Detect potential vulnerabilities (misconfigurations, outdated software, CVEs).

Executive Summary

The assessment identified **multiple critical vulnerabilities**, primarily stemming from severely **outdated software** with known, exploitable CVEs. The most significant finding is the presence of an **end-of-life PHP version (8.1.2)** and an **outdated Apache server (2.4.52)**, which together expose the server to remote code execution and request smuggling attacks. Furthermore, the server hosts a known vulnerable application (bWAPP), amplifying the attack surface.

---

1. Critical Vulnerabilities (CVEs) in Software Stack

1.1. Apache HTTP Server 2.4.52 - Multiple CVEs

Finding: The server is running Apache 2.4.52, released in January 2022. This version is outdated and contains numerous published vulnerabilities.

Detected CVEs (Sample):

- **CVE-2022-28330 (CVSS: 7.5 - High):** A critical vulnerability in mod_proxy_uj that allows HTTP Request Smuggling. This can lead to cache poisoning, session hijacking, and bypass of security controls.
- **CVE-2022-28614 (CVSS: 6.8 - Medium):** A flaw in the mod_lua module that could lead to a crash (DoS) or potential information disclosure.
- **CVE-2022-28615 (CVSS: 6.8 - Medium):** Another vulnerability in mod_lua related to crafted client requests causing a server crash.

Tool Evidence:

- **Nikto:** Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). Apache 2.4.52 is earlier than 2.4.53, a critical vulnerability may exist (CVE-2022-28330).
- **HTTP Header:** Server: Apache/2.4.52 (Ubuntu)

Impact: An attacker could exploit these vulnerabilities to bypass security mechanisms, crash the server, or steal sensitive data.

1.2. PHP 8.1.2 - End-of-Life with Known CVEs

Finding: The server is running PHP 8.1.2, which reached end-of-life (EOL) on **January 6, 2023**. This means it no longer receives security updates, leaving it exposed to all vulnerabilities discovered since that date.

Detected CVEs (Sample from 8.1.2 and prior):

- **CVE-2022-31629 (CVSS: 9.8 - Critical):** An integer overflow in password_verify() could lead to a heap overflow, potentially resulting in remote code execution.
- **CVE-2022-31630 (CVSS: 8.6 - High):** A stack overflow in xmlutf8_encode() could cause a denial-of-service or worse.
- Numerous other CVEs related to buffer overflows, use-after-free errors, and other memory corruption issues patched in later versions.

Tool Evidence:

- **HTTP Header:** X-Powered-By: PHP/8.1.2-1ubuntu2.14
- **WhatWeb:** PHP[8.1.2-1ubuntu2.14]

Impact: The most severe impact is **Remote Code Execution**, allowing an attacker to take complete control of the web server.

---

2. Misconfigurations & Security Hygiene

2.1. Information Disclosure

Finding: The server is configured to leak sensitive information about its software stack, greatly aiding attackers in vulnerability targeting.

Evidence:

- **Server Banner:** Server: Apache/2.4.52 (Ubuntu) provides exact version and OS.
- **PHP Banner:** X-Powered-By: PHP/8.1.2-1ubuntu2.14 provides exact PHP version and build.
- **Source Code:** <!-- bWAPP, version 2.2 --> confirms the vulnerable web app version.

Impact: Attackers can immediately search for and launch exploits specific to Apache 2.4.52 and PHP 8.1.2 without any guesswork.

2.2. TLS/SSL Misconfiguration

Finding: The SSL/TLS configuration supports deprecated and weak protocols.

Evidence (from testssl.sh):

- **TLS 1.0 and 1.1 are enabled.** These protocols are deprecated and contain known vulnerabilities (e.g., BEAST).
- **Weak Ciphers are supported**, including TLS_RSA_WITH_3DES_EDE_CBC_SHA (3DES) and TLS_RSA_WITH_RC4_128_SHA (RC4).

Impact: Weakened encryption that could be exploited to intercept or decrypt communications, especially from legacy clients. Fails PCI DSS compliance.

2.3. Missing Security Headers

Finding: The server lacks critical HTTP security headers that protect against common client-side attacks.

Evidence (from testssl.sh & Nikto):

- X-Frame-Options: not present - Leaves the site vulnerable to Clickjacking.
- X-Content-Type-Options: not present - Allows MIME-sniffing attacks.
- Content-Security-Policy: not present - Provides no mitigation against Cross-Site Scripting (XSS).
- Strict-Transport-Security: not present - Fails to enforce HTTPS.

Impact: Increased exposure to UI redress attacks, content sniffing, and cross-site scripting.

---

3. Exposed Attack Surface

3.1. Known Vulnerable Web Application (bWAPP)

Finding: The domain hosts "bWAPP" (Buggy Web Application), a project containing over 100 intentional vulnerabilities, including SQL Injection, XSS, and OS Command Injection.

Evidence:

- Page Title: bWAPP | A buggy web application!
- Source Code Comment: <!-- bWAPP, version 2.2 -->

Impact: This presents an **extremely high risk**. It provides a ready-made, easy-to-exploit platform for any attacker to practice on. A successful exploit on any of bWAPP's vulnerabilities could lead to a full compromise of the underlying server.

3.2. Sensitive Directory Exposure

Finding: Automated scanners discovered numerous sensitive paths.

Evidence (from Nikto & Nmap):

- /admin/ - Common administrative interface.
- /install.php - Software installation page.
- /server-status - Apache server status page (can leak internal information).

Impact: These endpoints provide attackers with additional targets for brute-forcing, vulnerability scanning, and information gathering.

Prioritized List of Findings

Priority	Vulnerability	Type	CVSS	Impact	Evidence
Critical	**PHP 8.1.2 (EOL)**	Outdated Software	9.8+	Remote Code Execution	X-Powered-By: PHP/8.1.2...
Critical	**Apache 2.4.52 (CVE-2022-28330)**	CVE	7.5	HTTP Request Smuggling	Nikto, Server header
High	**bWAPP Application Exposed**	Misconfiguration	8.0+	Full Server Compromise	Page title, source code
High	**TLS 1.0/1.1 Enabled**	Misconfiguration	5.9	Crypto Attack, Compliance Fail	testssl.sh report

Priority	Vulnerability	Type	CVSS	Impact	Evidence
Medium	**Information Disclosure (Headers)**	Misconfiguration	4.3	Reconnaissance Aid	Server, X-Powered-By headers
Medium	**Missing Security Headers**	Misconfiguration	4.3	Clickjacking, XSS	testssl.sh, Nikto
Low	**Sensitive Paths Exposed**	Misconfiguration	3.5	Information Disclosure	Nikto, Nmap http-enum

Immediate Mitigation Recommendations

1. **Patch Immediately: This is the highest priority.** Upgrade Apache and PHP to the latest supported versions. PHP must be upgraded to a non-EOL version (e.g., 8.3.x).
2. **Remove or Isolate bWAPP:** If this is not a public training server, remove it immediately. If it must stay, place it behind a strict firewall with IP whitelisting and multi-factor authentication.
3. **Harden TLS Configuration:** Disable TLS 1.0 and 1.1. Disable weak ciphers (3DES, RC4). Prefer forward-secret ciphers.
4. **Suppress Information Headers:**
    - Apache: Set ServerTokens Prod and ServerSignature Off.
    - PHP: Set expose_php = Off in php.ini.
5. **Implement Security Headers:** Add HSTS, X-Frame-Options, X-Content-Type-Options, and a Content-Security-Policy to the web server configuration.
6. **Restrict Access:** Block public access to /server-status, /admin/, and other sensitive paths via firewall rules or Apache configuration (<Location> directives).