetration testing in the dynamic and challenging field of cybersecurity, where threats are constantly evolving. The core of AutoPen lies in its sophisticated backend, which integrates top-tier penetration testing tools like Burp Suite with a cloud-enabled front service. This combination ensures a flexible yet reliable method for an easy-to-use and effective penetration testing process. The project's goals include developing a comprehensive system that facilitates autonomous penetration testing, creating a user-friendly dashboard for easy management and review of test results, and delivering actionable insights from identified vulnerabilities. AutoPen will be highly adaptable, regularly updating its testing protocols to keep pace with new and emerging threats. Commitment to compliance with established cybersecurity frameworks and regulations is also a priority, including features like automated incident report generation and options for periodic or on-demand vulnerability assessments. Through these features, AutoPen aims to offer organizations a more efficient, cost-effective, and thorough solution for detecting and addressing security weaknesses, thereby significantly enhancing overall cybersecurity resilience in an increasingly complex digital world.

**End of Sprint 1 Presentables - 2/8/2024**

1. **Technical Requirements Document**
2. **UI/UX: Functioning Dashboard Prototype**
3. **Complete Setup of Penetration Testing Environment (including updating tools and ensuring network isolation)**
4. **Recorded Preliminary Manual Penetration Test Demonstration**
5. **Initial Integration of Backend Systems (e.g., Burp Suite) with Cloud Infrastructure**
6. **Basic Usability Features Implementation (e.g., easy navigation, user-friendly interfaces)**
7. **Outline of Process Optimization Strategies (for efficient and effective testing procedures)**

**End of Sprint 2 Presentables - 3/7/2024**

1. **Enhanced Dashboard Features (including basic automation functionality and test initiation)**
2. **Data Logging System for Test Activities**
3. **Initial Test Results Display Interface (with basic visualization tools)**
4. **Development of Automated Reporting Mechanism (for clear and easily understandable reports)**
5. **Preliminary Integration of Additional Cybersecurity Software with the Backend**

**End of Sprint 3 Presentables - 4/25/2024**

1. **Full Integration of Automated Testing Processes**
2. **Comprehensive Reporting System (including automated incident reports and vulnerability assessments)**
3. **User Acceptance Tests (UAT) for Dashboard and Reporting Systems**
4. **Compliance Report with Standard Cybersecurity Frameworks and Regulations**
5. **Detailed User Guide/Manual for Utilizing AutoPen**
6. **Phase 2 Plan (focusing on further usability enhancements and process optimization)**

**Stretch Goals**

1. **Development of a Chatbot Assistant for the Dashboard (to aid in understanding and using the online tool effectively)**
2. **Advanced Usability Features and Dashboard Customization Options**

# // Section 1: Basic Framework, Research, and Cybersecurity Prep

// Objective: Rearrange and solidify the foundational structure of the project for phase two, conducting essential research, and preparing the environment for penetration testing without an AI focus, emphasizing usability and process optimization.

// Tasks: (1 week)

1. Revise the Project Vision Statement to align with new goals.

2. Set up version control (e.g., Git repository).

3. Create a modified project roadmap outlining the sprints, focusing on usability and backend integration.

4. Conduct research on existing penetration testing tools outside of just Burp Suite and potentially better methodologies than last semester.

5. Identify key cybersecurity frameworks and regulations to adhere to.

6. Develop an updated list of technical requirements for the project, focusing on user-friendly technologies (e.g., Node.js, Python with Django, HTML integration).

9. Re-evaluate testing environment (e.g., VMs, Docker containers) for penetration testing.

10. Conduct new preliminary manual penetration tests to understand the test environment.

// Section 2: Usability Enhancement and Backend Integration

// Objective: Develop the project's usability features, refine the dashboard, and finalize the integration of backend systems for effective penetration testing.

// Tasks: (3 weeks)

1. Reformat the basic UI/UX for the dashboard, focusing on ease of use.

2. Implement a basic version of automated testing processes.

3. Develop and document the process for the integration of cybersecurity tools with the backend.

4. Finalize the setup of the penetration testing environment (update tools, ensure network isolation, etc.).

5. Validate the environment by conducting a series of manual penetration tests.

6. Start building the UI for the dashboard, incorporating user-friendly features.

7. Simulate test results in the dashboard using dummy data.

8. Implement basic navigation and usability features in the dashboard.

9. Set up data logging for test activities.

10. Conduct initial tests on the dashboard and backend integration.

11. Document the development process with a focus on usability and security considerations.

// Section 3: Advanced Usability and Reporting Features

// Objective: Finalize the dashboard functionalities with advanced usability features, complete the reporting system, and demonstrate the working product.

// Tasks: (5 weeks)

1. Develop advanced usability features for the dashboard.

2. Integrate comprehensive reporting mechanisms in the dashboard.

3. Implement features in the dashboard to display and interpret test results.

4. Test the integrated system for usability, bugs, and vulnerabilities.

5. Create a prototype of the automated incident report generator.

6. Conduct user acceptance testing (UAT) with a focus group.

7. Make adjustments based on user feedback.

8. Prepare a presentation showcasing the working product with emphasis on usability and efficiency.

9. Present the working product.

// Section 4: Refinement, Optimization, and Chatbot Integration (Stretch Goals)

// Objective: Refine and optimize the AutoPen system, focusing on efficiency and the addition of a chatbot assistant.

// Tasks: (3 weeks)

1. Conduct code reviews to identify areas for usability and efficiency improvements.

2. Optimize backend processes for speed and accuracy.

3. Refine the dashboard UI/UX based on comprehensive user feedback.

4. Enhance the features of the incident report generator.

5. Test for compliance with standard cybersecurity frameworks and regulations.

6. Optimize the system for scalability, especially targeting SMEs.

7. Conduct further UAT with a broader user group.

8. Begin development of a chatbot assistant to aid users in navigating and utilizing the tool.

9. Update system documentation to reflect the changes.

10. Finalize user guides and FAQs, including instructions for the chatbot feature.

11. Prepare and distribute a project completion report with future development plans.