

X-Frame-Options Setting Malformed

Description:

The website was scanned using OWASP ZAP. An X-Frame-Options header was present in the response but the value was not correctly set.

Risk: Medium

Solution:

Ensure a valid setting is used on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

References:

<https://tools.ietf.org/html/rfc7034#section-2.1>

Evidence: Digilocker