Summary of rff-dev.ectostarservers.com Website Security

FINAL GRADE

A

DNS

SERVER IP
199.195.116.144

REVERSE DNS
199.195.116.144.static.a2webhostin…

INFO

DATE OF TEST
November 12th 2019, 11:11

SERVER LOCATION
Portage 🇺🇸

Web Server Analysis

HTTP RESPONSE

401 Authorization Required

REDIRECT TO

N/A

NPN

N/A

ALPN

No

CONTENT ENCODING

GZIP

SERVER SIGNATURE

Apache/2.2.15 CentOS

WAF

No WAF detected

LOCATION

A2 Hosting, Inc.

HTTP METHODS ENABLED

✓ GET ✓ POST ✓ HEAD ✓ OPTIONS ✓ DELETE ✓ PUT ✓ TRACE ✓ TRACK ✓ CUSTOM

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

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 is missing or insecure. Misconfiguration or weakness

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

Expect-CT Feature-Policy

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin

SERVER

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

Raw HTTP Header

Server: Apache/2.2.15 (CentOS)

STRICT-TRANSPORT-SECURITY

The header should not be sent through HTTP. Misconfiguration or weakness

Raw HTTP Header

Strict-Transport-Security: max-age=31536000

Directives

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

X-FRAME-OPTIONS

The header is properly set. Good configuration

Raw HTTP Header

X-Frame-Options: SAMEORIGIN

X-XSS-PROTECTION

The header is properly set. Dangerous web pages with the most frequent XSS payloads will be blocked by the browser. Good configuration

Raw HTTP Header

X-XSS-Protection: 1; mode=block

X-CONTENT-TYPE-OPTIONS

The header is properly set. Good configuration

Raw HTTP Header

```
X-Content-Type-Options: nosniff
```

Content Security Policy Analysis

CONTENT-SECURITY-POLICY

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

Cookies Security Analysis

No cookies were sent by the web application. Information