**CTF Topic: Using HSTS Preload List Submission**

**1. Introduction**

The HSTS (HTTP Strict Transport Security) Preload List is a feature that allows websites to be included in a list that browsers use to enforce secure connections. This challenge will introduce you to the process of submitting a website to the HSTS Preload List to ensure it always uses HTTPS.

A green shield with a check mark on a blue background

Description automatically generated

**2. Tools and Requirements**

* Access to the internet
* Access to the HSTS Preload List Submission page

**3. Scenario**

You are an ethical hacker tasked with ensuring that a website always uses HTTPS by submitting it to the HSTS Preload List. Your job is to follow the necessary steps to check if the website meets the requirements and then submit it to the HSTS Preload List.

**A red text on a screen

Description automatically generated**

**4. Process to Follow While Performing CTF**

**Step 1: Go to the HSTS Preload List Submission Page:**

[**https://hstspreload.org/**](https://hstspreload.org/)

**Step 2: Enter the Website URL**

Enter the website URL [**https://google-gruyere.appspot.com/**](https://google-gruyere.appspot.com/)in the search bar

**Step 3:**  **Solve the CTF**

**5. Let’s Begin the Challenge**

**Questions**

**Flag 1: Does the website redirect all HTTP traffic to HTTPS?**

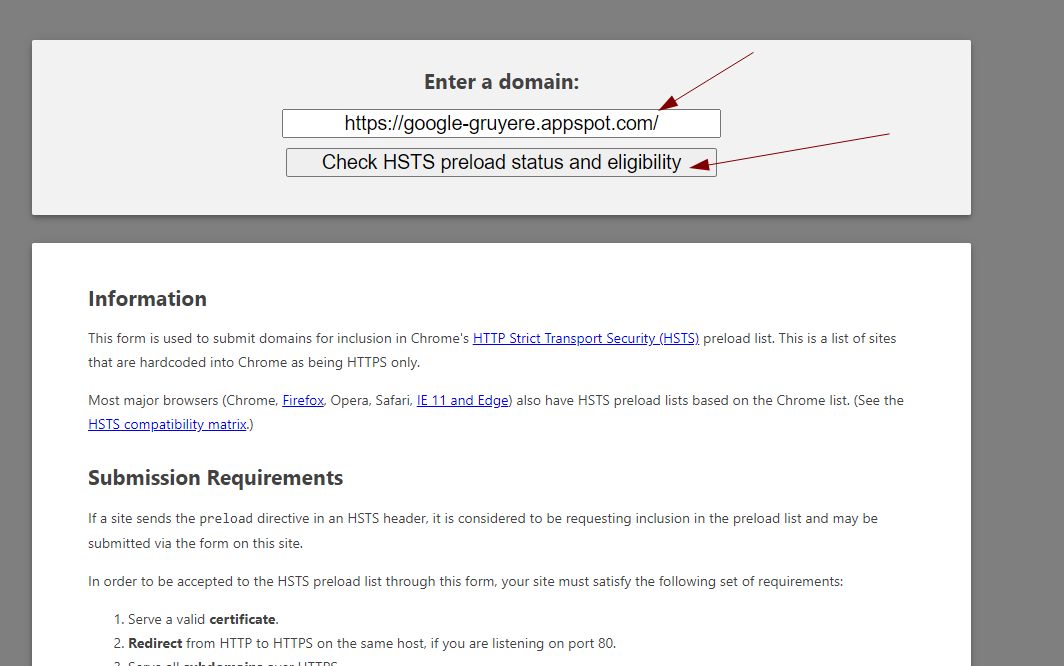
*Answer:* No

**Flag 2: Does the website serve an HSTS header on the base domain for HTTPS requests?**  
*Answer:* No

**Hint:**

A screenshot of a computer

Description automatically generated



A screenshot of a computer screen

Description automatically generated