ZAP Scanning Report

Summary of Alerts

Risk Level Number of Alerts

 High
 0

 Medium
 0

 Low
 2

 Informational
 0

Alert Detail

Low (Medium) Cookie Without Secure Flag

Description A cookie has been set without the secure flag, which means that the cookie can be accessed via

unencrypted connections.

URL https://eth.dapps.network/sitemap.xml

Method GET

Parameter ARRAffinity

Evidence Set-Cookie: ARRAffinity

URL https://eth.dapps.network

Method GET

Parameter ARRAffinity

Evidence Set-Cookie: ARRAffinity

URL https://eth.dapps.network/robots.txt

Method GET

Parameter ARRAffinity

Evidence Set-Cookie: ARRAffinity

Instances 3

Solution Whenever a cookie contains sensitive information or is a session token, then it should always be

passed using an encrypted channel. Ensure that the secure flag is set for cookies containing

such sensitive information.

Reference http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)

CWE Id 614 WASC Id 13 Source ID 3

Low (Medium) Web Browser XSS Protection Not Enabled

Description Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-

Protection' HTTP response header on the web server

URL https://eth.dapps.network

Method GET

Parameter X-XSS-Protection

Evidence X-XSS-Protection: 0

1

Instances

Solution Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP

response header to '1'.

Other information The X-XSS-Protection HTTP response header allows the web server to enable or disable the

web browser's XSS protection mechanism. The following values would attempt to enable it:

X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss

The following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer,

Chrome and Safari (WebKit).

Note that this alert is only raised if the response body could potentially contain an XSS payload

(with a text-based content type, with a non-zero length).

Reference https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/

 CWE Id
 933

 WASC Id
 14

 Source ID
 3