**CTF: Security Headers**



**Introduction**

Security headers are a critical component of web security, helping to protect against various attacks by controlling browser behaviour. This CTF challenge involves analysing security headers for a given website and identifying missing headers, misconfigurations, and potential security risks.

**Tools and Requirements**

* Access to https://securityheaders.com/
* Basic understanding of web security headers

**Link**

* <http://testphp.vulnweb.com/>

**Scenario**

****

You are a security analyst tasked with reviewing the security headers for the website "testphp.vulnweb.com" based on the scan result provided. Your goal is to identify missing security headers and understand their implications.

**Process**

1. Open the website “securityheaders.com”: <https://securityheaders.com/>
2. After that scan the website “testphp.vulnweb.com”: <http://testphp.vulnweb.com/>
3. Answer the questions based on the scan result.

**Questions**

Flag 1:What is the overall security grade given to the website "testphp.vulnweb.com" by the security headers scan?

Answer: F

Flag Captured.

Flag 2: Which security header effective measure to protect your site from XSS attacks?

Answer: Content-Security-Policy

Flag Captured.

Flag : What is the value of the "XPoweredBy" header in the raw headers?

Answer: PHP/5.6.4038+ubuntu20.04.1+deb.sury.org+1

Hint:





