Summary of login.cloudcc.com Website Security Test

FINAL GRADE

A

DNS

SERVER IP
47.254.56.253

REVERSE DNS
-

INFO

DATE OF TEST
May 7th 2020, 07:56

SERVER LOCATION
San Mateo

Web Server Analysis

HTTP RESPONSE
200

REDIRECT TO
N/A

NPN
H2 HTTP/1.1

ALPN
Yes

CONTENT ENCODING
None

SERVER SIGNATURE
N/A

WAF
No WAF detected

LOCATION
N/A

HTTP METHODS ENABLED

GET POST HEAD OPTIONS DELETE PUT CONNECT 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 were fingerprinted on the website. Information

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

jQuery 3.5.1

The fingerprinted component version is up2date, no security issues were found.

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 is found on the website. Good configuration

WEBSITE SOFTWARE SECURITY

No vulnerabilities found in the website CMS or its components. Good configuration

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 and its components seem to be up2date. Implement continuous monitoring for new security updates. Good configuration

REQUIREMENT 6.5

No publicly known vulnerabilities seem to be present in the fingerprinted versions the website CMS and its components. 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

Feature-Policy

MISSING OPTIONAL HTTP HEADERS

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

SERVER

The header was not sent by the server. Good configuration

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.

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 page content with the most frequent XSS payloads will be sanitized by the browser. Good configuration

Raw HTTP Header

X-XSS-Protection: 1

X-CONTENT-TYPE-OPTIONS

The header is properly set. Good configuration

Raw HTTP Header

X-Content-Type-Options: nosniff

EXPECT-CT

The header is not properly set. Misconfiguration or weakness

Raw HTTP Header

Expect-CT: enforce

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