CTF Topic: Identifying Vulnerabilities with Xposer

Introduction

The Xposer Firefox extension is a tool designed to help identify vulnerabilities in web applications. By scanning websites, this tool can help uncover common security flaws that can be exploited by attackers. Participants will use this extension to find vulnerabilities on the test site `http://testphp.vulnweb.com/`.

Tools and Requirements

- Mozilla Firefox browser  
- Install the [Xposer Firefox extension](<https://addons.mozilla.org/en-US/firefox/addon/xposer/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search>)   
- Basic understanding of web security vulnerabilities

Scenario

As a participant in this CTF challenge, your task is to use the Xposer extension to identify vulnerabilities on the provided test site `<http://testphp.vulnweb.com/>` . Use the extension to analyze the site and answer the following questions based on your findings.

Steps

1. Install the Xposer Firefox Extension  
   - Open Mozilla Firefox.  
   - Go to the [Xposer Firefox extension](https://addons.mozilla.org/en-US/firefox/addon/xposer/?utm\_source=addons.mozilla.org&utm\_medium=referral&utm\_content=search) link.  
   - Click "Add to Firefox" and complete the installation process.

2. Open the Test Site  
   - Navigate to the test site: [http://testphp.vulnweb.com/](http://testphp.vulnweb.com/).

3. Scan the Site with Xposer  
   - Open the Xposer extension from the Firefox toolbar.  
   - Click on "Start Scan" to begin scanning the test site for vulnerabilities.

4. Analyze the Results  
   - Review the scan results provided by the Xposer extension.  
   - Identify the types of vulnerabilities found and note specific details.

5. Answer the Questions  
   - Use the information from the scan results to answer the following questions.

Questions and Answers

Flag 1: Identify a Cross-Site Scripting (XSS) vulnerability on the site.

Answer:

(Example: The search functionality is vulnerable to reflected XSS.)

Flag Captured.

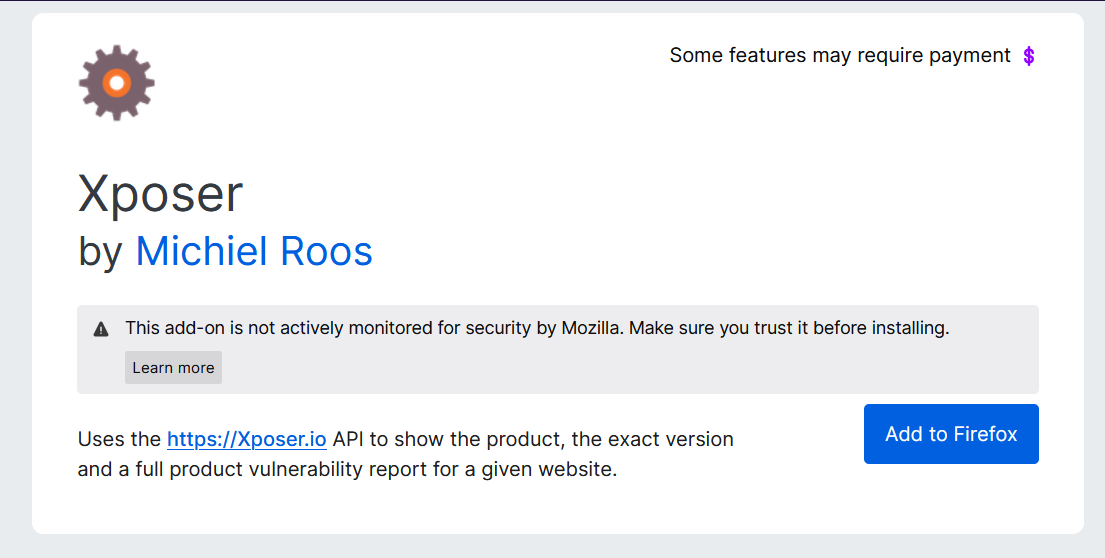
Flag 2: What HTTP header can be implemented to mitigate XSS attacks?

Answer:

Content-Security-Policy (CSP)

Flag Captured.

Hint



Install the Xposer Firefox extension and use it to scan the pages of the provided test site `http://testphp.vulnweb.com/`. Adjust settings and use the extension features as required to answer the questions accurately.