Comprehensive Security Assessment Report

Prepared For: Connected Pakistan

Date: July 18, 2025

Prepared By: Haroon Allahdad (Auditor)

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to Connected Pakistan or facilitate attacks against Connected Pakistan's assets. Haroon Allahdad or Khyam Javed shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on the client's environment. Any changes made to the environment during the period of testing may affect the results of the assessment. This was a short 2 day security audit conduct with limited physical and human resources.

Table of Contents

7. Conclusion

8. Appendices

8.1. Vulnerability Metrics Diagrams

8.2. Raw Scan Outputs (External Reference)

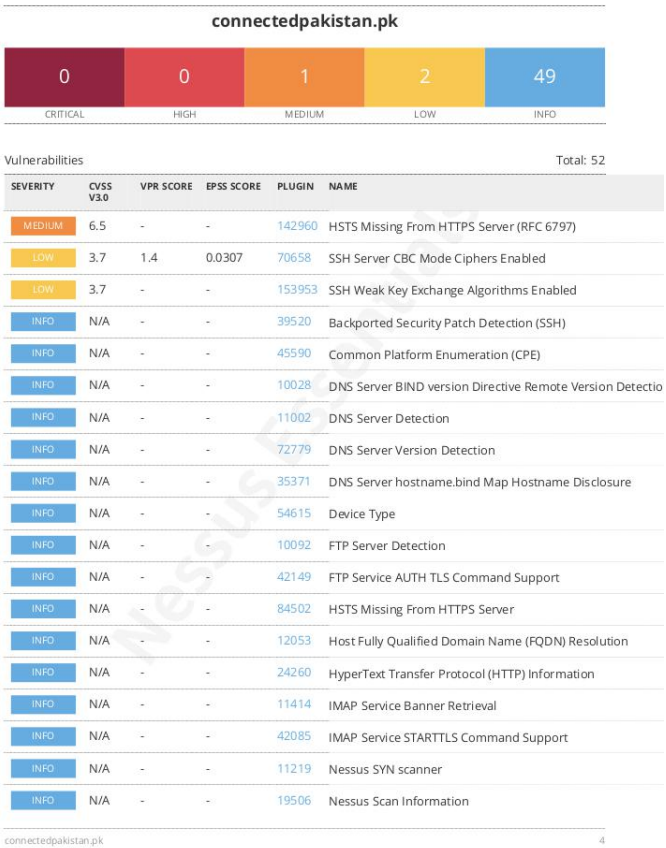
1. Executive Summary

- This report presents a comprehensive security assessment of Connected Pakistan's digital and physical security posture, integrating findings from web application scanning, network penetration testing, endpoint configuration analysis, and physical security observations. The assessment leveraged a multi-tool approach, incorporating data from Nessus, Nikto, a custom vulnerability scanning website, and a custom web pentesting application, alongside direct observations.

- The assessment identified a spectrum of vulnerabilities, ranging from critical to informational. Key areas demanding immediate attention include:
  - **Critical Data Leakage:** Direct exposure of Personally Identifiable Information (PII), including a credit card number, in web responses, posing an extreme data breach risk.
  - **Widespread Web Application Vulnerabilities:** Significant susceptibility to Cross-Site Request Forgery (CSRF) due to missing tokens, and increased risk of client-side attacks (XSS, clickjacking) due to the absence of crucial HTTP security headers (CSP, X-Frame-Options, HSTS).
  - **Network Exposure:** Public exposure of critical administrative interfaces (cPanel, WHM, Webmail) and mail services, broadening the external attack surface.
  - **Weak Cryptographic Configurations:** Use of deprecated SSH ciphers and weak key exchange algorithms, and advertising of discouraged SSL/TLS cipher suites across various services.

- **Information Disclosure:** Numerous instances of sensitive information leakage through robots.txt, sitemap.xml, directory listings, and server banners, aiding attacker reconnaissance.
- **Predictable Wi-Fi Password Patterns:** The observed Wi-Fi password policy follows a predictable pattern, making it susceptible to brute-force or dictionary attacks.
- **Physical Security Gaps:** While overall building security and surveillance are robust, a specific vulnerability was noted regarding unlocked employee rooms at night.

- Addressing these findings is paramount to safeguarding Connected Pakistan's data, maintaining operational integrity, preserving user trust, and ensuring compliance with relevant security standards. Immediate action is strongly recommended for critical and high-risk findings, followed by a structured remediation plan for all identified weaknesses.



connectedpakistan.pk

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	2	49

Vulnerabilities Total: 52

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detectio
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	42149	FTP Service AUTH TLS Command Support
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11414	IMAP Service Banner Retrieval
INFO	N/A	-	-	42085	IMAP Service STARTTLS Command Support
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

2. Introduction

2.1. Purpose of the Assessment

The purpose of this comprehensive security assessment is to identify, analyze, and report on security vulnerabilities and weaknesses present within Connected Pakistan's web application infrastructure, network environment, and physical security controls. This assessment aims to provide actionable recommendations to enhance the overall security posture, reduce the attack surface, and mitigate potential risks associated with various cyber and physical threats.

2.2. Scope of the Assessment

The scope of this assessment encompassed a multi-domain approach, focusing on the following key areas:

- **Web Application Assets:** Primary domain (https://connectedpakistan.pk/), associated subdomains, and services running on ehostpk.net (IP: 5.9.177.100), including administrative interfaces (cPanel, WHM, Webmail) and mail services. This also included the WordPress installation and underlying web server configurations.
- **Network Environment:** External network perimeter (public-facing IP addresses) and internal network segments (e.g., 192.168.18.0/24, 192.168.44.0/24, 192.168.122.0/24, 192.168.1.0/24), including active hosts, open ports, and running services.
- **Endpoint Configuration:** Assessment of a typical employee workstation's security configuration (e.g., Windows Defender status).
- **Physical Security:** On-site observation of physical access controls, surveillance systems, and internal security practices.

2.3. Methodology

A multi-faceted and ethical approach was employed to ensure comprehensive coverage and accurate findings, combining automated scanning with specialized tools and direct observation:

- **Reconnaissance & Scanning:**
  - **Nmap:** Utilized for extensive external and internal network scanning, including host discovery, port scanning, service version detection (-sV), and operating system identification (-O).
  - **Nessus:** Employed for comprehensive network and web application vulnerability scanning, including host-level and service-level checks, cryptographic configurations, and compliance.
  - **Nikto:** Used for web server and web application enumeration, focusing on common misconfigurations, outdated software, and known vulnerabilities.
  - **OWASP ZAP:** Used for comprehensive dynamic application security testing (DAST), including active and passive scanning for a wide range of web vulnerabilities.
  - **Crunch:** Employed for generating custom wordlists for password strength testing and brute-force scenarios.
  - **Custom Vulnerability Scanning Website:** Applied for dynamic application security testing (DAST), identifying vulnerabilities such as injection flaws, broken authentication, and security misconfigurations by actively interacting with the web application.
  - **Other Tools:** Various other specialized tools and scripts were used for targeted reconnaissance and vulnerability identification.

- **Penetration Testing (Limited & Demonstrative):**
  - **SEToolkit:** Used for demonstrating website cloning to illustrate phishing and typo-squatting attack vectors.
  - **Zphisher:** Utilized for demonstrating website cloning and phishing page generation capabilities.
  - Conceptual explanation of Wi-Fi cracking (Aircrack-ng/Hashcat) based on identified password patterns.

- **Configuration Review:** Manual and automated assessment of system and application configurations, including HTTP headers, firewall rules, and software update mechanisms.
- **Physical Security Assessment:** On-site observation and review of physical access controls, surveillance systems, and internal security protocols.
- **Information Gathering and Analysis:** Correlation of findings from various tools and observations, analysis of their cumulative impact, and prioritization based on risk.

3. Classification Definitions

To provide a clear understanding of the severity and impact of identified vulnerabilities, the following classification definitions are utilized:

3.1. Risk Classifications

- **Critical (Score 10):** The vulnerability poses an immediate and severe threat to the organization. Successful exploitation may permanently affect the organization's core operations, lead to massive data breaches, or complete system compromise. Remediation should be performed immediately.
- **High (Score 7-9):** The vulnerability poses an urgent threat to the organization. Successful exploitation could result in significant data loss, unauthorized access to sensitive systems, or major service disruption. Remediation should be prioritized.
- **Medium (Score 4-6):** Successful exploitation is possible and may result in notable disruption of business functionality, limited data exposure, or minor unauthorized access. This vulnerability should be remediated when feasible.
- **Low (Score 1-3):** The vulnerability poses a negligible or minimal threat to the organization. Exploitation might lead to minor information disclosure or slight operational inconvenience. The presence of this vulnerability should be noted and remediated if possible.
- **Informational (Score 0):** These findings have no clear direct threat to the organization but may cause business processes to function differently than

desired, reveal sensitive information about the company, or indicate areas for best practice improvement.

- **CVSS (Common Vulnerability Scoring System):** CVSS is an open and industry-standard framework for communicating the characteristics and impacts of IT vulnerabilities. It provides a numerical score (from 0.0 to 10.0) that can be translated into the qualitative risk ratings (Low, Medium, High, Critical) used above. The score is derived from metrics that assess the exploitability of the vulnerability and its impact on confidentiality, integrity, and availability.

3.2. Exploitation Likelihood Classifications

- **Likely:** Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
- **Possible:** Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
- **Unlikely:** Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

3.3. Business Impact Classifications

- **Major:** Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
- **Moderate:** Successful exploitation may cause significant disruptions to non-critical business functions.
- **Minor:** Successful exploitation may affect few users, without causing much disruption to routine business functions.

3.4. Remediation Difficulty Classifications

- **Hard:** Remediation may require extensive reconfiguration of underlying systems that is time-consuming. Remediation may require disruption of normal business functions.
- **Moderate:** Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
- **Easy:** Remediation can be accomplished in a short amount of time, with little difficulty.

4. High-Level Assessment Overview

4.1. Observed Security Strengths

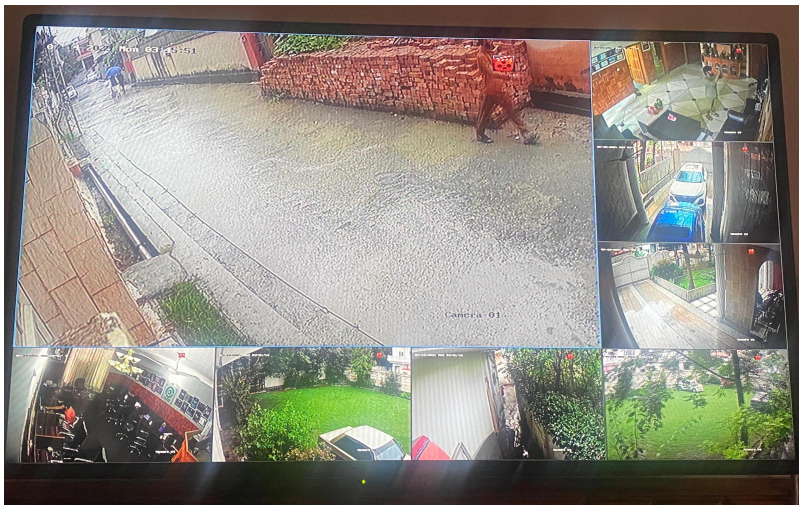
Connected Pakistan demonstrates several commendable security strengths across its infrastructure:

- **Robust Building Security:** The physical premises exhibit tight security measures, including strong access controls at entry points.
- **Exceptional Camera Surveillance:** The organization employs an advanced camera surveillance system, providing clear day footage and high-quality black and white clear footage at night, significantly enhancing physical monitoring capabilities.
- **Controlled Internal Endpoints:** Several internal network hosts (e.g., 192.168.18.13, 192.168.18.25, 192.168.1.85) appear to be well-protected by host-based firewalls, with no common open ports identified, indicating good endpoint security posture.
- **Denied Anonymous FTP:** The external FTP service explicitly denies anonymous login, preventing a common vector for unauthorized file access.
- **Managed External SMTP Access:** Ports 25 and 587 show tcpwrapped status, suggesting firewalling or rate-limiting is in place, which is a positive security measure for mail services.
- **HTTPS Enforcement:** The main website redirects HTTP traffic to HTTPS, demonstrating a commitment to encrypted web communication.

- **Hardened Website Administration:** Commendable security mechanisms and procedures are in place, particularly concerning the administration side of their website.

Viusal Evidence:

- **During Day:**



- **During Night:**

4.2. Areas for Improvement

Despite the strengths, several areas require significant improvement to bolster Connected Pakistan's overall security posture:

- **Extensive External Attack Surface:** A large number of open ports and exposed services, particularly administrative panels, create numerous potential entry points for attackers.

- **Web Application Vulnerabilities:** The web application is susceptible to critical data leakage, widespread CSRF, and various client-side attacks due to missing security headers and insecure configurations.
- **Weak Cryptographic Hygiene:** Outdated or weak cryptographic configurations across SSH and SSL/TLS services expose communication channels to compromise.
- **Information Disclosure:** Over-sharing of system and application details (e.g., server versions, file paths via robots.txt and directory listings) aids attacker reconnaissance.
- **Endpoint Configuration Gaps:** Issues with endpoint antivirus updates (Windows Defender path error) and a general organizational trend of predictable Wi-Fi password patterns.
- **Internal Physical Security:** Specific gaps were identified regarding the consistent locking of individual employee rooms at night.

5. Assessment Findings

This section details the specific vulnerabilities identified during the assessment, categorized by their assessed risk level.

5.1. Critical Risk Findings

5.1.1. PII Disclosure (Credit Card Number) (CWE-359)

- **Source:** Custom Vulnerability Scanning Website
- **Description:** The web application is directly disclosing Personally Identifiable Information (PII), specifically a Mastercard credit card number (5108880199188264) along with associated details (BIN, Brand, Issuer), within its responses.
- **Affected URL:** https://connectedpakistan.pk/cp-alumni/
- **Impact:** Major Business Impact (Severe Data Breach, Financial Fraud, Reputational Damage). This is an extremely critical data leakage, leading to immediate financial fraud, identity theft, and severe legal and reputational repercussions.
- **Exploitation Likelihood:** Likely

- **Remediation Difficulty:** Easy

5.2. High Risk Findings

5.2.1. Absence of Anti-CSRF Tokens (CWE-352)

- **Source:** Custom Vulnerability Scanning Website
- **Description:** Numerous HTML submission forms across the application lack proper Anti-CSRF tokens, making them vulnerable to Cross-Site Request Forgery attacks.
- **Affected URLs (Examples):** https://connectedpakistan.pk/become-a-member/, https://connectedpakistan.pk/blogstory/, https://connectedpakistan.pk/contact-us/, and 66 other instances.
- **Impact:** Moderate Business Impact (Unauthorized Actions, Account Takeover, Data Manipulation). High risk of unauthorized actions performed on behalf of authenticated users, compromising data integrity and user trust.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Moderate

5.2.2. Content Security Policy (CSP) Header Not Set

- **Source:** Custom Vulnerability Scanning Website, Nikto
- **Description:** The Content Security Policy (CSP) HTTP header, a critical security mechanism against XSS and data injection, is entirely missing from web responses.

- Affected URLs (Examples): https://connectedpakistan.pk/, and 461 other instances.
- **Impact:** Moderate Business Impact (Increased XSS Susceptibility, Data Injection). Without CSP, the application is highly vulnerable to XSS attacks, potentially leading to script injection, cookie theft, or website defacement.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Moderate

5.3. Medium Risk Findings

5.3.1. Missing Anti-clickjacking Header (X-Frame-Options)

- **Source:** Custom Vulnerability Scanning Website, Nikto
- **Description:** The X-Frame-Options HTTP header is missing from web responses, leaving the application susceptible to clickjacking attacks.
- **Affected URLs (Examples):** https://connectedpakistan.pk/, and 460 other instances.
- **Impact:** Minor Business Impact (Unauthorized User Actions, Information Disclosure). Users can be tricked into unintended actions on the legitimate site.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Easy

5.3.2. Cross-Domain Misconfiguration (CORS/Other Policy)

- **Source:** Custom Vulnerability Scanning Website
- **Description:** A cross-domain misconfiguration was identified, potentially due to overly permissive Cross-Origin Resource Sharing (CORS) policies related to a third-party JavaScript file.
- **Affected URL:** https://www.winaffiliatepro.com/wp-content/plugins/wp-affiliate-platform/js/jquery.dataTables.min.js
- **Impact:** Minor Business Impact (Potential Data Leakage, Unauthorized Interaction). Risk of unauthorized access to resources or data leakage from other domains.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Easy

5.3.3. HSTS Missing From HTTPS Server (RFC 6797)

- **Source:** Nessus, Nikto, Custom Vulnerability Scanning Website
- **Description:** The web server is not enforcing HTTP Strict Transport Security (HSTS), which forces secure HTTPS connections.

- **Affected Ports/URLs:** tcp/2083/www (cPanel), tcp/443/www (main website), and numerous pages on https://connectedpakistan.pk/.
- **Impact:** Minor Business Impact (Downgrade Attacks, SSL-Stripping, Cookie Hijacking). Creates a window for man-in-the-middle attacks where users might initially connect over insecure HTTP.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Moderate

5.4. Low Risk Findings

5.4.1. Exposed Administrative Portals (External Network)

- **Source:** Nmap (Network Penetration Testing)
- **Description:** Critical administrative interfaces (cPanel, WHM, Webmail) are directly accessible from the public internet.
- **Affected URLs:** https://5.9.177.100:2083/ (cPanel), https://5.9.177.100:2087/ (WHM), https://5.5.177.100:2096/ (Webmail).
- **Impact:** Minor Business Impact (Increased Attack Surface, Brute-Force Target). Broadens the attack surface for credential stuffing and platform-specific vulnerabilities.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Easy

5.4.2. Wi-Fi Password Pattern Vulnerability (Conceptual)

- **Source:** Network Penetration Testing (Reconnaissance)
- **Description:** The Wi-Fi password follows a predictable pattern (e.g., "Pakistan" followed by 1 to 5 digits), making it susceptible to dictionary or brute-force attacks.
- **Impact:** Moderate Business Impact (Internal Network Access, Data Exfiltration). A successful crack grants full access to the internal network.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Easy

- **Note:** Exploitation was not performed due to time and confidentiality constraints, but is theoretically 100% possible with appropriate tools.

5.4.3. Website Cloning and Typo Squatting Vulnerability (Demonstrative)

- **Source:** Network Penetration Testing (SEToolkit)
- **Description:** The Connected Pakistan website can be easily cloned using tools like SEToolkit, facilitating convincing phishing and typo-squatting attacks.
- **Impact:** Moderate Business Impact (Credential Theft, Malware Delivery, Reputational Damage). High risk of users being tricked into providing credentials or downloading malware.
- **Exploitation Likelihood:** Likely
- **Remediation Difficulty:** Easy

5.4.4. SSH Server CBC Mode Ciphers Enabled (CVE-2008-5161)

- **Source: Nessus**
- **Description:** The SSH server supports Cipher Block Chaining (CBC) encryption modes (aes128-cbc, aes256-cbc), which are considered less secure.
- **Affected Port:** tcp/22/ssh
- **Impact:** Minor Business Impact (Confidentiality Risk). Potential for plaintext recovery under specific conditions.

- **Exploitation Likelihood:** Unlikely
- **Remediation Difficulty:** Easy

5.4.5. SSH Weak Key Exchange Algorithms Enabled (RFC 9142)

- **Source:** Nessus
- **Description:** The SSH server allows weak key exchange algorithms, specifically diffie-hellman-group-exchange-sha1.
- **Affected Port:** tcp/22/ssh

- **Impact:** Minor Business Impact (Key Exchange Compromise). Weakens the key exchange process, potentially allowing session decryption.
- **Exploitation Likelihood:** Unlikely
- **Remediation Difficulty:** Easy

5.4.6. Cookie No HttpOnly Flag

- **Source:** Custom Vulnerability Scanning Website
- **Description:** Several cookies are missing the HttpOnly flag, making them accessible via client-side scripts.
- **Affected URLs (Examples):** https://connectedpakistan.pk/, https://connectedpakistan.pk/wp-comments-post.php
- **Impact:** Minor Business Impact (Session Hijacking Risk). Increases the risk of session hijacking if an XSS vulnerability exists.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Easy

5.4.7. Cookie without SameSite Attribute

- **Source:** Custom Vulnerability Scanning Website
- **Description:** Several cookies are missing the SameSite attribute, which helps protect against CSRF attacks.
- **Affected URLs (Examples):** https://connectedpakistan.pk/, https://connectedpakistan.pk/wp-comments-post.php
- **Impact:** Minor Business Impact (Weakened CSRF Protection). Weakens defense against CSRF attacks.
- **Exploitation Likelihood:** Possible
- **Remediation Difficulty:** Easy

5.5. Informational Risk Findings

5.5.1. Internal Network Host (192.168.44.135) - Directory Listing Enabled

- **Source:** Nmap (Internal Scan)

- **Description:** An internal web server on 192.168.44.135 (Port 5500/tcp) is configured to allow directory listing, exposing its file system contents.
- **Impact:** Information disclosure, aiding attacker reconnaissance.
- **Recommendations:** Disable directory listing immediately.

5.5.2. Cross-Domain JavaScript Source File Inclusion (CWE-829)

- **Source:** Custom Vulnerability Scanning Website
- **Description:** JavaScript files are included from external, third-party domains, introducing a supply chain risk.
- **Affected URLs (Examples):** https://stats.wp.com/e-202529.js, https://connect.facebook.net/signals/config/21235123123.js, https://www.google.com/recaptcha/api.js
- **Impact:** Risk of supply chain attacks if external scripts are compromised.
- **Recommendations:** Thoroughly vet third-party script providers, host critical scripts locally, or implement Subresource Integrity (SRI).

5.5.3. Timestamp Disclosure - Unix

- **Source:** Custom Vulnerability Scanning Website
- **Description:** Unix timestamps are disclosed in URLs or web content.
- **Affected URLs (Examples):** https://connectedpakistan.pk/wp-content/cache/wpo-minify/1752648739/assets/...
- **Impact:** Minor information disclosure, potentially aiding reconnaissance.
- **Recommendations:** Avoid exposing raw timestamps or obfuscate them.

5.5.4. X-Content-Type-Options Header Missing

- **Source:** Nikto, Custom Vulnerability Scanning Website
- **Description:** The X-Content-Type-Options HTTP header is missing, allowing browsers to "sniff" content types.
- **Impact:** Allows MIME-sniffing attacks, potentially leading to XSS.
- **Recommendations:** Implement X-Content-Type-Options: nosniff.

5.5.5. Web Server robots.txt Information Disclosure

- **Source:** Nessus, Nikto
- **Description:** The robots.txt file is publicly accessible and lists disallowed directories, potentially revealing sensitive paths.
- **Impact:** Provides attackers with a roadmap for reconnaissance.
- **Recommendations:** Review robots.txt contents; rely on proper access controls.

5.5.6. Web Application Cookies Are Expired

- **Source:** Nessus
- **Description:** Several HTTP cookies are set with an Expires attribute in the past, causing them to be immediately removed.
- **Impact:** Indicates a misconfiguration in cookie management, potentially affecting functionality.
- **Recommendations:** Review and configure cookie expiry dates correctly.

5.5.7. Web Server No 404 Error Code Check

- **Source:** Nessus
- **Description:** The web server does not consistently return 404 Not Found HTTP status codes for non-existent files, sometimes returning HTTP 301 instead.
- **Impact:** Can hinder automated scanning and mask true resource status.
- **Recommendations:** Configure the web server to return standard HTTP 404 Not Found responses.

5.5.8. SSL Certificate 'commonName' Mismatch

- **Source:** Nessus
- **Description:** The commonName in the SSL certificate for the FTP service (server.domaincontrol.pk) does not match the accessed hostname (connectedpakistan.pk).
- **Impact:** Can lead to user confusion and trust issues.
- **Recommendations:** Ensure certificates include the correct hostname in CN or SANs.

5.5.9. SSL Certificate Chain Contains Certificates Expiring Soon

- **Source:** Nessus
- **Description:** Multiple SSL certificates are expiring soon (within 60 days).
- **Impact:** Failure to renew will lead to service outages and security warnings.
- **Recommendations:** Initiate renewal process immediately; implement automated certificate management.

5.5.10. SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

- **Source:** Nessus
- **Description:** A root CA certificate in the SSL chain uses SHA-1, a cryptographically weak hashing algorithm.
- **Impact:** Raises concerns about cryptographic hygiene; may be flagged by modern tools.
- **Recommendations:** Migrate to certificates signed with stronger algorithms (SHA-256+).

5.5.11. SSL/TLS Recommended Cipher Suites

- **Source:** Nessus
- **Description:** Various SSL/TLS services advertise discouraged cipher suites.
- **Impact:** Allows attackers to force less secure encryption.

- **Recommendations:** Configure services to support only strong, modern cipher suites.

5.5.12. Server Leaks Version Information via "Server" HTTP Response Header Field (CWE-497)

- **Source:** Custom Vulnerability Scanning Website
- **Description:** The web/application server is disclosing specific version information via the "Server" HTTP header.

- **Impact:** Aids attackers in reconnaissance.
- **Recommendations:** Configure the web server to suppress or generalize the "Server" header.

5.5.13. Information Disclosure - Suspicious Comments

- **Source:** Custom Vulnerability Scanning Website
- **Description:** Suspicious comments (e.g., containing "admin") were found in the source code.
- **Impact:** Can provide internal system details or hints to attackers.
- **Recommendations:** Remove sensitive comments from source code.

5.5.14. User Controllable HTML Element Attribute (Potential XSS)

- **Source:** Custom Vulnerability Scanning Website
- **Description:** User-controlled values are reflected into HTML attributes without proper sanitization.
- **Impact:** Indicates a potential Cross-Site Scripting (XSS) vulnerability.
- **Recommendations:** Implement strict input validation and context-aware output encoding.

5.5.15. Re-examine Cache-control Directives

- **Source:** Custom Vulnerability Scanning Website
- **Description:** The Cache-control header is improperly set or missing, potentially allowing sensitive content to be cached.
- **Impact:** Risk of sensitive information being retrieved from caches.
- **Recommendations:** Set appropriate Cache-Control headers for sensitive and static content.

5.5.16. WordPress Specific Files & Installation Confirmed

- **Source:** Nikto
- **Description:** Presence of wp-links-opml.php and license.txt reveals WordPress installation and version.

- **Impact:** Simplifies finding and exploiting known WordPress vulnerabilities.
- **Recommendations:** Regularly update WordPress core, themes, and plugins; secure/remove sensitive files.

5.6. Physical Security Findings

- **Observation:** Connected Pakistan exhibits robust overall building security, including tight access controls at entry points and exceptional camera surveillance with clear day footage and high-quality black and white clear footage at night.
- **Finding:** While the main building security is strong, it was observed that individual employee rooms are not consistently locked at night.
- **Impact:** This presents a potential internal physical security vulnerability. Unauthorized access to employee rooms could lead to theft of sensitive documents, access to unattended workstations, or placement of malicious devices, even if the main building is secure.
- **Recommendations:**
  - **Policy Review:** Review existing physical security policies to determine if locking employee working rooms at night is a mandated procedure.
  - **Awareness & Enforcement:** If it is policy, reinforce employee awareness regarding the importance of securing their individual workspaces, especially at the end of the day. Implement measures to ensure compliance.

_x0006_ **Consideration of Implementation:** If not currently policy, evaluate the feasibility and benefits of implementing a policy requiring employees to lock their rooms at night, weighing it against operational needs and employee convenience. This enhances the layered security approach.

6. Consolidated Recommendations

This section provides a consolidated and prioritized list of recommendations to address all identified vulnerabilities and enhance Connected Pakistan's overall security posture.

6.1. Immediate Action (Critical & High Risk)

_x0006_ **Eliminate PII Disclosure:** Immediately identify and remediate the source of credit card number disclosure on https://connectedpakistan.pk/cp-alumni/. Implement strict data masking, encryption, or complete removal of sensitive data from public-facing responses.

_x0006_ **Implement Anti-CSRF Tokens:** Integrate robust Anti-CSRF token mechanisms into all web forms and state-changing requests to prevent Cross-Site Request Forgery attacks.

_x0006_ **Enforce Content Security Policy (CSP):** Configure a strict CSP header to whitelist trusted content sources, significantly mitigating XSS and data injection vulnerabilities. Begin with Report-Only mode to refine the policy before full enforcement.

_x0006_ **Implement HSTS:** Configure the Strict-Transport-Security header with an appropriate max-age for all HTTPS services, including the main website and administrative panels, to enforce secure connections and prevent downgrade attacks.

6.2. High Priority Remediation (Medium Risk)

_x0006_ **Implement Anti-Clickjacking Headers:** Add X-Frame-Options: DENY or SAMEORIGIN to all web pages to protect against clickjacking attacks.

_x0006_ **Correct Cross-Domain Configurations:** Review and restrict Cross-Origin Resource Sharing (CORS) policies to only explicitly trusted domains to prevent unauthorized resource access.

6.3. Medium Priority Remediation (Low Risk)

_x0006_ **Restrict Access to Administrative Portals:** Implement strict firewall rules to restrict access to cPanel, WHM, Webmail, SSH, and other custom admin portals

(8887, 8888) to only trusted IP addresses (e.g., specific office IPs, VPN users). Consider placing these behind a VPN.

_x0006_ **Strengthen Wi-Fi Password Policy:** Immediately change the Wi-Fi password to a strong, complex, and entirely random passphrase (minimum 16 characters). Enforce regular password changes and consider WPA3.

_x0006_ **Mitigate Website Cloning & Typo Squatting:** Implement proactive domain monitoring for similar domains and reinforce continuous employee security awareness training on URL verification and phishing.

_x0006_ **Harden SSH Configuration:** Disable CBC mode ciphers and weak key exchange algorithms on the SSH server. Prioritize modern, strong cryptographic algorithms.

_x0006_ **Secure Cookie Attributes:** Ensure all sensitive cookies have the HttpOnly and SameSite attributes set appropriately (Lax or Strict) to mitigate XSS and CSRF risks.

_x0006_ **Review Cross-Domain Script Inclusions:** Vet all third-party script providers. Host critical scripts locally where possible, or implement Subresource Integrity (SRI) for external scripts from trusted CDNs.

_x0006_ **Implement X-Content-Type-Options:** Add X-Content-Type-Options: nosniff header for all web pages and static assets.

6.4. Ongoing Maintenance & Best Practices (Informational Risk & General)

_x0006_ **Internal Network Hardening:** Identify and harden all internal network devices and IoT devices (like IP cameras/NVRs). Change all default credentials, remove default pages/services, and implement network segmentation. Review UPnP usage.

_x0006_ **Resolve Windows Defender Update Issue:** Investigate and resolve the Windows Defender path error on employee workstations to ensure signature updates are functioning correctly.

_x0006_ **Review robots.txt and 404 Handling:** Audit robots.txt for unintended disclosures and ensure consistent HTTP 404 Not Found responses for non-existent resources.

_x0006_ **Manage SSL/TLS Certificates:** Address commonName mismatches, implement robust certificate lifecycle management, and replace SHA-1 signed certificates with stronger alternatives.

_x0006_ **Harden Cipher Suites:** Configure all SSL/TLS services to support only strong, modern, and recommended cipher suites, disabling all weak and deprecated ones.

_x0006_ **WordPress Hardening:** Regularly update WordPress core, themes, and all plugins. Remove or secure wp-links-opml.php and license.txt. Implement WordPress security plugins and hardening best practices.

_x0006_ **Input Validation and Output Encoding:** Continuously enforce comprehensive input validation and context-aware output encoding across the entire application to prevent injection and XSS vulnerabilities.

_x0006_ **Error Handling & Information Disclosure:** Configure applications and web servers to provide generic error messages to users and suppress server version information in HTTP headers. Remove sensitive comments from source code.

_x0006_ **Re-examine Cache-control Directives:** Set appropriate Cache-Control headers for sensitive content and static assets.

_x0006_ **Implement a Web Application Firewall (WAF):** Consider deploying a WAF to provide an additional layer of protection against common web attacks.

_x0006_ **Security Development Lifecycle (SDL):** Integrate security best practices into the entire SDLC for any custom application development.

_x0006_ **Physical Security Enhancements:**

- Review and enforce existing policies regarding the locking of individual employee rooms at night.
- If not policy, evaluate the feasibility and benefits of implementing such a policy to enhance layered physical security.
- Reinforce employee awareness regarding the importance of securing their individual workspaces.

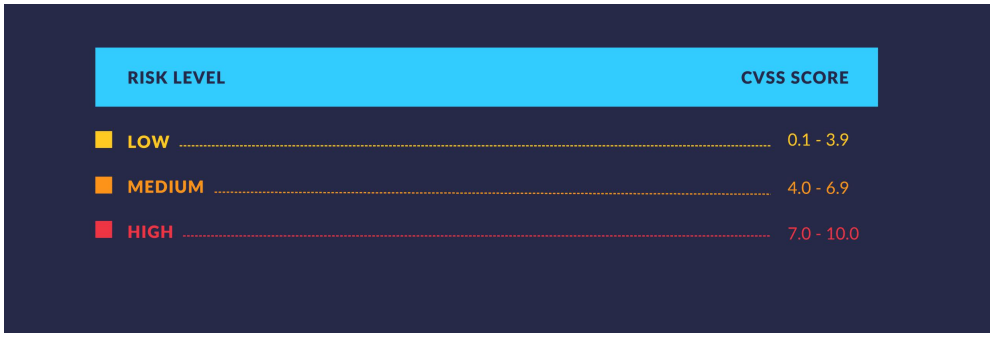
7. Conclusion

- This comprehensive security assessment has identified a range of vulnerabilities across Connected Pakistan's web application, network infrastructure, and physical security controls. From critical data leakage and widespread web application weaknesses to network exposures and internal physical security gaps, the findings highlight areas that demand immediate and strategic attention.
- Connected Pakistan has demonstrated commendable security mechanisms and procedures, particularly concerning the administration side of their website and overall building security with advanced surveillance. Nonetheless, the identified vulnerabilities, especially the critical PII disclosure and pervasive CSRF issues, pose significant risks to data confidentiality, integrity, and availability, as well as to the organization's reputation and compliance standing.
- By systematically implementing the prioritized recommendations outlined in this report, Connected Pakistan can significantly enhance its overall security posture, reduce its attack surface, protect sensitive data, and build greater trust with its users and stakeholders. Continuous monitoring, regular security assessments, and a proactive adherence to secure development and operational practices are essential for maintaining a robust defense in the evolving threat landscape.

8. Appendices

8.1. Vulnerability Metrics Diagrams

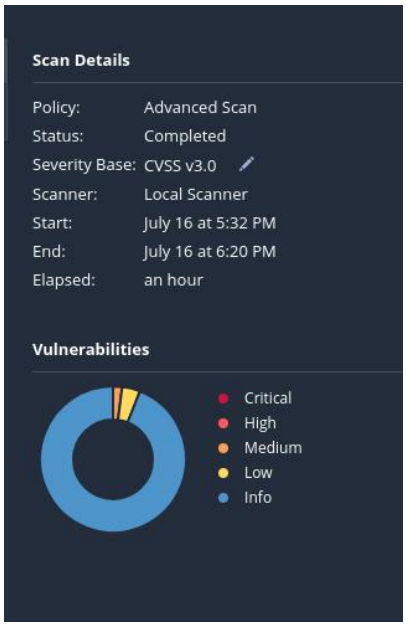
Figure 8.1.1: Vulnerability Distribution by Severity (Bar Chart)



(Credit belongs to NowSecure for this diagram)

Additionally Blue is reserved for informational risks in CVSS Score and their score is at 0. They are basically the public information that we shared on our web, it may be used against us, but it is also important for user-friendliness of the clients.

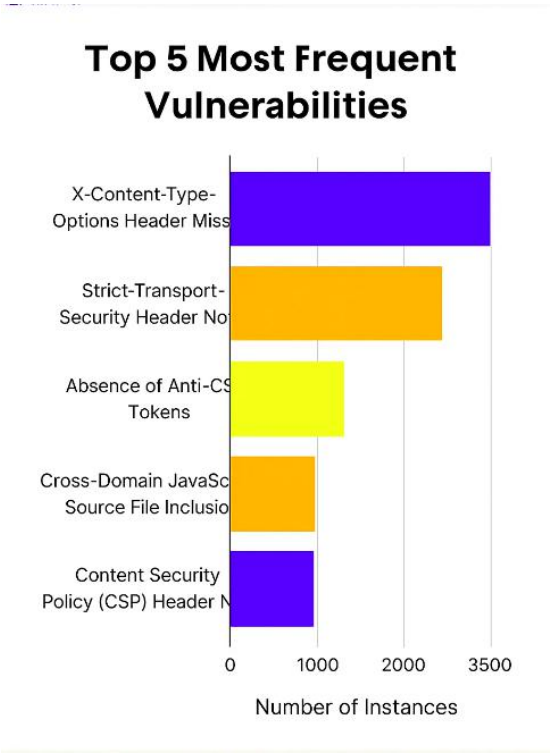
Figure 8.1.2: Vulnerability Distribution by CVSS Base Score (Pie Chart)



(Taken from Nessus, is a scan report pie chart of Connected Pakistan Website)

94% Informational CVSS Risk (No Risk), 4% Low CVSS Risks, 2% Medium CVSS Risks

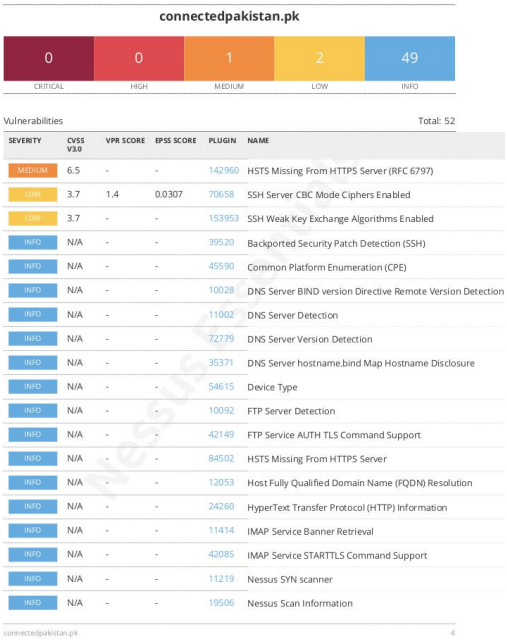
Figure 8.1.3: Top 5 Most Frequent Web Application Vulnerabilities (Bar Chart)



(Custom bar made from the vulnerabilities found for Connected Pakistan)

This is a bar chart showing the count of instances for the most frequently occurring vulnerabilities. It also shows their risk, by which the client company (Connected Pakistan can decide, which vulnerability to recover first).

Figure 8.1.4: Nessus Vulnerability Summary Diagram



connectedpakistan.pk

0	0	1	2	49
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 52

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	42149	FTP Service AUTH TLS Command Support
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11414	IMAP Service Banner Retrieval
INFO	N/A	-	-	42085	IMAP Service STARTTLS Command Support
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

(This is the report chart taken from nessus report of the Connected Pakistan)

A high-level summary diagram from the Nessus report, it also shortly states the highlighted ulnerabilities found during the Nessus scan of the Connected Pakistan's website (https://connectedpakistan.pk/)

8.2. Raw Scan Outputs (External Reference)

Full raw outputs from the following tools are available for detailed review and are referenced in this report:

Nessus Scan Report:

[https://drive.google.com/file/d/1xLf8nI7WsEaXiAR8JsZWxiAiO8BUFk_8/view?usp=sharing]

Nikto Scan Output:

[https://drive.google.com/file/d/19x30A1B7E64i0GcA8hUu7cOiV2jk14c7/view?usp=sharing]

OWASP ZAP Report:

[https://drive.google.com/file/d/1JKbSVhOPJoNOYmKnqOW32OJBgrpkZe1j/view?usp=sharing]

Custom Web Pentesting Application Logs:

[https://drive.google.com/file/d/1xLf8nI7WsEaXiAR8JsZWxiAiO8BUFk_8/view?usp=sharing]

Nmap Scan Logs (External & Internal):

[https://drive.google.com/file/d/1azlu_Y3j7mDdG4FMJqL6AHUyBQD62H6m/view?usp=sharing]

Security Audit Completion Signatures

We, the undersigned, certify that this Comprehensive Security Assessment Report accurately reflects the findings and recommendations of the security audit conducted for Connected Pakistan on July 16-17, 2025. This audit is hereby concluded, and it is mutually acknowledged that no further compensation is due to the auditors, nor shall the auditors be held liable by the Company for the implications of any future security breaches.

For Connected Pakistan:

Haseeb Ali
Director Admin & Partnerships

Signature: _____

Date: _____

Malik Umar
Project Manager Connected Pakistan

Signature: _____

Date: _____

For the Security Audit Team:

Haroon Allahdad
Primary Auditor

Signature: _____

Date: _____

Khyam Javed
Support Auditor, Communicator & Presenter

Signature: _____

Date: _____