HTTP Observatory | TLS Observatory | SSH Observatory | Third-party Tests

Scan Summary

Host:	www.fidelity.com
Scan ID #:	30275104
Start Time:	October 20, 2022 12:27 PM
Duration:	5 seconds
Score:	25/100
Tests Passed:	8/11

Recommendation

Initiate Rescan

You're doing a great job with HTTPS and HTTP Strict Transport Security!

Since you're now only allowing connections over HTTPS, consider using the `Secure` flag to protect your cookies against their accidental transmission over HTTP. Furthermore, the use of `HttpOnly` protects your session cookies from malicious JavaScript.

- Mozilla Web Security Guidelines (cookies)

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

Test Scores

Test	Pass	Score	Reason
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented
Cookies	✗	-30	Session cookie set without using the `HttpOnly` flag
Cross-origin Resource Sharing	✓	0	Content is visible via cross-origin resource sharing (CORS) files or headers, but is restricted to specific domains
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	Initial redirection is to HTTPS on same host, final destination is HTTPS
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)

Test	Pass	Score	Reason
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin
X-Content-Type-Options	✔	0	X-Content-Type-Options header set to `"nosniff"`
X-Frame-Options	✘	-20	X-Frame-Options (XFO) header not implemented
X-XSS-Protection	✔	0	X-XSS-Protection header set to `"1; mode=block"`

Cookies

Name	Expires	Path	Secure ⓘ	HttpOnly ⓘ	SameSite ⓘ	Prefixed ⓘ
MC	December 2, 1703 12:00 PM	/	✔	✘	None	✘
SESSION_CTX	Session	/ftgw/Fas/Fidelity	✔	✔	✘	✘
SESSION_SCTX	Session	/	✔	✘	✘	✘
XSRF-TOKEN	Session	/	✘	✘	✘	✘
_abck	December 2, 1703 12:00 PM	/	✔	✘	✘	✘
_neo.csrf	Session	/	✘	✔	✘	✘
akaalb_www_binpublic_alb	Session	/	✔	✔	None	✘
akaas_www_AWS_AS_NL	Session	/	✔	✘	None	✘
bm_sz	July 16, 1668 12:00 PM	/	✘	✘	✘	✘

Grade History

Click to View

Raw Server Headers

Header	Value
Access-Control-Allow-Credentials:	true
Access-Control-Expose-Headers:	X-XSRF-TOKEN
Cache-Control:	max-age=0, no-store
Connection:	keep-alive

Header	Value
Content-Encoding:	gzip
Content-Length:	27602
Content-Type:	text/html; charset=utf-8
Date:	Thu, 20 Oct 2022 16:27:16 GMT
ETag:	W/"23ab8-lBhPAqaYt33vSlUESvWdzAY6PRs"
P3P:	CP="UNI DEM GOV FIN STA COM NAV PRE INT ONL CUR ADM DEV PSA PSD CUSi IVDi IVAi TELi CONi TAI OUR OTRi"
Server:	Apache
Set-Cookie:	MC=IHCUq_BD9kJUdRJ0FIxJZ8cEGBMSAmNRduQRD7M4mP_YDznfqjMGBAAAAQAGBWNRduQAP03; path=/; domain=.fidelity.com; expires=Fri, 20-Oct-2023 16:27:16 GMT; secure; samesite=none, XSRF-TOKEN=ELFDw9k1-YGwy2nmJwp6agU0BXXtfPqXyjdA; path=/, _neo.csrf=dE1eSHJiP0ckLOUXD5nrE3Al; path=/; httponly, SESSION_CTX=1437E13A23E77B36575E7EF5CCE89240; path=/ftgw/Fas/Fidelity; domain=fidelity.com; secure; HttpOnly, SESSION_SCTX=1437E13A23E77B36575E7EF5CCE89240; path=/; domain=fidelity.com; secure, akaas_www_AWS_AS_NL=2147483647~rv=82~id=d60f972cb87b75fe1672ab0ca68c98b2; path=/; Secure; SameSite=None, _abck=06AE5B37C87B6132A3D340D9DFC0064C~-1~YAAQ5U9DF7YjsuaDAQAAoW049ghX21pPwBYu3cB60SP/GccTHC+LeXpypUGCBXi1AUiZtydB0+sFAzFvRaHNhDKdl9HkvWtIHnGRhOrJl6xIG0qnPnVvx50YdqJku0FhUAOY9zy9VWsDaGm18nXsJ7Sf9SqgwPWPIlcMWxsYBCNfvJChRvEhJh6l0iYb40qBttu81ZuUbvEjqPy6H4KqMEARCCmoISwMAXwyyu21g0ajAagRpHWCigzKy8SHXW/w9vHAcgop4QTBHVz3p5OyhU68egy4gHYzqeuAX8Gqot4BzY4pvydw0aC3pWmhKMGDduYne1OSTXhX3/WL8ScM1u9G/sJgMuFHtdkSJngVYblJYw/aPRGFObQZ7A==~-1~-1~-1; Domain=.fidelity.com; Path=/; Expires=Fri, 20 Oct 2023 16:27:16 GMT; Max-Age=31536000; Secure, bm_sz=D6954CBF1B5EEBFF9F79163EE4AAF0D9~YAAQ5U9DF7cjsuaDAQAAoW049hG4hluP8MVXg0s4doHb0tGlwLhGNrY0hU/olwrJw2bBGXxUYV+PcOhUxx9kP8348ObaBNwMtQzvwAPlfMFk0z2S3O92416ygOkbT4HB54ojcQckD9Lsbpc4VBT0EQ0YF240b8VimtosmXM8OzHBo6z0QUvsKmC7AizCs9+me3V/Y6TTqLdWJHPNwfTL9xBzwTTHsbMfA6l+nkuhHFQWgJmHWaBw2ufjN7F1GD4QYAJKwvvGMts9KmqW4J4JIjODwGq4ftDyyCerN3n+bYqtT1554w==~3293762~3618371; Domain=.fidelity.com; Path=/; Expires=Thu, 20 Oct 2022 20:27:16 GMT; Max-Age=14400
Vary:	Accept-Encoding
X-Akamai-Transformed:	9 31554 0 pmb=mTOE,2
X-Content-Type-Options:	nosniff
fscalleeid:	https-digital.fidelity.com-10000
fselapsedtime:	12477
fsreqid:	REQ635176e44557aac497311213a89daa33
strict-transport-security:	max-age=15552000; includeSubDomains
x-xss-protection:	1; mode=block