**VULNERABILITY ASSESSMENT REPORT**

**1. Introduction**

**1.1 Purpose**

This report provides a security assessment of the web application hosted at **cuk.ac.ke (41.204.161.153)**. The objective is to identify vulnerabilities and provide recommendations to mitigate potential risks.

**1.2 Scope**

* Target: **cuk.ac.ke**
* Assessment Date: **February 12, 2025**
* Tools Used: **Nmap, OWASP ZAP, Burp Suite**
* Testing Methods: **Automated Scanning, Manual Testing, Vulnerability Research**

**2. Summary of Findings**

| **Vulnerability** | **Severity** | **Impact** | **Recommendation** |
| --- | --- | --- | --- |
| **Outdated Apache 2.4.6** | High | Possible RCE, DoS, Privilege Escalation | Upgrade to **Apache 2.4.58+** |
| **Outdated PHP 7.4.33** | Critical | Security patches no longer provided | Upgrade to **PHP 8.2+** |
| **Server Version Disclosure** | Medium | Attackers can target known exploits | Hide server headers |
| **OPTIONS method enabled** | Medium | Allows method enumeration | Restrict HTTP methods |
| **Possible Weak SSL Configuration** | Medium | Potential for SSL downgrade attacks | Disable weak ciphers |
| **Linux Kernel Fingerprinting** | Medium | Possible kernel exploits | Ensure Linux is up to date |

**3. Detailed Vulnerability Analysis**

**3.1 Outdated Apache Version (2.4.6)**

**Risk:** Apache 2.4.6 is outdated and may contain **known vulnerabilities** like RCE, DoS attacks, and information leaks.

**Proof of Detection:**

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.6 (PHP 7.4.33)

443/tcp open ssl/http Apache httpd 2.4.6 (PHP 7.4.33)

**Recommendation:**

* Upgrade Apache to **2.4.58+**
* Regularly patch and update software

**3.2 Outdated PHP Version (7.4.33)**

**Risk:** PHP 7.4 reached **End-of-Life (EOL)** in **November 2022** and no longer receives security updates.

**Proof of Detection:**

|\_http-server-header: Apache/2.4.6 (PHP 7.4.33)

**Recommendation:**

* Upgrade to **PHP 8.2 or later**

**3.3 Server Version Disclosure**

**Risk:** Attackers can fingerprint the web server and target known vulnerabilities.

**Proof of Detection:**

|\_http-server-header: Apache/2.4.6

**Recommendation:**

* Modify httpd.conf to disable version disclosure:

ServerTokens Prod

ServerSignature Off

**3.4 HTTP OPTIONS Method Enabled**

**Risk:** Attackers can enumerate allowed methods and exploit misconfigurations.

**Proof of Detection:**

|\_ Supported Methods: GET HEAD OPTIONS (HTTP)

|\_ Supported Methods: GET HEAD POST (HTTPS)

**Recommendation:**

* Restrict allowed HTTP methods in **Apache config (httpd.conf)**:

<LimitExcept GET POST HEAD>

Deny from all

</LimitExcept>

**3.5 Weak SSL Configuration**

**Risk:** Potential for **SSL downgrade attacks** due to outdated TLS versions.

**Proof of Detection:**

| ssl-cert:

| Not valid before: 2024-09-13

| Not valid after: 2025-09-13

**Recommendation:**

* Disable weak SSL ciphers in ssl.conf:

SSLProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1

SSLCipherSuite HIGH:!aNULL:!MD5:!RC4:!3DES

* Test SSL security using:

openssl s\_client -connect cuk.ac.ke:443 -cipher LOW

**4. Conclusion & Recommendations**

**4.1 Summary**

The scan identified **outdated software, weak SSL configurations, and server fingerprinting risks**. The most critical findings are:

1. **Apache 2.4.6 and PHP 7.4.33 should be upgraded immediately**
2. **SSL/TLS settings need to be hardened**
3. **HTTP methods and server headers should be restricted**

**4.2 Next Steps**

✅ **Apply recommended fixes** and rerun vulnerability scans

✅ **Perform penetration testing with OWASP ZAP and Burp Suite**

✅ **Monitor web traffic for unusual activities**

**5. References**

* [Apache CVEs](https://www.cvedetails.com/version/148646/Apache-Http-Server-2.4.6.html)
* [PHP Security Updates](https://www.php.net/supported-versions.php)
* [SSL Labs Test](https://www.ssllabs.com/ssltest/)

**Report Prepared by:**  *Stephen Njoroge* **Date:** February 12, 2025