**CTF: Analysing web application with Mozilla Observatory**



**Introduction**

****

Mozilla Observatory is a tool that helps assess the security configuration of websites by analyzing their HTTP headers and other security-related settings. This CTF challenge involves analyzing the security report for the website "zero.webappsecurity.com" and identifying security misconfigurations and missing headers.

**Tools and Requirements**

* Access to observatory.mozilla.org: https://observatory.mozilla.org/
* Basic understanding of web security headers and TLS

**Scenario**

****

You are a security analyst tasked with reviewing the security headers for the website "zero.webappsecurity.com" based on a scan result from Mozilla Observatory. Your goal is to identify missing security headers, misconfigurations, and potential security risks.

**Process**

1. Open the website “observatory.mozilla.org”: <https://observatory.mozilla.org/>
2. After that scan the website “zero.webappsecurity.com”

: <http://zero.webappsecurity.com/>

1. Capture the Flag

**Questions**

Flag 1: What is the value of HTTP Raw Server Header Transfer-Encoding?

Answer: chunked

Flag Captured

Flag 2: What is the content type of the Raw Server Header?

Answer: text/html;charset=UTF-8

Flag Captured

Flag 3: What is the value of the Signature Algorithm?

Answer: SHA256WithRSA

Flag Captured

**Hint**





