CTF Topic: Identifying XSS Vulnerabilities

Introduction

Cross-site scripting (XSS) is a security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. The Check XSS Firefox extension helps identify such vulnerabilities in web applications.

Tools and Requirements

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

Scenario

As a participant in this CTF challenge, your task is to use the Check XSS extension to identify XSS 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.

Begin

1. Install the Check XSS Firefox extension from the provided link.  
2. Use the extension to scan the provided test site `<http://testphp.vulnweb.com/>`.  
3. Utilize the extension features to answer the questions.

Questions and Answers

Flag 1: Does the homepage of `http://testphp.vulnweb.com/` have any XSS vulnerabilities?

Answer:   
Yes, the homepage is vulnerable to XSS

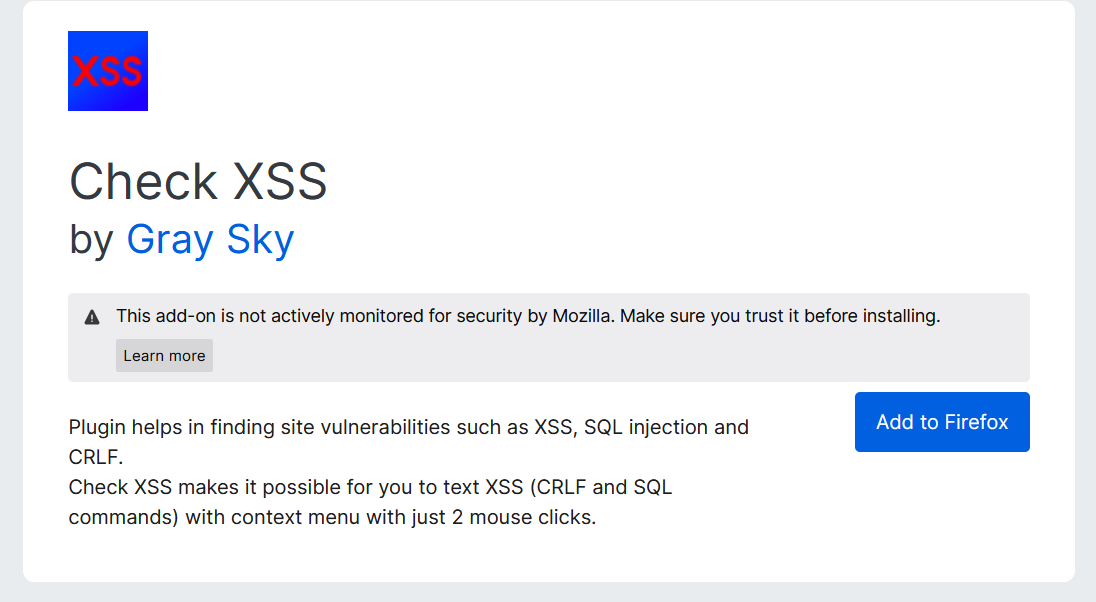
Flag Captured.

Flag 2: How many Total Vulnerabilities Where Found in this Site ?

Answer:   
<script>alert('XSS')</script>

Flag Captured.

Hint



Install the Check XSS 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.