OWASP ZAP

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	0

Alert Detail

Medium (Medium)	Encabezado X-Frame-Options no establecido
Description	El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.
URL	https://neocheckio.azurewebsites.net/VideoIdentification/Index/e0b3e432-c0ed-4c39-b455-262ec98ae445
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Nota.- El error de ZAP es fruto de una incompatibilidad de la herramienta con el nuevo estándar, que corresponde con el objeto del plugin: embeber nuestro iframe en la página web de un tercero:

The frame-ancestors directive obsoletes the X-Frame-Options header. If a resource has both policies, the frame-ancestors policy SHOULD be enforced and the X-Frame-Options policy SHOULD be ignored.

No obstante tampoco la aplicamos pues expondría a nuestros clientes al saltar el error de la consola:

Refused to display 'https://neocheckio.azurewebsites.net/VideoIdentification/Index/13b7615e-2bcb-4395-bc75-692cce973abf' in a frame because an ancestor violates the following Content Security Policy directive: "frame-ancestors 'self' https://company1.com https://company2.com"

La autenticación la realizamos mediante el establecimiento de sesión necesario para utilizar el plugin.

Sophos

https://securityheaders.com & https://www.sophos.com

Security Report Summary

A+

Site:	https://neocheck.net/
IP Address:	104.40.185.192
Report Time:	11 Oct 2018 13:39:35 UTC
Headers:	✔ X-Frame-Options ✔ X-Content-Type-Options ✔ X-XSS-Protection ✔ Strict-Transport-Security ✔ Content-Security-Policy ✔ Referrer-Policy ✔ Feature-Policy

Raw Headers

HTTP/1.1	200 OK
Cache-Control	no-cache, no-store, must-revalidate
Pragma	no-cache
Content-Length	2559
Content-Type	text/html
Last-Modified	Thu, 11 Oct 2018 10:13:11 GMT
Accept-Ranges	bytes
ETag	"1d4614b0383dc7f"
Server	Kestrel
X-Powered-By	ASP.NET
X-Frame-Options	SAMEORIGIN
X-Content-Type-Options	nosniff
X-XSS-Protection	1
Arr-Disable-Session-Affinity	True
strict-transport-security	max-age=31536000; includeSubDomains
Content-Security-Policy	**script-src** https://neocheckio.azurewebsites.net/ *'self'*
Referrer-Policy	same-origin
Feature-Policy	**sync-xhr** 'self'
Date	Thu, 11 Oct 2018 13:39:34 GMT

Other Services

Sophos	IT security products have become as complex as the networks they're trying to secure. At Sophos we know that the solution to complexity is not more complexity. We tackle security challenges with clarity and confidence, knowing that simple security is better security. We offer free security software so you can check for security risks, remove viruses and protect your network.

Upcoming Headers

Expect-CT	Expect-CT allows a site to determine if they are ready for the upcoming Chrome requirements and/or enforce their CT policy.

Additional Information

Server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
X-Powered-By	X-Powered-By can usually be seen with values like "PHP/5.5.9-1ubuntu4.5" or "ASP.NET". Trying to minimise the amount of information you give out about your server is a good idea. This header should be removed or the value changed.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
X-XSS-Protection	X-XSS-Protection sets the configuration for the cross-site scripting filters built into most browsers. The best configuration is "X-XSS-Protection: 1; mode=block".
strict-transport-security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyse this policy in more detail.
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Feature-Policy	Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.