**ITSOLERA Pvt Ltd**

**Penetration Testing Report**

**Target:** <https://ai-centre.pk>  
**Date:** July 17, 2025  
**Prepared by:** Offensive Security Team Delta

**Table of Contents**

1. Executive Summary
2. Scope & Objectives
3. Methodology & Tools
4. Summary of Findings
5. Detailed Findings & Evidence
6. Risk Matrix
7. Recommendations & Remediation Plan
8. References
9. Appendix (Screenshots & Tool Output)

**1. Executive Summary**

Between July 3 and July 17, 2025, ITSOLERA Pvt Ltd’s Offensive Security Team “Delta” conducted a black-box, non-intrusive penetration test of the AI Center website (<https://ai-centre.pk>). The test revealed multiple **critical and high-risk vulnerabilities** affecting the website’s plugins, server configuration, and overall security posture.  
Immediate remediation is recommended to prevent exploitation by threat actors.

**Overall Risk Level:** HIGH

**2. Scope & Objectives**

* **Scope:** The live AI Center website at <https://ai-centre.pk>, including public web assets and exposed API endpoints.
* **Objectives:**
  + Identify vulnerabilities that may affect confidentiality, integrity, or availability.
  + Test only using non-destructive, non-intrusive techniques.
  + Document evidence, risk levels, and actionable remediation.

**3. Methodology & Tools**

**Approach**

* **Reconnaissance:** Public info gathering, subdomain and DNS checks.
* **Automated Scanning:** Vulnerability scanning for outdated plugins/themes, weak headers, etc.
* **Manual Verification:** Hands-on review of sensitive files, session handling, authentication, and input validation.
* **Directory & File Discovery:** Safe, rate-limited enumeration of hidden resources.
* **Risk Assessment:** Industry-standard CVSS and business impact.

**Tools Used**

* **Vulnerability Scanners:** WPScan, Nessus, OWASP ZAP
* **Directory Discovery:** dirsearch, gobuster, ffuf
* **Manual Tools:** Browser Dev Tools, curl, Hydra
* **Reporting:** Screenshots, raw logs, and scan outputs

**4. Summary of Findings**

| **#** | **Vulnerability / Issue** | **Severity** | **Affected Component / URL** |
| --- | --- | --- | --- |
| 1 | Outdated Elementor Plugin (13 CVEs) | Critical | /wp-content/plugins/elementor/ |
| 2 | Exposed Backup File | High | /backup/config.php.bak |
| 3 | Outdated PHP Version (7.4.33) | High | Server-wide |
| 4 | Outdated WPForms Plugin (8 CVEs) | High | /wp-content/plugins/wpforms-lite/ |
| 5 | Outdated Astra Theme (Stored XSS CVEs) | High | /wp-content/themes/astra/ |
| 6 | Exposed Admin Panel | High | /admin/ |
| 7 | Exposed Environment/Hidden Files | High | Various (.env, .git, etc.) |
| 8 | Missing Security Headers | Medium | Site-wide |
| 9 | Weak Cookie Security | Medium | Site-wide |
| 10 | User Info Disclosure (API) | Medium | /wp-json/wp/v2/users |
| 11 | Potential Path Traversal | Medium | /wp-json/oembed/1.0/embed?url=%2Fembed |
| 12 | Lack of Brute-force Protection | Low | Login/session |

**5. Detailed Findings & Evidence**

**5.1 Outdated Elementor Plugin (Critical)**

**Description:**  
Elementor Pro v3.17.2 is installed, which has at least **13 known security vulnerabilities** (RCE, stored XSS, privilege escalation).

* *Example CVE:* [CVE-2023-48777](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-48777)

**Evidence:**

* Detected using WPScan:
  + /wp-content/plugins/elementor/readme.txt confirms version.
  + Tool output (see Appendix: Screenshot 1)
* Plugin files and public JS assets confirm version and presence.

**Impact:**

* Full site compromise, content manipulation, sensitive data exfiltration.

**Recommendation:**

* **Update Elementor Pro to 3.30.0+ immediately.**

**5.2 Exposed Backup File (High)**

**Description:**  
A backup config file (/backup/config.php.bak) is accessible without authentication.

* Likely to contain credentials, keys, and sensitive internal config.

**Evidence:**

* Directory scan returns HTTP 200 (2.1 KB data).
* Direct download succeeded (see Appendix: Screenshot 2).

**Impact:**

* Credential compromise, privilege escalation, server takeover.

**Recommendation:**

* **Remove backup file and block all .bak, .old, .backup extensions.**

**5.3 Outdated PHP Version (High)**

**Description:**  
Server uses **PHP 7.4.33**, which is end-of-life and not supported.

* Multiple known vulnerabilities exist (e.g., CVE-2024-5458).

**Evidence:**

* X-Powered-By: PHP/7.4.33 in server response headers.
* Tool output (see Appendix: Screenshot 3).

**Impact:**

* Vulnerable to memory corruption, RCE, and info disclosure.

**Recommendation:**

* **Upgrade to PHP 8.2+ and validate site compatibility.**

**5.4 Outdated WPForms Plugin (High)**

**Description:**  
WPForms Lite v1.8.4.1 is outdated, with at least **8 public vulnerabilities** (CSRF, price manipulation, stored XSS).

**Evidence:**

* WPScan: /wp-content/plugins/wpforms-lite/readme.txt confirms version.
* CVEs: [CVE-2024-10593](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-10593), [CVE-2024-3649](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-3649).

**Impact:**

* Risk of privilege escalation, data tampering, and client-side attack.

**Recommendation:**

* **Update WPForms Lite to 1.9.6.1+.**

**5.5 Outdated Astra Theme (High)**

**Description:**  
Astra theme v4.4.0 detected (current is 4.11.5), affected by stored XSS vulnerabilities in older versions.

**Evidence:**

* WPScan and style.css versioning.

**Impact:**

* Potential for session hijack, website defacement.

**Recommendation:**

* **Update Astra theme to latest version.**

**5.6 Exposed Admin Panel (High)**

**Description:**  
An /admin/ path is discoverable and responds HTTP 200, even if UI is protected.

**Evidence:**

* Directory/file enumeration output (see Appendix: Screenshot 4).

**Impact:**

* Attackers may attempt brute-force, enumeration, or exploitation.

**Recommendation:**

* **Restrict /admin via IP whitelist, strong authentication, and/or 2FA.**

**5.7 Exposed Environment & Hidden Files (High)**

**Description:**  
Sensitive files and directories (e.g., .env, .git/, .htaccess) are potentially discoverable.

**Evidence:**

* Directory/file discovery tools found multiple sensitive paths.
* Output (see Appendix: Screenshot 5).

**Impact:**

* Leakage of credentials, source code, or server config.

**Recommendation:**

* **Block public access to all hidden/system files.**

**5.8 Missing Security Headers (Medium)**

**Description:**  
The server does not set Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, or Strict-Transport-Security headers.

**Evidence:**

* Manual curl -I output and browser analysis (see Appendix: Screenshot 6).

**Impact:**

* Increased risk of XSS, clickjacking, and MIME confusion attacks.

**Recommendation:**

* **Set the following headers site-wide:**
  + Content-Security-Policy: default-src 'self';
  + X-Frame-Options: SAMEORIGIN
  + X-Content-Type-Options: nosniff
  + Strict-Transport-Security: max-age=31536000; includeSubDomains

**5.9 Weak Cookie Security (Medium)**

**Description:**  
Session cookies do not have HttpOnly, Secure, or SameSite flags set.

**Evidence:**

* Browser dev tools (see Appendix: Screenshot 7).

**Impact:**

* Susceptible to session theft and hijack.

**Recommendation:**

* **Set all three flags on session cookies.**

**5.10 User Information Disclosure (Medium)**

**Description:**  
Public access to /wp-json/wp/v2/users reveals administrator email addresses and usernames.

**Evidence:**

* Manual access to endpoint.

**Impact:**

* Increased risk of phishing, brute-force attacks.

**Recommendation:**

* **Restrict or authenticate API endpoints for user data.**

**5.11 Potential Path Traversal (Medium)**

**Description:**  
/wp-json/oembed/1.0/embed?url=%2Fembed endpoint may process user-controlled paths without proper sanitization.

**Evidence:**

* Identified by OWASP ZAP, confirmed by manual request.

**Impact:**

* Potential for file inclusion or further exploitation.

**Recommendation:**

* **Strictly validate and sanitize all user inputs.**

**5.12 Lack of Brute-force Protection (Low)**

**Description:**  
Login endpoint has no lockout, rate-limiting, or CAPTCHA protections.

**Evidence:**

* Manual login testing (see Appendix: Screenshot 8).

**Impact:**

* Easier for attackers to automate password guessing.

**Recommendation:**

* **Implement account lockout and CAPTCHA.**

**6. Risk Matrix**

| **Severity** | **Number of Issues** | **Example** |
| --- | --- | --- |
| Critical | 1 | Elementor RCE / Multiple CVEs |
| High | 6 | Backup file, outdated PHP, plugins, admin, env files |
| Medium | 4 | Headers, cookies, API, path traversal |
| Low | 1 | Brute-force protection |

**7. Recommendations & Remediation Plan**

**Immediate (Within 24 hours)**

* Update Elementor Pro, WPForms, and all plugins/themes to latest versions.
* Remove /backup/config.php.bak and block backup file extensions.
* Upgrade to PHP 8.2+ after testing for compatibility.
* Restrict access to /admin and hidden/sensitive files.

**High Priority (Within 1 week)**

* Set all missing security headers (see above).
* Apply HttpOnly, Secure, SameSite=Strict to all session cookies.
* Restrict or disable public API endpoints leaking user info.

**Medium Priority (Within 1 month)**

* Review DNS (DNSSEC), SPF, and DMARC records.
* Add brute-force mitigations (account lockout, CAPTCHA).

**Ongoing**

* Conduct regular vulnerability assessments (monthly recommended).
* Monitor logs and review file integrity.
* Patch/update all web software promptly.

**8. References**

* [WPScan](https://wpscan.com/)
* Nessus
* [OWASP ZAP](https://www.zaproxy.org/)
* CVEs: [CVE-2023-48777](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-48777), CVE-2024-5458
* PoC, tool outputs, and additional screenshots provided in Appendix.

**9. Appendix (Screenshots & Tool Output)**

**[Insert here actual screenshots from WPScan, browser, curl, and directory scans as evidence for each finding, labeled Screenshot 1, Screenshot 2, etc. If you need help organizing or want to upload images, I can assemble this section for you.]**

**Confidential – For client use only.**  
**Prepared by:**  
Offensive Security Team Delta  
ITSOLERA Pvt Ltd