This site returned an HTTP status code other than **200 (OK)**, which may cause its results to be inaccurate.

Scan Summary

A+

Host:	fdsa.apersona.com
Scan ID #:	39088538 (unlisted)
Start Time:	June 28, 2023 5:08 PM
Duration:	8 seconds
Score:	115/100
Tests Passed:	11/11

Recommendation

Initiate Rescan

You're on the home stretch!

The use of Referrer Policy can help protect the privacy of your users by restricting the information that browsers provide when accessing resources kept on other sites.

- Mozilla Web Security Guidelines (Referrer Policy)

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✓	+10	Content Security Policy (CSP) implemented with `default-src 'none'` and no `'unsafe'`	
Cookies	–	0	No cookies detected	
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	
HTTP Strict Transport Security	✓	0	HTTP Strict Transport Security (HSTS) header set to a minimum of six months (15768000)	
Redirection	✓	0	Not able to connect via HTTP, so no redirection necessary	
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	
Subresource Integrity	–	0	Subresource Integrity (SRI) is only needed for html resources	
X-Content-Type-Options	✓	0	X-Content-Type-Options header set to `"nosniff"`	
X-Frame-Options	✓	+5	X-Frame-Options (XFO) implemented via the CSP `frame-ancestors` directive	
X-XSS-Protection	✓	0	X-XSS-Protection header not needed due to strong Content Security Policy (CSP) header	

Content Security Policy Analysis

Test	Pass	Info
Blocks execution of inline JavaScript by not allowing `'unsafe-inline'` inside `script-src`	✓	
Blocks execution of JavaScript's `eval()` function by not allowing `'unsafe-eval'` inside `script-src`	✓	
Blocks execution of plug-ins, using `object-src` restrictions	✓	
Blocks inline styles by not allowing `'unsafe-inline'` inside `style-src`	✓	
Blocks loading of active content over HTTP or FTP	✓	
Blocks loading of passive content over HTTP or FTP	✓	
Clickjacking protection, using `frame-ancestors`	✓	
Deny by default, using `default-src 'none'`	✓	
Restricts use of the `<base>` tag by using `base-uri 'none'`, `base-uri 'self'`, or specific origins	✗	
Restricts where `<form>` contents may be submitted by using `form-action 'none'`, `form-action 'self'`, or specific URIs	✗	
Uses CSP3's `'strict-dynamic'` directive to allow dynamic script loading (optional)	–	

Looking for additional help? Check out Google's CSP Evaluator!

Grade History

Date	Score	Grade
June 28, 2023 5:08 PM	115	A+

Raw Server Headers

Header	Value
Connection:	keep-alive
Content-Length:	50
Content-Security-Policy:	default-src 'none'; frame-ancestors 'none'
Content-Type:	application/json
Date:	Wed, 28 Jun 2023 21:08:31 GMT
Server:	nginx
Strict-Transport-Security:	max-age=63072000
X-Content-Type-Options:	nosniff