



Vulnerability Assessment Report

Kenya Power eRecruitment Portal

Target URL: <http://erecruitment.kplc.local/>

Assessment Tool: OWASP ZAP

Assessment Type: Web Application Vulnerability Assessment (VA)

Assessment Date: 12 May 2026

1. Executive Summary

A vulnerability assessment was conducted on the Kenya Power eRecruitment platform to evaluate the security posture of the web application and identify weaknesses that could expose the system to cyber threats.

The assessment identified several medium-to-low severity security misconfigurations related to missing HTTP security headers and server information disclosure. While no critical exploitation vulnerabilities were identified during this assessment, the observed weaknesses increase the platform's exposure to risks such as:

- Cross-Site Scripting (XSS)
- Clickjacking attacks
- MIME-type confusion attacks
- Information disclosure
- Session hijacking risks
- Browser-based attacks

The platform currently lacks several recommended browser security protections including:

- Content Security Policy (CSP)
- X-Frame-Options / frame-ancestors protection
- HTTP Strict Transport Security (HSTS)
- X-Content-Type-Options

Additionally, the server discloses underlying technology stack information (nginx/1.24.0 (Ubuntu)), which may assist attackers in reconnaissance and targeted exploitation activities.

Overall Risk Rating: **Medium**

2. Key Findings Summary

Finding	Risk Level	Impact
Missing Content Security Policy (CSP)	Medium	Increased exposure to XSS and injection attacks
Missing Clickjacking Protection	Medium	Application can be embedded in malicious frames
Missing HTTP Strict Transport Security (HSTS)	Medium	Increased risk of SSL stripping and insecure transport
Missing X-Content-Type-Options Header	Low	Potential MIME-sniffing attacks
Server Information Disclosure	Low	Reveals server and OS information to attackers

3. Detailed Findings

3.1 Missing Content Security Policy (CSP)

Risk Level: Medium

The application does not implement a Content Security Policy (CSP) header.

CSP is an additional security layer used to mitigate:

- Cross-Site Scripting (XSS)
- Content injection attacks
- Malicious script execution

Without CSP, browsers cannot restrict trusted sources of executable content such as:

- JavaScript
- CSS

- Images
- Frames
- Fonts

Risk Impact

An attacker may exploit client-side injection vulnerabilities to:

- execute malicious scripts
- steal user sessions
- redirect users
- manipulate page content

Recommendation

Implement a strict Content Security Policy header.

Example:

Content-Security-Policy: default-src 'self';

References

- [MDN CSP Guide](#)
- [OWASP CSP Cheat Sheet](#)

3.2 Missing Clickjacking Protection

Risk Level: Medium

The application does not implement protections against clickjacking attacks.

Neither:

- X-Frame-Options
nor
- Content-Security-Policy: frame-ancestors headers were detected.

Risk Impact

Attackers may embed the application inside malicious iframes to:

- trick users into unintended actions
- hijack clicks
- manipulate authenticated sessions

Recommendation

Configure either:

X-Frame-Options: DENY

or:

Content-Security-Policy: frame-ancestors 'none';

If framing is required internally:

X-Frame-Options: SAMEORIGIN

References

- [MDN X-Frame-Options](#)

3.3 Missing HTTP Strict Transport Security (HSTS)

Risk Level: Medium

The application does not enforce HTTP Strict Transport Security (HSTS).

HSTS ensures browsers interact with the application exclusively over HTTPS.

Risk Impact

Without HSTS:

- users may be vulnerable to SSL stripping attacks
- browsers may downgrade connections to HTTP
- attackers on insecure networks may intercept traffic

Recommendation

Enable HSTS with an appropriate max-age value.

Example:

Strict-Transport-Security: max-age=31536000; includeSubDomains

Reference

- [RFC 6797 HSTS Specification](#)

3.4 Missing X-Content-Type-Options Header

Risk Level: Low

The X-Content-Type-Options header was not configured.

Risk Impact

Some browsers may perform MIME-sniffing and interpret files as different content types, potentially enabling:

- malicious script execution
- content interpretation attacks

Recommendation

Configure:

X-Content-Type-Options: nosniff

3.5 Server Information Disclosure

Risk Level: Low

The application discloses backend server information through HTTP response headers:

Server: nginx/1.24.0 (Ubuntu)

Risk Impact

Information disclosure assists attackers in:

- reconnaissance
- targeted exploit identification
- vulnerability mapping

Recommendation

Suppress or obfuscate server version information.

Example:

```
server_tokens off;
```

4. Positive Security Observations

The following secure practices were observed:

- Cache-control directives implemented
- Referrer policy configured (no-referrer)
- HTTPS usage observed
- Asset versioning implemented for static resources

5. Risk Assessment

Category	Assessment
Application Security Posture	Moderate
Exploitability	Medium
Immediate Business Risk	Moderate
Data Exposure Risk	Moderate
Overall Security Maturity	Developing

6. Recommendations Summary

The following actions are recommended in order of priority:

High Priority

- Implement Content Security Policy (CSP)
- Enable Clickjacking protection headers
- Configure HTTP Strict Transport Security (HSTS)

Medium Priority

- Configure X-Content-Type-Options
- Harden HTTP response headers

Low Priority

- Disable server version disclosure
- Conduct periodic vulnerability assessments
- Implement secure configuration baselines

7. Conclusion

The Kenya Power eRecruitment platform demonstrates a functional security foundation; however, several important browser-side security controls are currently absent.

The identified issues primarily relate to:

- security hardening
- secure HTTP header configuration
- information disclosure prevention

Addressing these findings will significantly improve the application's resilience against common web-based attacks and strengthen overall cybersecurity posture.

Continued vulnerability assessments, secure configuration reviews, and adherence to secure development practices are recommended to maintain and improve the platform's security maturity.

Prepared by;

Christopher Khayere

ISC & BCP