**CTF Topic: Attack Vector Discovery with PentestTools**



**Introduction**

****

PentestTools.com provides a suite of online tools for penetration testing and vulnerability assessment. These tools can help identify various attack vectors and security weaknesses in web applications. In this challenge, you will use PentestTools to analyze the website http://testphp.vulnweb.com/ and uncover potential attack vectors.

**Tools and Requirements**

To perform this CTF, you will need the following tools and resources:

A web browser (e.g., Chrome)

* PentestTools website: <https://pentest-tools.com/>
* The target website: <http://testphp.vulnweb.com/>

**Scenario**

**A person sitting in front of several computer screens

Description automatically generated**

A security researcher, Alex, wants to evaluate the security posture of the website http://testphp.vulnweb.com/ using the online tools provided by PentestTools.com. Alex's goal is to identify potential vulnerabilities and weak points that could be exploited by attackers. The researcher will follow a structured approach to scan the website, analyze the results, and document any significant findings.

**Process to Perform**

**Step 1: Visit the PentestTools Website**

* Open https://pentesttools.com/ in your browser.

**Step 2: Sign In to Pentest-Tools**

**Step 2: Perform a Website Scan**

* Navigate to the "Website Scanning" section.
* Enter the target website URL "http://testphp.vulnweb.com/" into the provided field.
* Select the type of scan you want to perform, such as a Full Website Scan, OWASP Top 10 Scan, or a CMS Vulnerability Scan.
* Start the scan and wait for the results to be generated.

**Step 3: Analyze the Results**

* Review the detailed report provided by PentestTools about the target website.
* Look for identified vulnerabilities, weak points, and potential attack vectors.
* Note down any significant findings, such as SQL injection points, XSS vulnerabilities, or outdated software versions.

**Let's Begin the Challenge**

With the tools and techniques outlined above, let's dive into the challenge. Use PentestTools to uncover potential attack vectors and security weaknesses in the target website. Document each step you take and any findings along the way.

**Questions**

Based on the website vulnerability scanner report for "http://testphp.vulnweb.com/" from Pentest Tools, here are CTF questions with their answers:

1. What is the overall risk level of the scanned website?

Answer: High

2. Which missing security header increases the risk of XSS?

Answer: ContentSecurityPolicy

3. Which server software version was identified in the scan?

Answer: Nginx 1.19.0

4. What is the CVE identifier for the PHP vulnerability that allows arbitrary code execution?

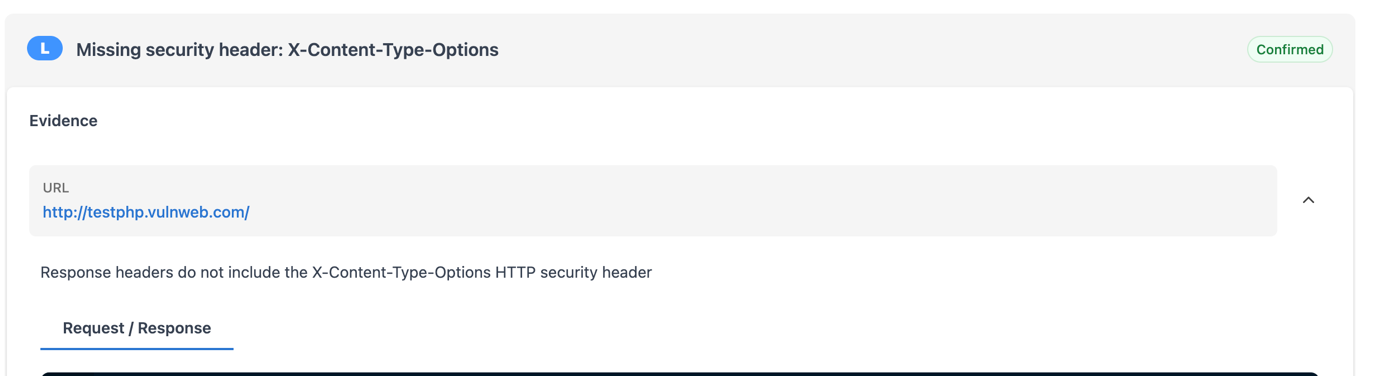
Answer: CVE20244577

5. What is the HTTP status code for the homepage of http://testphp.vulnweb.com/ as reported by PentestTools?

Answer: 200

**Happy hunting!**

**Hint**

****