

1. Perform a vulnerability scan on a demo website using online scanners like OWASP ZAP.

mdn\_ReferencesLearnPlusCurriculumBlogToolsThemeLog inSign up for free

HTTP Observatory > Report: www.itsecgames.com

# HTTP Observatory Report

Report Feedback

HTTP Observatory

Tests & Scoring

FAQ

Scan summary: www.itsecgames.com

F

Score: 0 / 100  
Scan Time: 3 minutes ago  
Tests Passed: 6 / 10

Rescan

Scan another website

Scan results

ScoringCSP analysisCookiesRaw server headersScan historyBenchmark comparison

Test	Score	Reason	Recommendation
<u>Cookies</u>	-	No cookies detected	None
<u>Cross Origin Resource Sharing (CORS)</u>	0	Content is not visible via cross-origin resource sharing (CORS) files or headers.	None
<u>Redirection</u>	-20	Does not redirect to an HTTPS site.	Redirect to the same host on HTTPS first, then redirect to the final host on HTTPS.
<u>Referrer Policy</u>	-	Referrer-Policy header not implemented.	Set to strict-origin-when-cross-origin at a minimum.
<u>Strict Transport Security (HSTS)</u>	-20	Strict-Transport-Security header cannot be set, as site contains an invalid certificate chain.	HSTS can only work with a valid TLS certificate on the server. Let's Encrypt is a good choice, as are certificates managed by your cloud provider or commercially sold ones.

HTTP Observatory > Report: www.itsecgames.com				HTTP Observatory	
<a href="#">Subresource Integrity</a>	-50	✖	Subresource Integrity (SRI) not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via <code>src="//..."</code> .	Load external scripts over HTTPS, and add SRI to them.	Tests & Scoring
<a href="#">X-Content-Type-Options</a>	0	✔	<code>X-Content-Type-Options</code> header set to <code>nosniff</code> .	None	FAQ
<a href="#">X-Frame-Options</a>	0	✔	<code>X-Frame-Options</code> (XFO) header set to <code>SAMEORIGIN</code> or <code>DENY</code> .	Implement frame-ancestors CSP.	
<a href="#">Cross Origin Resource Policy</a>	-		Cross Origin Resource Policy (CORP) is not implemented (defaults to <code>cross-origin</code> ).	None	

2.