CTF Topic: Identifying Clickjacking Vulnerabilities

Introduction

Clickjacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The ClickJacking Firefox extension helps identify such vulnerabilities in web applications.

Tools and Requirements

- Mozilla Firefox browser   
- Basic understanding of web security and clickjacking

- Install the (<https://addons.mozilla.org/en-US/firefox/addon/clickjacking/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search>)

Scenario

As a participant in this CTF challenge, your task is to use the ClickJacking extension to identify clickjacking 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 ClickJacking 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: Is the `X-Frame-Options` header present on the homepage of `<http://testphp.vulnweb.com/>`?

Answer: (No, the X-Frame-Options header is not present)

Flag Captured.

Flag 2: Which HTTP header can be used to prevent clickjacking attacks?

Answer: X-Frame-Options or Content-Security-Policy (CSP)

Flag Captured.

Hint

A screenshot of a computer error

Description automatically generated

Install the ClickJacking 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.