CYB-206 Web Application Security

Blue Team Report

Team Nu: Suryarajsinh Vala | Rahul Peter | Harpreet Kaur

Executive Summary

This report provides analysis and feedback on the Red Team's findings on six web applications that have been tested for security vulnerabilities. This includes current application status, processes, analysis of known vulnerabilities, and mitigation recommendations.

Current Application Status

The following sections summarize the status of each application, including screenshots and tables summarizing the findings from the Red Team report.

1. **RadGarden**
    - **URL:** https://radgarden.azurewebsites.net/
    - **Status:** Several security enhancements recommended.
2. **TheNaturalTouch**
    - **URL:** https://thenaturaltouchh.azurewebsites.net/
    - **Status:** Potential vulnerabilities identified.
3. **InkCraft**
    - **URL:** https://inkcraft.azurewebsites.net/
    - **Status:** Security improvements needed.
4. **MirrorsProd**
    - **URL:** https://mirrorsprod.azurewebsites.net/
    - **Status:** Potential vulnerabilities identified.
5. **SpringPi**
    - **URL:** https://springpi20240620143324.azurewebsites.net/
    - **Status:** Security enhancements needed.
6. **QuillLite**
    - **URL:** https://quillliteapp.azurewebsites.net/
    - **Status:** Vulnerabilities and improvements needed.

Methodology and Approach

The Blue Team used a combination of manual and mechanical techniques to verify the findings of the Red Team. Methods included reviewing web applications, header analysis, SSL/TLS policy, and a review of recommended security protocols for use.

Red Team Report Analysis

The Red Team identified multiple vulnerabilities in six web applications, such as missing security headers and possible exposure to clickjacking and MIME type sniffer attacks the following sections detail the analysis of each application.

1. **RadGarden**

    - **Findings:** Missing X-Frame-Options and X-Content-Type-Options headers, presence of X-Powered-By header.
    - **Analysis:** This missing header exposes the application to clickjacking and MIME type sniffing attacks. The presence of an X-Powered-By header can give attackers access to server technology, potentially making it easier to exploit known vulnerabilities.

2. **TheNaturalTouch**

    - **Findings:** Missing X-Frame-Options and X-Content-Type-Options headers, presence of X-Powered-By header.
    - **Analysis:** Problems such as missing security headers can lead to unauthorized data access and modification, leaving the application vulnerable to clickjacking and MIME type sniffing attacks.

3. **InkCraft**

    - **Findings:** Missing X-Frame-Options and X-Content-Type-Options headers, presence of X-Powered-By header.
    - **Analysis:** The lack of necessary security headers makes the application vulnerable to clickjacking and MIME type sniffing attacks. The X-Powered-By header can expose server technical information, helping an attacker exploit the system.

4. **MirrorsProd**

    - **Findings:** Missing X-Frame-Options and X-Content-Type-Options headers.
    - **Analysis:** The lack of these security headers exposes the application to clickjacking and MIME type sniffing vulnerabilities, which can compromise the security and integrity of the user data.

5. **SpringPi**

    - **Findings:** Missing X-Frame-Options and X-Content-Type-Options headers, presence of X-Powered-By header.
    - **Analysis:** As with other applications, missing security headers and the presence of X-Powered-By headers expose the application to clickjacking, MIME type sniffing, and potential exploitation based on server technical issues

6. **QuillLite**

   - **Findings:** Missing X-Frame-Options, X-Content-Type-Options, and Strict-Transport-Security headers, presence of X-Powered-By header.
   - **Analysis:** The lack of this critical security header makes the application vulnerable to clickjacking, inadequate transport layer security, and MIME type sniffing. The X-Powered-By theme reveals information about server technology, helping attackers exploit known vulnerabilities.

Incident Response and Detection Analysis

No specific events were reported in the red group study. However, in many applications, the lack of required security headers can hinder effective incident response and investigation.

Exploited Vulnerabilities

The Red Team report identified common issues such as:

- Missing X-Frame-Options header
- Missing X-Content-Type-Options header
- Presence of the X-Powered-By header

Privileged Access and Lateral Movement

No indications of privileged access or lateral movement vulnerabilities were detected across the web applications.

Data Exfiltration and Impact Assessment

Although no direct vulnerabilities related to data exfiltration were identified, the issues reported could impact user trust and data integrity.

Recommendations and Mitigation Strategies

The following recommendations aim to mitigate the identified vulnerabilities:

1. **Implement Critical Security Headers**
    - X-Frame-Options
    - X-Content-Type-Options
    - Strict-Transport-Security (for some applications)
2. **Regular Updates and Patching**
    - Ensure server components and applications are up to date with the latest security patches.
3. **Periodic Security Assessments**
    - Conduct regular security assessments and penetration testing to identify and address new vulnerabilities.
4. **Content Security Policy (CSP)**
    - Implement a CSP to protect against cross-site scripting (XSS) attacks.

Lessons Learned and Best Practices

- Comprehensive implementation of security headers is crucial.
- Regular updates and proactive security measures can significantly reduce the risk of vulnerabilities.
- Continuous monitoring is essential for maintaining a secure environment.

Conclusion and Next Steps

Immediate actions to improve the security level of the evaluated web application should focus on implementing missing security headers and maintaining thorough security audits and proactive security measures will help reduce the risks and maintain a safe environment.