**Vulnerability Assessment Proposal**  
**For PNexus Web-Based Application**

**Prepared for:**

Department of Social Welfare and Development (DSWD)  
Pantawid Pamilyang Pilipino Program (4Ps)

**Prepared by:**

Alden A. Quiñones  
Information Technology Officer I  
Department of Social Welfare and Development Field Office XII

**Date:**

[Insert Date]

**1. Introduction**

The Department of Social Welfare and Development (DSWD), particularly the Pantawid Pamilyang Pilipino Program (4Ps), has developed a web-based application known as PNexus. This system integrates multiple microservices such as document indexing and grievance verification. Given its critical role in program operations and data management, ensuring the security of PNexus is of utmost importance.

This document outlines a vulnerability assessment proposal aimed at identifying security gaps in the application and recommending mitigations to enhance its overall security posture.

**2. Scope of Assessment**

The vulnerability assessment will focus on the following key areas:

**2.1 Application Architecture & Technologies**

* **Backend:** CodeIgniter v3 (instead of v4) with PostgreSQL
* **Frontend:** Bootstrap, jQuery
* **Environment:**
  + Running in XAMPP instead of Nginx
  + Uses HTTP instead of HTTPS
  + Running inside a VPN requiring Active Directory authentication
* **Security Concerns:**
  + No CSRF protection on jQuery POST requests
  + Weak password restrictions
  + No CAPTCHA implementation
  + Active Directory-based authentication without additional security controls
  + Debug mode is enabled

**2.2 Assessment Methodology**

The assessment will involve the following phases:

1. **Information Gathering:** Understanding system components and architecture.
2. **Threat Modeling:** Identifying potential attack vectors.
3. **Vulnerability Scanning:** Utilizing security tools to detect vulnerabilities.
4. **Manual Testing:** Simulating real-world attack scenarios.
5. **Analysis & Reporting:** Compiling findings with risk ratings and recommendations.

**3. Key Security Concerns & Approach**

**3.1 Lack of HTTPS Implementation**

* **Risk:** Data transmission is unencrypted, making it susceptible to interception.
* **Approach:** Implement SSL/TLS to encrypt communication.

**3.2 Debug Mode Enabled**

* **Risk:** Exposes sensitive system information that can be exploited.
* **Approach:** Disable debug mode in the production environment.

**3.3 Weak Password Policy**

* **Risk:** Increases susceptibility to brute force and credential stuffing attacks.
* **Approach:** Enforce strong password policies (e.g., minimum length, complexity rules, expiration policy).

**3.4 No CSRF Protection on jQuery POST Requests**

* **Risk:** Application vulnerable to Cross-Site Request Forgery attacks.
* **Approach:** Implement CSRF tokens in all form submissions and AJAX requests.

**3.5 Lack of CAPTCHA on Login Pages**

* **Risk:** Increases susceptibility to automated brute force attacks.
* **Approach:** Implement CAPTCHA (e.g., Google reCAPTCHA) on authentication and sensitive forms.

**3.6 Use of Active Directory Without Additional Security Controls**

* **Risk:** Potential for unauthorized access if AD accounts are compromised.
* **Approach:** Implement Multi-Factor Authentication (MFA) and enforce least privilege access control.

**4. Deliverables**

Upon completion of the assessment, the following reports will be provided:

* **Executive Summary Report:** High-level overview of findings and recommended actions.
* **Technical Vulnerability Report:** Detailed description of identified vulnerabilities, risk levels, and remediation steps.
* **Penetration Testing Report:** Insights from manual testing simulating real-world attacks.
* **Remediation Roadmap:** Prioritized list of security improvements with estimated implementation timelines.

**5. Timeline**

| **Phase** | **Duration** |
| --- | --- |
| Information Gathering | 1 week |
| Threat Modeling | 1 week |
| Vulnerability Scanning | 2 weeks |
| Manual Penetration Testing | 2 weeks |
| Reporting & Recommendations | 1 week |
| **Total Estimated Time** | **7 weeks** |

**6. Conclusion**

The PNexus application plays a critical role in the operations of the Pantawid Pamilyang Pilipino Program. Addressing security vulnerabilities is essential to protect sensitive beneficiary data, maintain system integrity, and ensure uninterrupted service. This assessment aims to identify and mitigate security risks, providing actionable recommendations to enhance the overall security posture of PNexus.

We look forward to your approval and collaboration in executing this security assessment.

**Prepared by:**  
Alden A. Quiñones  
Information Technology Officer I  
DSWD Field Office XII