Website Security Analysis Using "Website Risk Analyzer" Extension

Introduction

"Website Risk Analyzer" is a Chrome extension designed to provide an analysis of a webpage's security and potential risks. This Capture the Flag (CTF) scenario introduces beginners to the basics of using the "Website Risk Analyzer" extension to identify security risks on a given webpage.

Tools and Requirements

* Website Risk Analyzer Chrome Extension: An extension for Google Chrome that provides a detailed analysis of a webpage's security risks

Link: <https://chromewebstore.google.com/detail/website-risk-analyzer/apcjcfdafnbllnjjeljjanlbfmjkebho>

Scenario

In this scenario, you will use the "Website Risk Analyzer" extension to analyze the security metrics of the webpage for Mozilla. Your tasks include identifying key security elements, understanding their impact, and capturing flags based on the analysis.

Begin

To start, install the "Website Risk Analyzer" extension from the Chrome Web Store. Use this extension to analyze the security metrics of the provided webpage and solve the challenges to capture the flags.

Questions

Flag 1: SSL/TLS Certificate Analysis

Task: Use the "Website Risk Analyzer" extension to analyze the SSL/TLS certificate of the Mozilla webpage.

URL: <https://www.mozilla.org/en-US/>

Question: Is the SSL/TLS certificate valid and properly configured for the Mozilla webpage?

Hint: Use the extension to view the SSL/TLS certificate analysis under the security section.

Answer: Yes, the SSL/TLS certificate is valid and properly configured.

Flag Captured.

Flag 2: HTTP Security Headers

Task: Use the "Website Risk Analyzer" extension to identify the presence of HTTP security headers on the Mozilla webpage.

URL: <https://www.mozilla.org/en-US/>

Question: List any two HTTP security headers that are present on the Mozilla webpage.

Hint: Use the extension to view the HTTP security headers under the security section.

Answer: Content-Security-Policy, X-Frame-Options

Flag Captured.

Hint: