msu management & science university | Artificial Intelligence and Cyber Security Centre (AICS)

eklas.msu.edu.my - Security Assessment

Date: October 10, 2024

Target System: https://eklas.msu.edu.my

Target IP: 46.250.229.119

Tools Used: Burp Suite v2024.9, Nmap 7.94, Zenmap

Time: 13:09 MYT

Executive Summary

This report presents a comprehensive security assessment of the application hosted at https://eklas.msu.edu.my and its associated infrastructure. The assessment combines vulnerability scanning using Burp Suite, network scanning with Nmap and Zenmap, and additional reconnaissance revealing the target IP address 46.250.229.119 on FOFA, a cyber intelligence search engine.

Our findings reveal several critical vulnerabilities that require immediate attention, including outdated JavaScript libraries, insecure cookie configurations, and potential network exposure risks. The system also shows signs of some security best practices being implemented, such as the use of HTTPS and some firewall protections.

Key Findings

1. **High Severity:**
   - Vulnerable JavaScript Dependencies
   - Open Redirection (DOM-based)
2. **Medium Severity:**
   - TLS Cookie Without Secure Flag Set
   - Unencrypted Communications
3. **Low Severity:**
   - Cookie Without HttpOnly Flag Set
   - Strict Transport Security Not Fully Enforced
   - Mixed Content
4. **Network Exposure:**
   - SSH (Port 22) and HTTPS (Port 8443) services exposed
   - Potential unnecessary UDP services active

5. **Informational:**
    - Valid TLS Certificate Presented
    - Robots.txt File Exposure
    - Host indexed on FOFA cyber intelligence platform

Detailed Findings

1. Application Security (Burp Suite Analysis)

1.1 High Severity Vulnerabilities

1.1.1 Vulnerable JavaScript Dependencies

- **Description:** Multiple JavaScript files (jQuery, Bootstrap, etc.) are outdated and contain known vulnerabilities.
- **Affected URLs:**
    - `/eklas_v7/v701/js/3.7.7.bootstrap.min.js`
    - `/eklas_v7/v701/js/jquery.min.js`
    - `/eklas_v7/v701/uep/js/jquery-ui.min.js`
- **Impact:** Potential for XSS attacks, leading to session hijacking or data theft.
- **Recommendation:** Update all JavaScript libraries to their latest stable versions.

1.1.2 Open Redirection (DOM-based)

- **Description:** Unvalidated user input used in URL construction, allowing potential redirects to malicious sites.
- **Affected URLs:** `/eklas_v7/v701/resource/index.php`
- **Impact:** Users could be redirected to phishing sites or malicious domains.
- **Recommendation:** Implement strict input validation for all URL redirects.

1.2 Medium Severity Vulnerabilities

1.2.1 TLS Cookie Without Secure Flag Set

- **Description:** Session cookie (PHPSESSID) transmitted without the Secure flag.
- **Impact:** Increased risk of session hijacking through man-in-the-middle attacks.
- **Recommendation:** Set the Secure flag on all session cookies.

1.2.2 Unencrypted Communications

- **Description:** Some resources accessible over unencrypted HTTP connections.
- **Impact:** Potential interception and manipulation of data.
- **Recommendation:** Enforce HTTPS across the entire application.

1.3 Low Severity Vulnerabilities

1.3.1 Cookie Without HttpOnly Flag Set

- **Description:** PHPSESSID cookie lacks the HttpOnly flag.
- **Impact:** Increased risk of XSS attacks capturing session cookies.

- **Recommendation:** Set the HttpOnly flag on session cookies.

1.3.2 Strict Transport Security Not Fully Enforced

- **Description:** Missing or misconfigured HSTS header on certain endpoints.
- **Affected URLs:** Multiple endpoints under `/cdn-cgi/` and `/resources/`
- **Recommendation:** Configure HSTS header with appropriate max-age and includeSubDomains directives.

1.3.3 Mixed Content

- **Description:** Secure HTTPS pages loading resources over insecure HTTP connections.
- **Affected URLs:**
  - `/app/recovery/password_reminder.php`
  - `/login_msu.php`
- **Recommendation:** Ensure all resources are loaded over HTTPS.

2. Network Security (Nmap and Zenmap Analysis)

2.1 Open Ports and Services

2.1.1 TCP Port 22 (SSH)

- **Service:** OpenSSH 9.2p1 Debian
- **Findings:**
  - Supports modern key exchange and encryption algorithms
  - Host keys include ECDSA and ED25519
- **Recommendation:** Restrict SSH access to trusted IPs, implement key-based authentication, and consider fail2ban to mitigate brute-force attacks.

2.1.2 TCP Port 8443 (HTTPS)

- **Service:** Nginx
- **Findings:**
  - Responds with 403 Forbidden status
  - Valid SSL certificate for msucollege.edu.my (expires January 1, 2025)
  - HSTS header set with max-age of 86400 seconds
- **Recommendation:** Review access controls and ensure proper HTTPS configuration.

2.2 Filtered Ports

- Several common ports (25, 80, 443, 445) are filtered, suggesting firewall rules are in place.
- **Recommendation:** Regularly review and update firewall rules to maintain security.

2.3 UDP Ports

- Multiple UDP ports open|filtered, including those associated with LDAP, NetBIOS, and UPnP.

- **Recommendation:** Disable unnecessary UDP services to reduce attack surface.

2.4 Operating System Detection

- Linux kernel version 2.6.x to 4.x detected (88% confidence)
- **Recommendation:** Upgrade to the latest stable kernel version to address potential vulnerabilities.

2.5 Network Path

- Traceroute shows approximately 10 hops to the target
- Last hop located in Singapore based on IP geolocation
- **Recommendation:** Review network path for potential security implications.

3. Additional Findings

3.1 Presence on FOFA

- The target IP (46.250.229.119) is indexed on FOFA cyber intelligence platform.
- **Impact:** Increased risk of being targeted by automated attacks or reconnaissance.
- **Recommendation:** Regularly monitor for new exposures and implement additional access controls.

3.2 Valid TLS Certificate

- Server presents a valid TLS certificate issued by Let's Encrypt.
- **Recommendation:** Continue monitoring certificate validity and renew before expiration.

3.3 Robots.txt File Exposure

- The robots.txt file is accessible and may reveal sensitive directories.
- **Recommendation:** Review contents to ensure no sensitive information is disclosed.

Conclusion and Recommendations

The security assessment revealed several critical areas requiring immediate attention:

1. **Update Vulnerable Libraries:**
   - Upgrade all outdated JavaScript libraries to their latest versions.
   - Implement a regular audit process for third-party components.
2. **Enhance Cookie Security:**
   - Set both Secure and HttpOnly flags on all session cookies.
   - Consider implementing SameSite attributes to prevent CSRF attacks.
3. **Enforce HTTPS Everywhere:**
   - Redirect all HTTP traffic to HTTPS.
   - Implement HSTS with a sufficient max-age and include subdomains.
4. **Mitigate Open Redirection:**
   - Implement strict input validation on all URL redirects.
   - Avoid using user-supplied input for redirect destinations.

5. **Restrict Network Access:**
    - Close unnecessary open ports, especially SSH if not required externally.
    - Implement firewall rules to limit access to trusted IP addresses.
6. **Operating System and Service Updates:**
    - Upgrade the Linux kernel to the latest stable version.
    - Keep all services, especially OpenSSH and Nginx, updated to their latest secure versions.
7. **Monitor Public Exposure:**
    - Regularly check for the server's presence on platforms like FOFA.
    - Implement alerts for any new exposures or mentions.
8. **Continuous Security Practices:**
    - Schedule regular vulnerability scans and penetration tests.
    - Implement intrusion detection and prevention systems.
    - Conduct security awareness training for all staff involved in managing the application.

By addressing these issues promptly, the overall security posture of the eklas.msu.edu.my system can be significantly improved, reducing the risk of potential breaches or unauthorized access.

Report prepared by: SHAHSWIENE SUTHAS, SOC ANALYST 1

Attachments: - Detailed Nmap and Zenmap Scan Reports