Summary of responsiblefinanceforum.org Website Security

FINAL GRADE

C

DNS

SERVER IP
109.199.98.152

REVERSE DNS
vm1636.sgvps.net

INFO

DATE OF TEST
November 12th 2019, 09:25

SERVER LOCATION
Mount Hope

The website has at least one folder with enabled directory listing, putting its content at risk. Misconfiguration or weakness

Web Server Analysis

HTTP RESPONSE
200 OK

REDIRECT TO
N/A

NPN
H2 HTTP/1.1

ALPN
Yes

CONTENT ENCODING
GZIP

SERVER SIGNATURE
nginx

WAF
Custom

LOCATION
SingleHop, Inc.

HTTP METHODS ENABLED

GET POST HEAD OPTIONS DELETE PUT TRACK CUSTOM

DIRECTORY LISTING ENABLED

The website has at least one folder with enabled directory listing: https://responsiblefinanceforum.org/wp-includes/js/ .

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 was fingerprinted on the website.

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

No CMS components were detected

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

GDPR Security Analysis

PRIVACY POLICY

Privacy Policy is found on the website. — Good configuration

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

Cookies with potentially sensitive information are sent without secure flag. — Misconfiguration or weakness

COOKIES DISCLAIMER

Cookies with potentially sensitive or tracking information are sent, but no cookie disclaimer is found on the website. — Misconfiguration or weakness

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

The website seems to be protected by a WAF. Review its logs and configuration on a periodic basis. — Good configuration

HTTP Headers Security Analysis

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

MISSING REQUIRED HTTP HEADERS

Strict-Transport-Security | 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

Web server does not disclose its version. Good configuration

Raw HTTP Header

Server: nginx

X-POWERED-BY

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

Raw HTTP Header

X-Powered-By: W3 Total Cache/0.9.7.5

REFERRER-POLICY

The header is properly set. Good configuration

Raw HTTP Header

Referrer-Policy: no-referrer-when-downgrade

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

Some cookies have missing secure flags or attributes. Misconfiguration or weakness

COOKIE: WPSGCACHEBYPASS

The cookie is missing Secure, HttpOnly and SameSite flags, make sure it does not store sensitive information. Misconfiguration or weakness

Raw HTTP Header

Set-Cookie: wpSGCacheBypass=0; expires=Tue, 12-Nov-2019 07:06:40 GMT; Max-Age=-3600; path=/

Attributes

Name	Value	Description
expires	Tue, 12-Nov-2019 07:06:40 GMT	Sets the maximum lifetime of the cookie using a date.
max-age	-3600	Sets the maximum lifetime of the cookie using a time in seconds.
path	/	Sets the path of the application where the cookie should be sent.

COOKIE: PHPSESSID

The cookie is missing Secure, HttpOnly and SameSite flags, make sure it does not store sensitive information. Misconfiguration or weakness

Raw HTTP Header

Set-Cookie: PHPSESSID=2tphflkg4uaed2dp79gq13fro4; path=/

Attributes

Name	Value	Description
path	/	Sets the path of the application where the cookie should be sent.