Paola N. Baez Hernandez

Lab 2.1 - Application Hardening – eCom

Task 1: Perform a web application scan using OWASP ZAP (Zed Attack Proxy)

1. Answer the following questions:
    1. How many HIGH vulnerabilities did OWASP ZAP find on the HammerCorp eCom server?

       The report identified 1 High-risk vulnerability.

    2. What type of vulnerabilities were the HIGH findings?

       The High-risk vulnerability found was Cross-Site Scripting Reflected (XSS).

    3. Are the HIGH findings on the OWASP Top 10?

       Yes, Cross-Site Scripting (XSS) is part of the OWASP Top 10. In the 2021 OWASP Top 10, it falls under A03:2021 – Injection, which includes XSS vulnerabilities.

    4. Were there any other findings from the OWASP ZAP report? If so, what?

       Yes, the report included multiple findings;

       Medium Risk Findings:

       - Content Security Policy (CSP) Header Not Set
       - Vulnerable JavaScript Library
       - Absence of Anti-CSRF Tokens

Low Risk Findings:

- Cookies missing security attributes (HttpOnly and SameSite)
- Cross-Domain JavaScript Source File Inclusion
- Server information leakage via "X-Powered-By" headers
- X-Content-Type-Options Header Missing
- Timestamp Disclosure (Unix)

Informational Findings:

- Sensitive information in URLs
- Suspicious comments in the source code
- Session management issues
- User Agent Fuzzer alerts
- Modern Web Application detection

Task 2: Review the HammerCorp E-Commerce website, and the files on the HammerCorp FTP Server.

1. Answer the below questions:

    1. Are all the products hammers?

        Yes, Also there's a book of hammers and important tools.

    2. Is the connection to the HammerCorp website secure (HINT: View Site Information).

        No, Website is not secure.

    3. Does Hammer Corp have a Privacy Policy?

        Their privacy policy only says (Don't start nothin', won't be nothin' Mind your own business and we will too.) In my opinion, I believe that doesn't count as a privacy policy.

    4. Does the HammerCorp Ecomm website require a secure password when you create an account?

        Yes, it does require a secure password.

2. Answer the below questions:

    1. Are all the customers located in the United States?

       Not all the customers are from the US, there's customers from other countries.

    2. What privacy regulations should apply to Hammer Corp's customers?

       Privacy regulations such as GDPR and CCPA should apply to Hammer Corp's customers.

    3. Is Hammer Corp's Privacy Policy adequate for its customers?

       Not at the moment, Hammer Corp's Privacy Policy may need an urgent update to comply with the relevant privacy regulations.

    4. Is there any information in the files that may put Hammer Corp's IT infrastructure at risk?

       The logging information of the company's server.

    5. Is any of the customer's personal information at risk (e.g. name, address)?

       I didn't specifically see any name or address information displayed. However some irregularities may put credit cards at risk.

    6. Is there any customer credit card information at risk (e.g. credit card numbers)?

       Theres is credit card information at risk, as credit cards where shown on the retrive files.

Deliverable: Capture the answers in your deliverable document.

Task 3: SSL Certificate Analysis

1. What grade did badssl.com get for their certificate on SSL Labs?

   It got a grade of B.

2. Is there anything in the results that makes you think the grade should be lower than it is?
   HINT: Is the grade capped?

   The grade is capped I believe there were no other significant issues that could suggest a lower grade.

3. Does badssl.com support downgrade prevention?

   Yes, badssl.com supports downgrade prevention.

4. What TLS protocols support downgrade attack protection?

   It supports TLS 1.2 which supports downgrade attack protection.

5. Did badssl.com support any unsecure protocols? If so, which one(s)?

   Badssl.com doesn't support any unsecure protocol.

6. What grade did amazon.com certificate get?

   It got a grade of B.

7. Did the amazon.com certificate show any major issues?

   Yes, a major issue was identified that Amazon supports TLS .0 and TSL 1.1 which were outdated and less secure.

8. Why do you think Amazon might support older or less secure SSL/TLS connections?

   Amazon likely supports older SSL/TLS connections to ensure backward compatibility for users who are using outdated browsers or devices.

9. Based on the scan of amazon.com's certificate do you feel safe making purchases there? Why or why not?

   In my personal opinion, Amazon is still a safe platform for purchases. If you are using an updated browser and a secure internet connection, your transactions should remain safe.

Lab Write-up

1. Provide at least one paragraph answering the following questions:

    1. Do you think all websites check themselves for issues related to the OWASP Top 10 before going live? Why or why not?

        Not every website checks for OWASP Top 10 vulnerabilities before going live. Most companies, mostly the smaller ones, often lack on the resources or security expertise to conduct testing. Larger companies may have more dedicated security teams that will prioritize testing beforehand. Smaller companies always go through functionality and deployment speed over security. Some developers think or assume that security is handled at the framework or hosting level, which is not always the case.

    2. Do you think you should use Qualys's SSL Labs tool to check websites you will use your credit card on? Why or why not?

        Yes, In my opinion, using Qualys's SSL Labs tool is a very good practice to follow and check the security of websites where you will enter the most sensitive information, like credit card details. This tool helps identify weaknesses such as outdated TLS protocols, missing security headers, and weak ciphers. If a site scores poorly, it indicates heavy potential security risk, and people should hold off and be cautions before proceeding with any transaction.

    3. Take a look at BadSSL.com. It presents a series of sites that are guaranteed to have certain SSL/TLS issues. How might a security team use this to test their compensating controls?

        Security Teams can leverage BadSSl.com to evaluate how proper their security measures respond to SSL/TLS issues, which includes checking if the browser and security tools block insecure connections. Also, they can ensure that intrusion detection systems detect and flag weak SSL/TLS configurations. The platform could also contribute to training exercises to educate developers and IT personnel about SSL/TLS security beast practices.