Lab: Authorized External Security & Compliance Assessment

1. Introduction

GRC analysts, this lab provides a rare opportunity to conduct a **full, authorized security assessment** on a live, public-facing web application. You have been formally granted permission by the relevant authorities to test the Nasarawa State Pension Bureau member portal. This exercise will simulate a real-world external penetration test and compliance audit, allowing you to apply all the technical skills you've learned within a legal and ethical framework. Your findings will be used to help the organization improve its security posture.

2. Scenario

The Nasarawa State Pension Bureau has proactively engaged your GRC team to perform a comprehensive security assessment of their online portal. The goal is to identify technical vulnerabilities and compliance gaps before they can be exploited maliciously. You have been provided with a formal, signed agreement authorizing testing, including the use of automated scanners and controlled exploitation attempts.

3. Objectives

- Conduct full reconnaissance and enumeration against the target domain.
- Utilize Burp Suite Professional to perform active vulnerability scanning and manual testing.
- Identify and validate vulnerabilities, mapping them to the OWASP Top 10 and other compliance frameworks.
- Assess the configuration and strength of underlying infrastructure (HTTP headers, SSL/TLS).
- Produce a professional report detailing technical findings, associated risks, and compliance implications.

4. Lab Setup & Authorization

- **Authorization Letter:** You are operating under a signed document stating: *"This assessment is authorized by the Nasarawa State Pension Bureau. Testing is permitted from the IP range of [Your Lab IP]. Testing may include security scanning and controlled exploitation attempts."* **This is a critical document for your audit trail.**
- **Your Machine:** Kali Linux (Attacker)
- **Target Website:** https://pension.nasarawastate.gov.ng
- **Tools:** nmap, Burp Suite Professional, nikto, nuclei, sslscan, browser developer tools

5. Step-by-Step Instructions

Phase 1: Reconnaissance & Mapping

Step 1: Active Reconnaissance with Nmap

- **Task:** Discover the target's online infrastructure and attack surface.
- **Commands:**

Perform a comprehensive scan, saving all outputs and generating an HTML report

nmap -sV -sC -O -p- -oA nasarawa_pension_scan pension.nasarawastate.gov.ng

xsltproc -o nasarawa_nmap_report.html nasarawa_pension_scan.xml

- **Analysis:** Identify all open ports. Pay special attention to:
  - Port 80 (HTTP) and 443 (HTTPS)
  - Any unexpected open ports (e.g., 21/FTP, 22/SSH, 3389/RDP) which would be a critical finding.

Step 2: Web Application Discovery

- **Task:** Actively discover directories, files, and applications on the web server.
- **Commands (Choose one or both):**

Using dirb for directory brute-forcing (common practice in authorized tests)

dirb https://pension.nasarawastate.gov.ng /usr/share/wordlists/dirb/common.txt -o dirb_scan.txt

Using Nikto to identify known vulnerabilities and misconfigurations

nikto -h https://pension.nasarawastate.gov.ng -o nikto_scan.txt

- **Action:** Analyze the results for sensitive files (admin.php, config.txt, backup.zip), outdated software, and informative messages.

Phase 2: Automated Vulnerability Scanning

Step 3: Burp Suite Professional Setup & Scan

- **Task:** Configure Burp as your proxy and launch a full active scan.
- **Actions:**
  1. Configure your browser to use Burp's proxy (127.0.0.1:8080).

2. Browse to https://pension.nasarawastate.gov.ng, accepting Burp's CA certificate.
3. In Burp, right-click on the site in **Target > Site map** and select **"Scan" > "Scan defined URLs"**.
4. In the scan configuration, ensure **"Audit checks - Active"** is selected. Launch the scan.
5. Monitor the results in the **Dashboard** tab. This will identify a range of issues like SQLi, XSS, and server misconfigurations.

Step 4: Specialized Scanning with Nuclei

- **Task:** Use Nuclei to check for specific known vulnerabilities.
- **Command:**

```
# Scan for a wide range of known vulnerabilities and exposures
nuclei -u https://pension.nasarawastate.gov.ng -o nuclei_scan.json -json
# Convert the JSON output to an HTML report for readability
python3 -m json.tool nuclei_scan.json > nuclei_scan_formatted.json
```

- **Review:** Nuclei is excellent for finding specific CVEs and misconfigurations in content management systems, frameworks, and servers.

Phase 3: Manual Testing & Exploitation Validation

Step 5: Manual Testing in Burp Suite

- **Task:** Manually probe for logic flaws and complex vulnerabilities that automated tools miss.
- **Actions:**
    1. **Authentication Testing:** Use Burp's **Intruder** to test the login form for weak passwords against a known username (if discovered) or for account lockout policies.
    2. **Session Management:** Log in, then use Burp's **Repeater** to see if session tokens are invalidated after logout or password change.
    3. **Input Validation:** Test all form fields (login, search, contact forms) in **Repeater** for SQL Injection (' OR 1=1--), XSS (<script>alert('XSS')</script>), and Command Injection (; whoami).

Step 6: SSL/TLS & Security Headers Assessment

- **Task:** Evaluate the encryption and client-side security settings.
- **Commands:**

Check SSL/TLS configuration for weaknesses

sslscan pension.nasarawastate.gov.ng > ssl_scan.txt

- **Action:** Use browser developer tools (F12 > Network > reload page > click on request > Headers) to check for missing security headers:
    - ✓ Strict-Transport-Security
    - ✓ Content-Security-Policy
    - ✓ X-Content-Type-Options
    - ✓ X-Frame-Options

Phase 4: Analysis, Reporting, and Compliance Mapping

Step 7: Triage and Risk Assessment
Create a comprehensive findings table.

Finding	Tool Source	OWASP Top 10	CVE	NIST CSF	PCI DSS	Risk (L/M/H)
SQL Injection in login.php	Burp Scanner	A03:2021-Injection	N/A	PR.AC-1, DE.CM-1	6.5.1	**High**
Missing HSTS Header	Manual Check	A05:2021-Misconfig	N/A	PR.DS-2	4.1, 6.5	**Medium**
Weak TLS 1.0 Enabled	SSLScan	A02:2021-Crypto Failures	N/A	PR.DS-2	4.1	**High**
Verbose Server Banner	Nmap	A01:2021-Broken Access Control	N/A	DE.CM-1	2.2.4	**Low**

Step 8: Drafting the Formal Report

To: Nasarawa State Pension Bureau Management
From: GRC Security Assessment Team

Date: [Date]
Subject: Report on Authorized Security Assessment of pension.nasarawastate.gov.ng

1. Executive Summary: An authorized comprehensive assessment was conducted on [dates]. The assessment revealed several critical and high-severity vulnerabilities that require immediate attention to protect member data and system integrity.

2. Methodology: Testing included automated vulnerability scanning (Burp Suite, Nuclei), manual penetration testing, and configuration review, all conducted from an external perspective.

3. Critical Findings:

- **SQL Injection Vulnerability:** A critical flaw was identified in the login mechanism that could allow attackers to extract sensitive member data from the database.
- **Weak Cryptographic Protocols:** The server supports outdated and insecure TLS protocols, weakening encryption for all users.

4. Compliance Implications: The identified findings constitute violations of multiple controls within the **NIST Cybersecurity Framework** and **PCI DSS** standards. The lack of strong encryption also raises concerns under the **Nigeria Data Protection Regulation (NDPR)**.

5. Recommended Remediation Timeline:

- **Immediate (Within 72 hours):** Address the SQL Injection vulnerability and disable weak TLS protocols.
- **Short-Term (Within 2 Weeks):** Implement missing security headers and configure a proper CSP policy.
- **Ongoing:** Institute a quarterly penetration testing and code review program.

6. Lab Conclusion
This lab provided a realistic experience of an authorized external security assessment. You have practiced the end-to-end process of testing, analysis, and reporting, directly linking technical findings to business risk and compliance requirements.

7. Deliverables
Please submit the following:

1. All scan output files (Nmap, Nikto, Nuclei, SSLScan).
2. **Screenshots** of critical vulnerabilities validated in Burp Suite (e.g., successful SQLi exploit).
3. The **Burp Suite Professional** project file.

4. Your completed **Risk Assessment Table**.
5. The full **Formal Report**.