REPORTE DE HALLAZGOS

Riesgo medio

Cross-Domain Misconfiguration (6)

URL	https://dvwa.co.uk/ https://dvwa.co.uk/css/all.css https://dvwa.co.uk/css/nivo-slider.css https://dvwa.co.uk/js/jquery-1.6.2.min.js https://dvwa.co.uk/js/jquery.nivo.slider.pack.js https://dvwa.co.uk/nivo-slider/themes/default/default.css
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
Risk	Medium
Confidence	Medium
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
CWE Id	264
WASC Id	14
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_perm

	issive_cors_policy

Vulnerable JS Library(1)

URL	https://dvwa.co.uk/js/jquery-1.6.2.min.js
Description	The identified library jquery, version 1.6.2 is vulnerable.
Risk	Medium
Confidence	Medium
Parameter	
Attack	
Evidence	jquery-1.6.2.min.js
CWE Id	829
WASC Id	-1
Other Info	CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2012-6708
Solution	Please upgrade to the latest version of jquery.
Reference	https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/11290 https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969

X-Frame-Options Header Not Set (1)

URL	https://dvwa.co.uk/
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
Risk	Medium
Confidence	Medium
Parameter	
Attack	
Evidence	
CWE Id	1021
WASC Id	15
Other Info	
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set 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. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options