X-XSS-Protection

summary :

this header is introduced to protect against injection attacks in the form of cross-site scripting.

this header was intended as a way to control the filtering functionality

severity :

best practice

impact :

This issue is reported as additional information only. There is no direct impact arising from this issue.

remediation : Add the X-XSS-Protection header with a value of "1; mode= block".

..............................................................................................................................................................

X-Content-Type-Options : (ايجابية)

summary :

this header is introduced to block content sniffing and could transform non-executable MIME types into executable MIME types.

severity: Low

impact :

if The server did not return a correct 'X-Content-Type-Options' header, which means that this

website could be at risk of a Cross-Site Scripting (XSS) attack.

remediation :

Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'

.............................................................................................................................................................

cashe-control

summary :

Cache-control is an HTTP header used to specify browser caching policies in both client requests and server responses.

Policies include how a resource is cached, where it’s cached and its maximum age before expiring

severity: critical

impact : if The server did not return or returned an invalid 'Cache-Control' header which means page containing sensitive information

(password, credit card, personal data, etc) could be stored and then be exposed to unauthorised persons.

remediation :

Configure your web server to include a 'Cache-Control' header with the value 'no-store'

...................................................................................................................................................

HTTP Strict Transport Security (HSTS): (ايجابية)

summary :

HSTS is a mechanism that lets you make sure your website or web application is only accessed using secure HTTPS (SSL/TLS) connections.

If you enable HSTS for your domain name, all web browsers will make encrypted connections to web pages hosted on this domain

severity: Medium

impact: could allow the attackers to fool the browser into expiring HSTS entries and allowing insecure HTTP connections.

remediation :HSTS is considered a vital component of web security, and you should consider implementing it in your security policy.