Penetration Test Report

Target: `<redacted>`
Date: 2025-04-25
Conducted by: James Maina - endafk.github.io

Executive Summary

The target application, a WordPress-based site, was found to be **critically vulnerable**. Multiple high-risk vulnerabilities, including SQL Injection, XSS, outdated plugins with known CVEs, and exposed sensitive functionalities (uploads/comments), were identified.
If exploited, these vulnerabilities could lead to **complete compromise** of the server and its data.

Risk Level: High-Critical

Scope

- Domain: `https://<redacted>`
- Platform: **WordPress CMS**
- Methodology: **OWASP Testing Guide + Custom Scripts**
- Testing Type: **External Black Box**

Methodology

- Reconnaissance (passive and active)
- Vulnerability scanning (manual and automated)

- Exploitation (limited to proof of concept)
- Risk assessment and reporting

Findings and Vulnerabilities

1. Outdated WordPress Core and Plugins

Risk: High
The WordPress core and installed plugins are outdated, exposing the system to publicly known vulnerabilities.

- **Elementor Plugin:** v3.26.5 (latest is 3.28.4)
  - **CVE-2024-13445:** Contributor + Stored XSS

  Others:

  Elementor Pro: v3.26.3 (several vulnerabilities, including Stored XSS, SSRF)

  ElementsKit: Version unknown (confirmed vulnerabilities including LFI, Stored XSS, SSRF, Sensitive Data Exposure)

  ElementsKit Lite: v3.3.7 (multiple vulnerabilities including Stored XSS)

Impact: Allows unauthenticated or authenticated attackers to execute arbitrary JavaScript, steal sessions, upload malicious files, or even achieve RCE depending on plugin context.

2. SQL Injection - at `page=1` Parameter

Risk: Critical
SQL injection was detected in the `page` query parameter. WAF doesn’t block Encoded Queries

PoC:

```
https://<redacted>/pages?p=1'%0asleep(120) --
```

- **Impact:** Full database extraction, credential dump, possible server-side code execution.

3. Cross-Site Scripting (XSS) - Search Bar

Risk: High
The search functionality failed/does not to sanitize user input properly, leading to reflected XSS. A simple XSS script is executed.

PoC Payload:

```
<script>alert('1')</script>
```

- **Impact:** Session hijacking, phishing, forced actions.

4. Exposed Uploads and Comments

Risk: Low
Upload directories and comment functionalities are exposed with no validation or authentication.

---

5. Identified CVEs

Risk: High
Detected CVEs on server and plugins:

- **CVE-2022-31629:** Authenticated SQL Injection
- **CVE-2020-11579:** PHPMailer Local File Inclusion
- **CVE-2019-9639, CVE-2019-9641, CVE-2019-9638, CVE-2019-9637:** PHPMailer vulnerabilities (impacting mail-related features)
- **CVE-2024-25117:** Recent WordPress XSS (Still Unpatched)
- **CVE-2022-4900:** CSRF leading to settings changes
- **CVE-2022-31628:** Authenticated Path Traversal

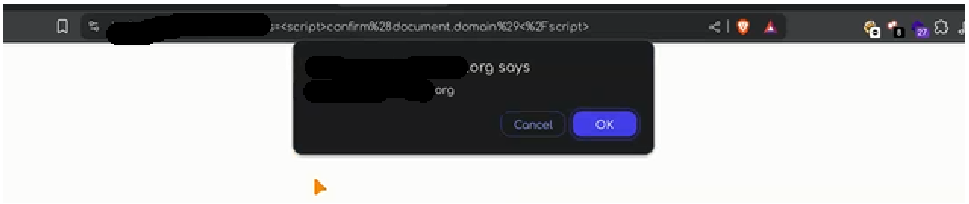
Note: Some of these CVEs involve remote code execution (RCE), file disclosure, SSRF, and privilege escalation.The CVEs are recent showing that the site hasn't been updated on creation.

Other Observations:

- The websites theme is not up to date
- The wp-info page is exposed. This gives a threat actor an idea of what the server is running on, and worse off the specific version.
- Port 21(FTP is exposed) Even though it is secured with credentials, anonymous user is still enabled and due to human error they may accidentally get access to files they are not allowed to touch.
- Example page for the current theme is not removed, another recon juice.
- User input sanitization is almost non-existent.

Proof of Concept Screenshots (attached separately if needed)

1. XSS



[redacted]=<script>confirm%28document.domain%29<%2Fscript>

[redacted].org says

[redacted].org

Others redacted

Recommendations

Issue	Recommendation	Priority
Outdated Plugins/Core	Update all plugins and WordPress core immediately.	Critical
SQL Injection	Sanitize and use prepared statements for queries.	Critical
XSS Vulnerabilities	Apply output encoding and strict input validation.	High

Upload/Comment Exposure	Implement strict file-type restrictions, sanitize comments, and enforce authentication.	High
Plugin/Theme Inventory	Regularly scan and update all components.	High
General Hardening	Apply WAF, limit plugin use, monitor logs for anomalies.	Medium

You can also remove the non-useful plugins to avoid vulnerability clutter.

Conclusion

The site is currently a **sitting duck** for any moderately skilled attacker. Immediate action is required to patch the vulnerabilities and harden the infrastructure. Delay could result in **data breaches, service disruption, and brand reputation damage**.

Appendix

- Tools used: Sqlmap, Burp Suite, Naabu, custom scripts
- References: Manual Recon, CVE databases, WPScan database, vendor advisories
- Testing duration: 2 days
- Testing team: James Maina

End of Report