Website Vulnerability Scanner: VulnXposer

Thesis/Project Part I (CSE4192)

Department of Computer Scrience & Engineering

TMSS Engineering College, Bogura.

(Affiliated with University of Rajshahi)

A Project Proposal

Submitted for the partial fulfillment of the requirements

for the degree of B.Sc. Engineering in Computer Science & Engineering

Submitted by

Mohammad Omor Faruk

ID: 1937820111

Session: 2018-2019

Supervised by

Mohadeb Kumar

Lecturer (CSE),

TMSS Engineering College, Bogura

Table of Contents:

Introduction:

This project is all about making websites more secure. In today's online world, it's crucial to protect websites from cyber-attacks. We're creating a tool, a website vulnerability scanner, to help with this.

The idea is to have a scanner that can find and report potential security problems on websites. Cyber-attacks are happening more often, and we want to provide a solution to identify and fix these issues before they become big problems.

Our goal is to make a user-friendly tool that not only spots common web vulnerabilities but also gives users helpful insights. This way, people can easily understand and manage the security of their websites. The upcoming sections will explain in detail what we aim to achieve, how the tool will work, and what features it will have.

Project Objectives:

The main goals of our project are clear, and with the expanded scope, we aim to:

1. Identify a Broad Range of Vulnerabilities:
- Develop the capability to identify a comprehensive array of web vulnerabilities, including those outlined in the OWASP Top 10. This ensures a thorough examination of potential security threats.

2. Report Vulnerabilities Clearly:
- Enhance reporting mechanisms to provide users with clear and actionable insights into identified vulnerabilities. Clarity in reporting is essential for effective remediation.

3. Improve Overall Web Security:
- Contribute to the enhancement of overall web security by addressing a wider spectrum of vulnerabilities. Our tool seeks to not only identify but also assist in the improvement of security practices.

Tools:

1. **Node.js:** Powers the backend, ensuring robust and scalable operations.
2. **React:** Drives the user-friendly frontend, providing an interactive experience.
3. **Bash Scripts:** Executed by the backend to collect information, involving **Python**, **Go**, and **Bash scripting.**

Features:

1. Port Scanning:
- Identifies open ports, highlighting potential entry points for vulnerabilities.

2. Host Identification and DNS Analysis:
- Robust features for identifying hosts and performing DNS analysis, offering insights into the website's infrastructure.

3. CVE Detection:
- Detects Common Vulnerabilities and Exposures (CVEs), promptly recognizing known security issues.

4. OWASP Top 10 vulnerability Scanning:
- Scans for vulnerabilities listed in the OWASP Top 10, ensuring a comprehensive examination within the defined **scope**.

5. User-friendly Web Interface:
- Presents results in a user-friendly web interface, enhancing comprehension and facilitating action on identified vulnerabilities.

Scope:

- SQL Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

Implementation Plan:

Creating our tool is a process, and here's how we plan to do it:

- Break the development into phases, like working on the backend, designing the frontend, and integrating scanning scripts.
- Set milestones and timelines to keep us on track.

This way, we make sure we're building things step by step, and we have a clear plan for when each part will be ready. In the upcoming sections, we'll detail these phases and milestones.

Testing, Quality Assurance and Risk Analysis

Making sure our tool works well is crucial. Here's our plan for testing and analysing risks:

- We'll use different methods to test the tool and make sure the results are reliable.
- Quality assurance processes will be in place to maintain high performance.
- Identify possible risks, like technical challenges or concerns about data security.
- Come up with strategies to deal with each risk.

User Interface and User Experience

- User Authentication
- Intuitive Dashboard
- Real-time Progress Updates
- Detailed Scan Reports
- Historical Scan Data
- Alerts and Notifications
- User Feedback Mechanism
- Responsive Design

Security Measures

Security is a top priority. Here's what we're doing to keep our tool and user data safe:

- Implement measures to ensure the confidentiality and integrity of scanned data.
- Ensure the tool itself doesn't introduce vulnerabilities.

We want users to trust our tool, and that starts with making it secure. In the next sections, we'll provide more details on the security measures we're putting in place.

Legal and Ethical Considerations

To make sure our project is on the right side of the law and follows ethical standards. Here's our approach:

- Detail how our project complies with laws and regulations.
- Emphasize the ethical use of the vulnerability scanner.

Being legal and ethical is not just a choice; it's a commitment we take seriously. In the next sections, we'll explain our compliance strategies and ethical considerations.

Future Implementation Plan

- Subscription Model

Now, let's talk about how our tool will be available to users and what benefits come with a subscription:

- We'll offer our tool as a service (SAAS), meaning users can access it online.
- Subscription users get extra features that free users don't have access to.

By having a subscription model, we can keep the basic scanning available for everyone while providing additional perks to those who subscribe. In the next sections, we'll go deeper into what users get with and without a subscription.

Impact on the society

It will addresses potential impacts of cybersecurity breaches in the following ways:

1. Financial Losses:
- Identifies vulnerabilities to prevent unauthorized access and financial losses.

2. Trust and Confidence:
- Enhances security to rebuild trust in financial institutions, both locally and internationally.

3. Operational Disruption:
- Minimizes the risk of disruptions by detecting and resolving vulnerabilities early on.

4. Reputational Damage:
- Prompts prompt action on vulnerabilities, mitigating the risk of reputational harm.

5. Increased Regulatory Scrutiny:
- Supports compliance with cybersecurity regulations through active vulnerability management.

6. National Security Concerns:
- Strengthens the cybersecurity of critical financial infrastructure for national security.

7. Cybersecurity Awareness:
- Promotes a security-conscious culture through proactive vulnerability scanning.

In summary, VulnXposer offers a preventive solution, fortifying the various online sector against potential cyber threats and their associated impacts.

Signature of Student

Mohammad Omor Faruk
ID: 1937820111
Session: 2018-2019

Signature of Supervisor

Mohadeb Kumar
Lecturer (CSE),
TMSS Engineering College, Bogura.

Signature of Department Head

Md. Khairul Hassan
Lecturer (CSE),
TMSS Engineering College, Bogura.

Signature of External Examiner

Md. Tohidul Islam
Associate Professor,
Department of CSE, Rajshahi University, Rajshahi.