Alden A. Quiñones
IT Protection and Security: MIT 264

Proposal for Security Audit of PNexus Web Application and its Deployment Environment.

Project Type: Security Audit

This proposal outlines a comprehensive security audit of the PNexus Web Application used by the Department of Social Welfare and Development (DSWD) under the Pantawid Pamilyang Pilipino Program (4Ps). The audit will focus on identifying vulnerabilities within the application, deployment environment, and infrastructure, specifically using OWASP ZAP and Wireshark as the primary tools for testing and analysis.

Scope and Limitations

1. The primary focus will be on identifying vulnerabilities within the **PNexus Web Application** and its associated security components, which are part of the Pantawid Pamilyang Pilipino Program. This will include a comprehensive evaluation of the application's front-end, back-end, authentication mechanisms, and its integration with the underlying infrastructure.
2. The audit will focus on the **security of the PNexus application** and the **OCP Server** where the application is deployed, including the server's network infrastructure and security configurations.
3. The audit will not cover potential data inconsistencies or security issues related to **data imported from the official Pantawid information system**.
4. The audit will be limited strictly to the **OCP Server** hosting the PNexus application and will not include other systems or infrastructure within **DSWD FO12**.
5. The audit will not assess the **backup policy**, as it is not implemented in the current infrastructure.

Objectives

The main objectives of the security audit are as follows:

1. To identify possible vulnerabilities within the PNexus Web Application and deployment environment.
    - This includes identifying potential vulnerabilities in the codebase, user authentication, and front-end technologies.
    - Assess the security of the server environment, including issues such as insecure configurations, improper server hardening, and other potential deployment flaws.
2. To provide recommend best practices and security enhancements to mitigate identified vulnerabilities.

Target System or Case Study

The case study for this audit focuses on the PNexus Web Application, a system used by the Department of Social Welfare and Development (DSWD) as part of the Pantawid Pamilyang Pilipino Program. This application is built using several key technologies, which include CodeIgniter version 3 for the back-end, with the system lacking built-in ORM support, potentially exposing it to SQL injection vulnerabilities. The system currently operates over HTTP, an insecure protocol that poses a risk to data integrity and confidentiality. On the front-end, the application utilizes jQuery, HTML5, and Bootstrap 4, which can be

susceptible to security issues like cross-site scripting (XSS) or cross-site request forgery (CSRF) if not properly configured.

Regarding security mechanisms, the application lacks CAPTCHA, most like it more vulnerable to bot attacks, and there is no implementation of Two-Factor Authentication (2FA), which increases the probability of account compromises. The system integrates with Active Directory for user authentication, which seems to be secure but the way it integrates with the web-application should also be checked. Access to the system is limited to the GlobalProtect VPN, which adds a layer of security but requires thorough assessment to identify potential vulnerabilities. The ICT infrastructure also includes a VPN network that provides secure remote access, though the configuration and security of this network need to be reviewed. In deployment environment, the system runs in a Hyper-V virtualized environment on an OCP server, which requires a detailed security review for potential vulnerabilities. One possible critical issue is the possible absence of a formal backup policy; thus critical data may be at risk of loss in the event of a breach or system failure.

Tools and Frameworks to be Used

1. OWASP ZAP - An open-source web application security scanner will be the primary tool used to perform dynamic application security testing (DAST) on the PNexus Web Application. ZAP will help identify issues such as SQL injection, Cross-Site Scripting (XSS), insecure HTTP methods, and other common vulnerabilities in web applications.

2. Wireshark - A network protocol analyzer will be used to capture and analyze network traffic to check for unencrypted data transmission and other potential vulnerabilities in communication between the client and server.

3. Nmap (Network Mapper) - will be used to perform network reconnaissance and vulnerability scanning. With its Nmap Scripting Engine (NSE), it can detect open ports, service versions, operating system fingerprints, and common vulnerabilities in running services (e.g., outdated Apache, weak SSL ciphers, known CVEs).

Ethical and Legal Considerations

The security audit will be conducted in accordance with ethical standards, ensuring that no data is compromised, and privacy is respected throughout the process. The following legal and ethical guidelines will be adhered to:

1. Philippine Data Privacy Act of 2012 (Republic Act No. 10173) - A law mandates that the collection, processing, and storage of personal data must be done securely, and it provides guidelines for data protection. All actions during the audit will comply with the provisions of this law to ensure the protection of personal and sensitive data.
2. Prior to starting the audit, consent will be obtained from the relevant authorities at the DSWD to ensure that the audit is conducted with full knowledge and approval.