**CTF: HSTS Preloading and Subdomain Issues**

A green shield with a check mark on a blue background

Description automatically generated

**Introduction**

**A cartoon of a person holding a piece of paper

Description automatically generated**

HSTS (HTTP Strict Transport Security) is a web security policy mechanism that helps protect websites against man-in-the-middle attacks. Preloading HSTS involves submitting a domain to a list of sites that enforce HSTS by default in browsers. This CTF challenge focuses on understanding HSTS preloading, subdomain policies, and related troubleshooting.

**Tools and Requirements**

* Understanding of HSTS and subdomain policies
* Target Website: testphp.vulnweb.com: <http://testphp.vulnweb.com/>
* HSTS Preload Website: hstspreload.org: <https://hstspreload.org/>

**Scenario**

**A red text on a screen

Description automatically generated**

You are a cybersecurity analyst tasked with ensuring that `testphp.vulnweb.com` is preloaded with HSTS. During the preloading process, you encounter several errors. Your challenge is to analyse these errors, understand their causes, and find the solutions.

**Challenge Process**

* Visit hstspreload.org: <https://hstspreload.org/>
* Enter the domain testphp.vulnweb.com: <http://testphp.vulnweb.com/>
* Analyse the errors returned by the HSTS preload checker.
* Resolve the issues to make the domain eligible for HSTS preloading.

**Questions**

1. Flag 1: What is the first error encountered when checking the preload status of “testphp.vulnweb.com”?

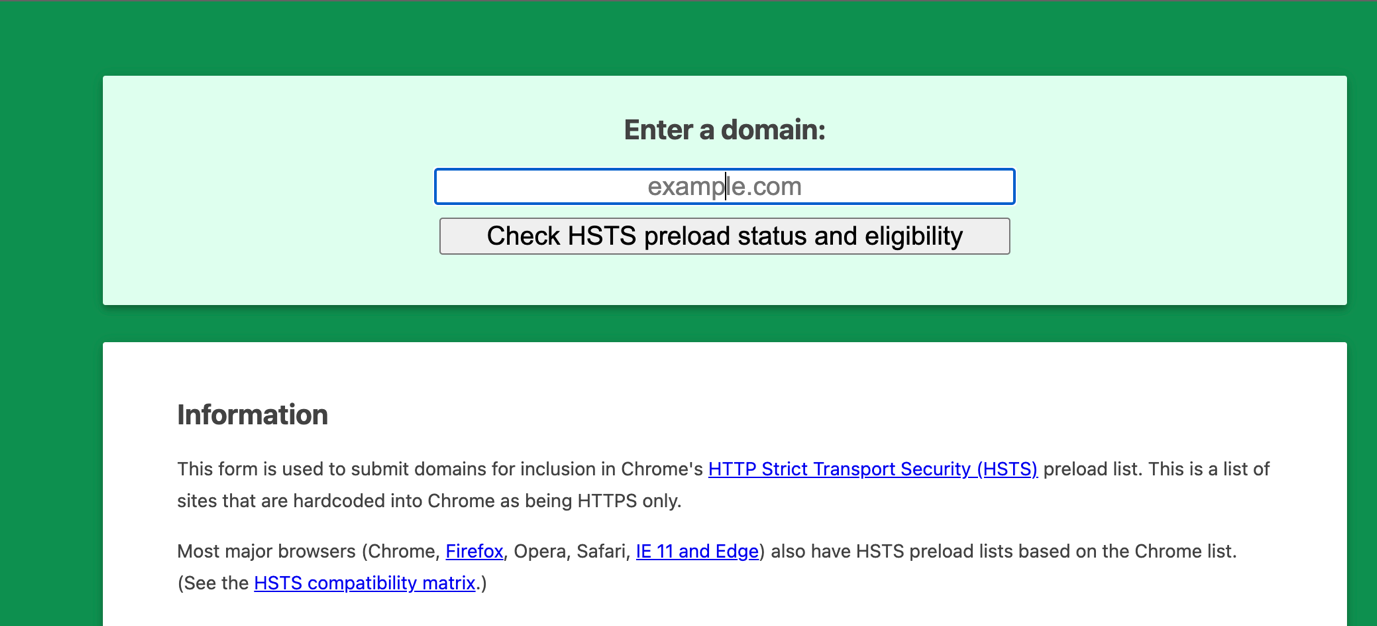
Answer: Subdomain

Flag Captured

2. Flag 2: Is testphp.vulnweb.com preloaded?

Answer: No

Flag Captured

**Hint**

A screenshot of a computer

Description automatically generated