Sri Lanka Institute of Information Technology

Audit Report

Submitted by:

Student Registration Number	Student Name
IT20613518	Madhusanka D.N.V

28/05/2023

Executive Summary:

This secure audit report presents the findings of the audit conducted on a machine learning-based malicious website detection chrome extension. The audit focused on identifying security vulnerabilities within the software application based on the OWASP (Open Web Application Security Project) framework. The report provides an assessment of the identified vulnerabilities and offers recommendations to address these security concerns, aiming to enhance the overall security posture of the system.

Audit Scope:

The audit covered the following areas using the OWASP framework:

Input Validation:

- Ensuring proper input validation to prevent malicious data injections and potential security breaches.
- Assessing the effectiveness of data validation mechanisms in detecting and handling invalid or malicious inputs.

Authentication and Authorization:

- Evaluating the strength and security of authentication mechanisms to ensure only authorized users have access to the system.
- Assessing the effectiveness of access controls and authorization mechanisms in protecting sensitive data and functionalities.

Session Management:

- Analysing the session management implementation to prevent session hijacking and session fixation attacks.
- Assessing the session timeout, session regeneration, and session token handling mechanisms for security vulnerabilities.

Secure Communication:

- Evaluating the implementation of secure communication protocols (e.g., SSL/TLS) to ensure data confidentiality and integrity during transmission.

- Assessing the handling of sensitive data, such as user credentials, to prevent unauthorized access or interception.

Error Handling and Logging:

- Analysing error handling mechanisms to prevent the exposure of sensitive information or potential vulnerabilities.
- Assessing the logging mechanisms to ensure proper recording of security-related events for monitoring and incident response.

Audit Findings:

Based on the assessment using the OWASP framework, the following security vulnerabilities were identified:

- Lack of input validation: The system does not sufficiently validate user inputs, which may lead to potential security vulnerabilities, such as SQL injection or cross-site scripting (XSS) attacks.
- Inadequate authentication and authorization: The authentication mechanism does not employ strong password policies, and the authorization mechanism lacks proper access controls, increasing the risk of unauthorized access to sensitive data and functionalities.
- Weak session management: The session management implementation lacks sufficient protection against session hijacking or fixation attacks, potentially compromising user sessions and their associated data.
- Insufficient secure communication: The system does not consistently enforce secure communication protocols, leaving sensitive data vulnerable to interception or unauthorized access during transmission.
- Poor error handling and logging: The error handling mechanism does not adequately sanitize error messages, potentially exposing sensitive information. Additionally, logging mechanisms lack proper protection and may not capture crucial security events effectively.

According to OWSAP zap following vulnerabilities were found.

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	4 (66.7%)
Missing Anti-clickjacking Header	Medium	4 (66.7%)
Strict-Transport-Security Header Not Set	Low	5 (83.3%)
Timestamp Disclosure - Unix	Low	3 (50.0%)
X-Content-Type-Options Header Missing	Low	4 (66.7%)
Re-examine Cache-control Directives	Informational	4 (66.7%)
Total		6

Recommendations:

To address the identified vulnerabilities, the following recommendations are proposed:

- Implement robust input validation mechanisms to sanitize user inputs and prevent common attack vectors, such as SQL injection and XSS attacks.
- Strengthen the authentication mechanism by enforcing strong password policies, implementing multi-factor authentication where applicable, and conducting regular security audits of the authentication system.
- Enhance session management security by implementing secure session handling techniques, including secure session tokens, session timeouts, and regular session regeneration.
- Enforce the use of secure communication protocols, such as SSL/TLS, throughout the application to protect sensitive data during transmission.
- Improve error handling mechanisms to prevent the leakage of sensitive information and implement proper logging practices to capture security-related events effectively.
- Implement CSP header and Anti-clickjacking header.

Conclusion:

The secure audit conducted using the OWASP framework has identified several security vulnerabilities within a machine learning-based malicious website detection chrome extension. By implementing the recommended measures and addressing the identified vulnerabilities, the

system can significantly enhance its security posture, ensuring the protection of user data and mitigating potential security risks.