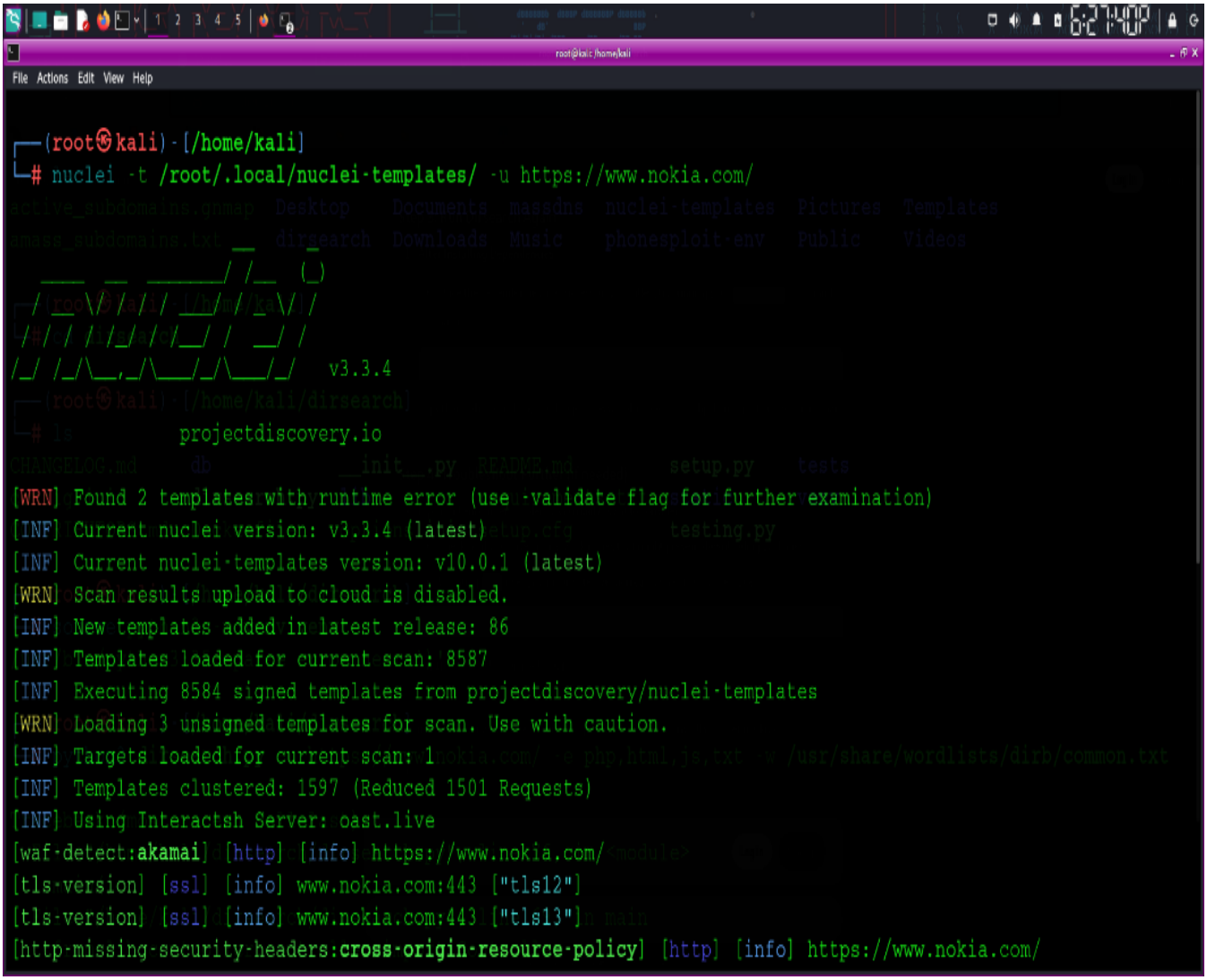
A Research Report on Nokia Website (Vulnerability Scanning)

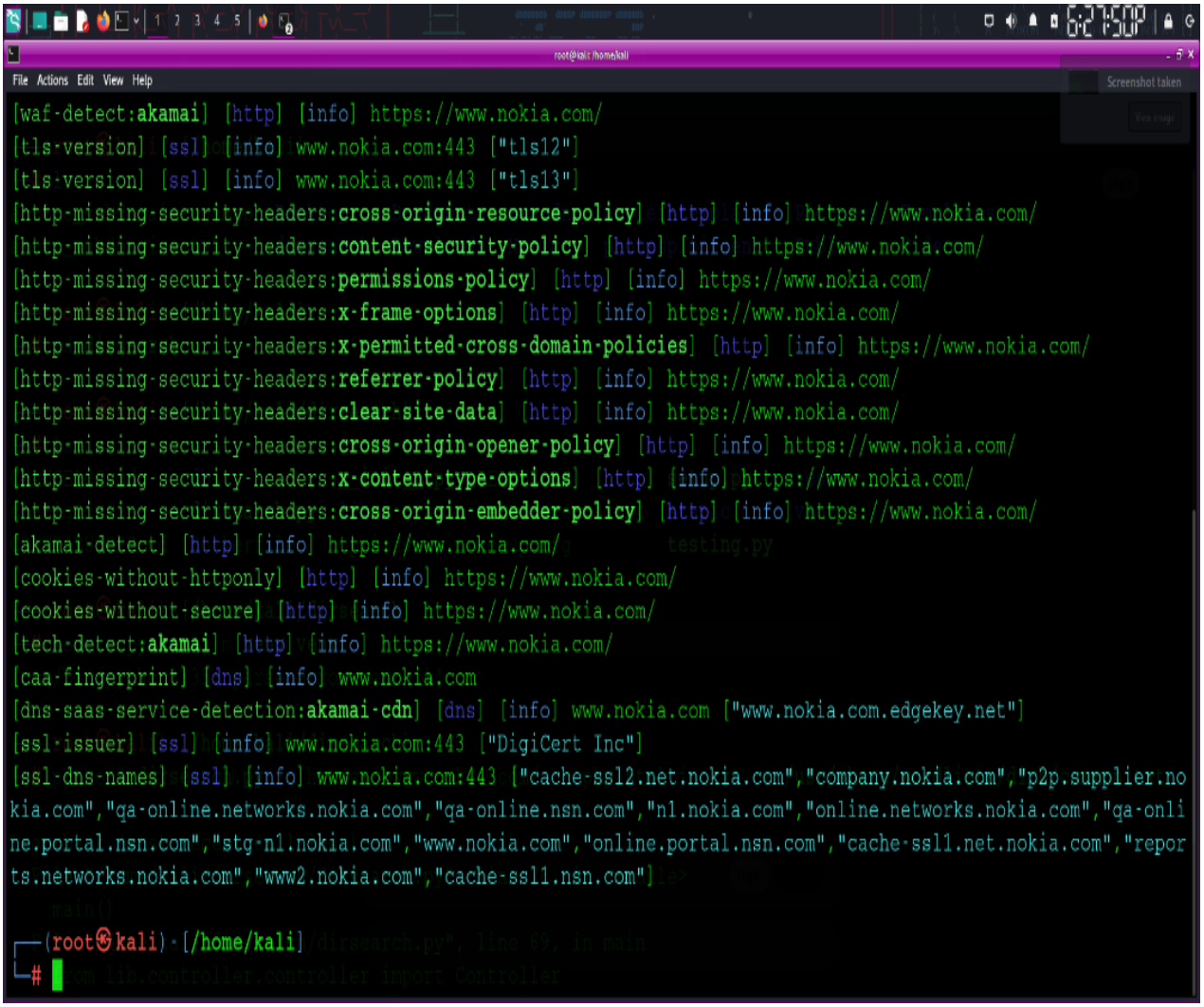
Prepared by
Siva Krishna Siripurapu

Report on Nokia Website Vulnerability Scanning

2. NUCLEI VULNERABILITY SCANNING:

Command: nuclei -t /root/. local/nuclei-templates/ -u https://www.nokia.com/





Observations from the Scan Output:

Missing Security Headers: [Click here to see nuclei file.]

- Several security headers are missing:
- Content-Security-Policy
- X-Frame-Options
- Cross-Origin Resource Policy
- Permissions Policy
- Referrer Policy
- X-Content-Type-Options
- Clear-Site-Data
- Cross-Origin Opener Policy
- Cross-Origin Embedder Polic

Implication: Missing security headers can expose the site to various attacks such as cross-site scripting (XSS), clickjacking, and information leaks.

Cookies Without Secure and HttpOnly Flags:

Cookies Without HttpOnly: This flag helps mitigate the risk of client-side scripts accessing the cookie data.

Cookies Without Secure: This flag ensures that cookies are only sent over HTTPS connections.

Implication: Cookies without these flags can be susceptible to theft via XSS attacks or can be sent over insecure connections.

TLS Versions:

The scan confirms support for TLS 1.2 and TLS 1.3, which are secure.

Implication: This is good practice as older TLS versions (like 1.0 and 1.1) have known vulnerabilities.

Akamai CDN Detection:

The scan detected that the site uses Akamai for content delivery.

Implication: This can provide benefits in terms of performance and security, as CDNs often include DDoS protection and caching.

SSL Certificate Information:

The SSL certificate is issued by DigiCert, which is generally regarded as a reputable certificate authority.

Implication: This indicates that the connection to the site is secure.

Summary and Recommendations

Address Missing Security Headers:

Recommend implementing the missing security headers in the web server configuration. This will enhance security against common web vulnerabilities.

Secure Cookie Configuration:

Ensure that cookies have the HttpOnly and Secure flags set to protect against common web attacks.

Regular Security Assessments:

Consider running regular security scans to check for any new vulnerabilities or misconfigurations.

Monitor Security Practices:

Stay updated on best security practices and recommendations from OWASP and other security organizations.

Conclusion:

Overall, while there are no direct vulnerabilities detected from this specific scan, the missing security headers and cookie configurations should be addressed to bolster the site's security posture.