Cybersecurity Analyst Challenge 2: Server Security V2

A cybersecurity analyst is frequently responsible for testing and maintaining server security. It is their job to run penetration tests on various server components in order to discern areas of potential weakness and discover how any concerns might be addressed.

Challenge objective

Identify and report vulnerabilities on a chosen web platform via penetration testing.

Challenge Description

Test the security of a website. After installing a site, follow the instructions given below to test the security of the server and discover areas of vulnerability. Install a website, force SSL on domain, and run a penetration test. Be sure to accurately synthesize and present your findings.

1. Install a website.
2. Force SSL on domain.
3. Run penetration tests.
4. Assess difference in results from first assessment to second assessment.
5. Extract the report.
6. Synthesize information.
7. Create a presentation highlighting key areas.
8. Record or screenshot your test completion notification.
9. Upload your test results to files.
10. Think and answer (within the Project):
    a. What did you learn?
    b. How can you improve your skills?
    c. What would you have done differently?

Instructions

1. Start the Challenge.
2. Select the Project Pitch Template.
3. Follow the Task Checklist and make sure to do each step - the Resources provided have all the information needed to learn each task.
4. Track your work for each step.
5. Submit your Project and move on to the next Challenge.

Challenge Tasks

- Review Challenge Description
- Review resources associated to the Challenge
- Research other sources if needed (ie: Google)
- Follow outlined steps in the Challenge
- Answer Challenge Questions
- Document your process and upload necessary photos and/or videos to the 'Project Gallery'
- Finalize and upload your solution to files
- Add any additional links related to your project

Challenge Questions

- How did you approach the Challenge?
- What did you learn?
- What skills did you need to complete the Challenge?
- How can you improve your skills?
- What tools and processes did you use?
- What roadblocks did you have, if any? Or, what would you have done differently?

Solution

1. SSL Information

- **Cipher Used:**
  The site is using `TLS_AES_128_GCM_SHA256`, which is a secure and modern cipher suite for TLS communications.

- **Certificate Issuer:**
  The SSL certificate is issued by **Amazon RSA 2048 M02**, suggesting the site is hosted via **Amazon Web Services (AWS)**.

2. Security Issues Identified

- **Missing X-Frame-Options Header:**
  Without this header, the site is vulnerable to **clickjacking** attacks, as it can be embedded in iframes.

- **Missing Strict-Transport-Security (HSTS) Header:**
  HSTS ensures browsers only use **HTTPS connections**. Its absence exposes users to potential **man-in-the-middle (MITM)** attacks.

- **Missing X-Content-Type-Options Header:**
  This allows browsers to **mismatch MIME types**, potentially leading to exploitation through content interpretation errors.

- **Content-Encoding: deflate:**
  The site uses "deflate" compression, which may make it vulnerable to the **BREACH attack**, a side-channel attack on compressed HTTPS responses.

- **Uncommon Headers Detected:**
  Headers like `x-amz-error-message`, `x-amz-error-code`, and `x-amz-error-detail-key` suggest the server is using **Amazon S3** infrastructure and may be referencing a **missing file (NoSuchKey)**.

3. Additional Information

- **Server Banner Behavior:**
  The server header changes between **AmazonS3** and **CloudFront**, indicating the use of **Amazon's Content Delivery Network (CDN)**.

- **Alt-SVC Header:**
  The site supports **HTTP/3 over QUIC**, which modernizes communication but was not testable by Nikto.

- **SSL/TLS Handshake Failure:**
  The scan was terminated early due to **handshake errors**, suggesting potential **misconfigurations** or issues with the server's SSL/TLS setup.

4. No CGI Directories Found

- The scan found **no CGI scripts**, which reduces exposure to certain common **script-based vulnerabilities**.

Recommendations

- **Implement X-Frame-Options Header:**
  To protect against clickjacking vulnerabilities.

- **Enable Strict-Transport-Security (HSTS):**
  To enforce secure HTTPS connections across all users and sessions.

- **Add X-Content-Type-Options Header:**
  To ensure browsers honor the correct MIME type and avoid content spoofing.

- **Review Content-Encoding Settings:**
  Either disable or securely configure "deflate" compression to mitigate **BREACH attack** risks.

- **Resolve Amazon S3 Errors:**
  Investigate and fix the `NoSuchKey` and related errors indicated by the `x-amz-error-*` headers to ensure no broken or missing resources.

1. How did you approach the Challenge?

I approached the challenge by first setting up the penetration testing environment with Kali Linux and ensuring the website was running on SSL. Once the environment was ready, I used Nikto to scan the website for common vulnerabilities. I then analyzed the results to identify potential security flaws and compared them before and after implementing SSL to see how the security posture of the site improved.

2. What skills did you need to complete the Challenge?

I needed skills in web security to understand common vulnerabilities, especially related to SSL/TLS. Familiarity with Kali Linux and penetration testing tools like Nikto was crucial, as well as the ability to analyze HTTP headers and server configurations. I also needed knowledge of web protocols (e.g., HTTPS, HTTP/2) to assess the website's security thoroughly.

3. What tools and processes did you use?

I used Nikto, a web vulnerability scanner, to identify weaknesses in the website's configuration and headers. I followed the process of scanning the site both before and after enforcing SSL to assess changes in security. For testing SSL/TLS, I looked at the website's cipher suites and headers to ensure they met security best practices.

4. What roadblocks did you have, if any? Or, what would you have done differently?

One roadblock I encountered was a SSL/TLS handshake failure, which prevented the scan from completing fully. This was likely due to server-side misconfigurations. If I had more time, I would have performed additional troubleshooting to resolve this issue and rerun the test. I also would have tested using a broader set of tools to verify the site's security from multiple perspectives.

5. What did you learn?

I learned how to perform a comprehensive security scan using Nikto and how to assess SSL configurations to ensure secure communication. I also realized how vulnerable a website can be without proper headers, such as X-Frame-Options or Strict-Transport-Security.

6. How can you improve your skills?

To improve my skills, I could focus on gaining more hands-on experience with a variety of security tools and learning how to use them more effectively. It would be helpful to better understand the common challenges that websites face with security, such as issues with encrypted connections, and how to solve them. I could also expand my knowledge of general best practices for setting up and maintaining secure servers, which is important for any cybersecurity role. Additionally, I would like to learn more about advanced penetration testing techniques, such as how to simulate real-world cyber-attacks more accurately. Finally, improving my problem-solving skills, especially when things don't go as expected.