**CTF Topic: Detecting XSS Vulnerabilities Using "Baby XSS" Extension**

**1. Introduction**

"Baby XSS" is a Firefox extension designed to help users detect basic Cross-Site Scripting (XSS) vulnerabilities on a webpage. This Capture the Flag (CTF) scenario introduces beginners to the basics of using the "Baby XSS" extension to identify XSS vulnerabilities on a given webpage.

**2. Tools and Requirements**

Baby XSS Firefox Extension: An extension for Firefox that helps in detecting XSS vulnerabilities on websites

**3. Scenario**

In this scenario, you will use the "Baby XSS" extension to analyze the webpage for example.com. Your tasks include identifying XSS vulnerabilities and capturing flags based on the analysis.

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

Step 1: To start, install the "Baby XSS" extension from the Firefox Add-ons Store or open the link provided to you:

:<https://addons.mozilla.org/en-US/firefox/addon/baby-xss/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search>

Step 2: Use this extension to analyze the provided webpage and solve the challenges to capture the flags.

**Questions and Answers**

Flag 1: Presence of XSS Vulnerability

Task: Use the "Baby XSS" extension to check if the example.com webpage has any XSS vulnerabilities.

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

Question: Does the http://testphp.vulnweb.com/ webpage have any XSS vulnerabilities?

Hint: Use the extension to scan the webpage for XSS vulnerabilities.

Answer: Yes

Flag Captured.

Flag 2: Security Best Practices

Task: Use the "Baby XSS" extension to check if the example.com webpage follows security best practices to prevent XSS.

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

Question: Does the http://testphp.vulnweb.com/ webpage follow security best practices to prevent XSS?

Hint: Use the extension to analyze the webpage's adherence to security best practices.

Answer: No

Flag Captured.