Summary of react.safeplaces.extremesolution.com Website

FINAL GRADE

C+

DNS

SERVER IP
34.71.54.90

REVERSE DNS
90.54.71.34.bc.googleusercontent.com

INFO

DATE OF TEST
May 24th 2020, 13:38

SERVER LOCATION
Houston 🇺🇸

Web Server Analysis

HTTP RESPONSE	REDIRECT TO	NPN	ALPN
200 OK	N/A	H2 HTTP/1.1	Yes

CONTENT ENCODING	SERVER SIGNATURE	WAF	LOCATION
GZIP DEFLATE	nginx/1.17.8	No WAF detected	N/A

HTTP METHODS ENABLED

✓ GET ✓ POST ✓ HEAD ✓ OPTIONS ✓ DELETE ✓ PUT

CMS Security Analysis

A non-intrusive CMS fingerprinting technology thoroughly crawls some parts of the CMS to fingerprint its version in the most accurate manner:

FINGERPRINTED CMS & VULNERABILITIES

No CMS were fingerprinted on the website. Information

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

No components were fingerprinted on the website. Information

GDPR Security Analysis

If the website processes or stores any PII of EU residents, the following requirements of EU GDPR may apply:

PRIVACY POLICY

Privacy Policy was not found on the website or is not easily accessible. Misconfiguration or weakness

WEBSITE SOFTWARE SECURITY

Website software and its components could not have been reliably fingerprinted.
Make sure it is up2date. Information

SSL/TLS TRAFFIC ENCRYPTION

SSL/TLS encryption seems to be present. Good configuration

COOKIE CONFIGURATION

No cookies with potentially sensitive information seem to be sent. Information

COOKIES DISCLAIMER

No cookies with potentially sensitive or tracking information seem to be sent. Information

PCI DSS Security Analysis

If the website falls into a CDE (Cardholder Data Environment) scope, the following Requirements of PCI DSS may apply:

REQUIREMENT 6.2

Website CMS could not have been reliably fingerprinted. Make sure it is up2date. Information

REQUIREMENT 6.5

No publicly known vulnerabilities seem to be present on the website. Good configuration

REQUIREMENT 6.6

No WAF was detected on the website. Implement a WAF to protect the website against common web attacks. Misconfiguration or weakness

HTTP Headers Security Analysis

Some HTTP headers related to security and privacy are missing or misconfigured. Misconfiguration or weakness

MISSING REQUIRED HTTP HEADERS

X-Frame-Options X-XSS-Protection X-Content-Type-Options Expect-CT Feature-Policy

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin Public-Key-Pins Public-Key-Pins-Report-Only

SERVER

The web server discloses its version, potentially facilitating further attacks against it. Misconfiguration or weakness

Raw HTTP Header

Server: nginx/1.17.8

STRICT-TRANSPORT-SECURITY

The header is properly set. Good configuration

Raw HTTP Header

Strict-Transport-Security: max-age=15724800; includeSubDomains

Directives

Name	Description
max-age	Sets the time browsers must enforce the use of HTTPS to browse the website.

Content Security Policy Analysis

CONTENT-SECURITY-POLICY

The header was not sent by the server. Misconfiguration or weakness

CONTENT-SECURITY-POLICY-REPORT-ONLY

The header was not sent by the server. Information

Cookies Security Analysis

No cookies were sent by the web application. Information