**Analyzing Web Page Security Using "Security Tweaks" Extension**

**1. Introduction**

"Security Tweaks" is a Chrome extension designed to enhance the security of your browsing experience by providing various security checks and features. This Capture the Flag (CTF) scenario introduces beginners to the basics of using the "Security Tweaks" extension to identify potential security issues on a given webpage.

**2. Tools and Requirements**

Security Tweaks Chrome Extension: An extension for Google Chrome that enhances security by providing various security checks and features.

**3. Scenario**

In this scenario, you will use the "Security Tweaks" extension to analyze the webpage for [example.org](https://www.example.org). Your tasks include identifying security issues and capturing flags based on the analysis.

**4. Process to follow while performing CTF**

To start, install the "Security Tweaks" extension from the Chrome Web Store: <https://chromewebstore.google.com/detail/cbfhjbllealmkfknkpfmpkpljmlcjpjl>

Use this extension to analyze the provided webpage and solve the challenges to capture the flags.

**Questions and Answers**

Flag 1: Content Security Policy

Task: Use the "Security Tweaks" extension to check if the example.org webpage has a Content Security Policy (CSP) implemented.

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

Question: Does the http://testphp.vulnweb.com/ webpage have a CSP implemented?

Hint: Use the extension to check for CSP headers.

Answer: No

Flag Captured.

Flag 2: HTTP Strict Transport Security (HSTS)

Task: Use the "Security Tweaks" extension to determine if the example.org webpage uses HTTP Strict Transport Security (HSTS).

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

Question: Is the http://testphp.vulnweb.com/ webpage using HSTS?

Hint: Use the extension to check for HSTS headers.

Answer: No

Flag Captured.