Injecting Scripts with Browser Injector Chrome Extension

Introduction

"Browser Injector" is a Chrome extension designed to inject custom JavaScript, CSS, and HTML into any webpage. This Capture the Flag (CTF) scenario introduces beginners to the basics of using the "Browser Injector" extension to analyze and modify a given webpage's content.

Tools and Requirements

Browser Injector Chrome Extension: An extension for Google Chrome that allows injecting custom JavaScript, CSS, and HTML into webpages.

Link: <https://chromewebstore.google.com/detail/browser-injector/ledhhmfbjmdkeaabnnkagbkbcilfdgim>

Scenario

In this scenario, you will use the "Browser Injector" extension to analyze and manipulate the content on the Wikipedia webpage. Your tasks include identifying key elements, modifying them, and capturing flags based on your findings.

Begin

To start, install the "Browser Injector" extension from the Chrome Web Store. Use this extension to analyze and manipulate the content on the provided webpage and solve the challenges to capture the flags.

Questions

Flag 1: Inject a New Header

Task: Use the "Browser Injector" extension to inject a new header with the text "CTF Challenge" at the top of the Wikipedia homepage.

URL: Wikipedia

Question: What is the exact HTML tag you used to inject the new header?

Hint: Use the extension to inject a header tag (<h1>).

Answer: <h1>CTF Challenge</h1>

Flag Captured.

Flag 2: Use Browser Injector to inject a script that changes the background color of the webpage to light blue. What is the JavaScript code used?

URL: <http://testphp.vulnweb.com/>

Answer:

javascript

alert('CTF Challenge');

Flag Captured.

Hint: