Content Security Policy and Security Headers Test of https://mrcloud01.recordservices.net

Test your Content Security Policy (CSP), HTTP Security Headers and overall web server security.

Assessment of mrcloud01.recordservices.net Executive Summary

FINAL GRADE

A+

DNS

SERVER IP
13.88.20.159

REVERSE DNS
-

INFO

DATE OF TEST
February 22nd 2017, 01:39 CET

SERVER LOCATION
San Jose, United States

Web Server Security Overview

TESTED URL

https://mrcloud01.recordservices.net

REDIRECT TO

N/A

HTTP RESPONSE

200 OK

NEXT PROTOCOL NEGOTIATION

No

APPLICATION-LAYER PROTOCOL NEGOTIATION

No

CONTENT ENCODING

None

HTTP METHODS OVERVIEW

✓ GET ✓ POST ℹ HEAD ℹ OPTIONS

HTTP HEADERS OVERVIEW

✓ Server ✓ X-Powered-By ✓ Strict-Transport-Security ✓ Public-Key-Pins ✓ X-Frame-Options ✓ X-XSS-Protection

✓ X-Content-Type-Options ℹ Content-Security-Policy

COOKIES OVERVIEW

Cookie name:

✓ Yacht

HTTP Headers Security Analysis

SERVER

The header was not sent by the server. Good configuration

X-POWERED-BY

Webserver does not send detailed information about its version. Good configuration

Raw HTTP Header

X-Powered-By: ASP.NET

STRICT-TRANSPORT-SECURITY

The header is properly set. Good configuration

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.

PUBLIC-KEY-PINS

The header is properly set. **Good configuration**

Raw HTTP Header

Public-Key-Pins: pin-sha256="ixhQvkuKYVw+tdzmLB2Z3Fq1J2l3r0zkjVqmw4MlxbI="; pin-sha256=
"keduhseXI/jGKRlgTjMACweWTZt7DDut4tFy/VLwCuc=" ; max-age=5184000; includeSubDomains

Directives

Name	Description
pin-sha256	Sets the pins that browsers must record.
max-age	Sets the time browsers must record the allowed pins.
includeSubDomains	Used to record the same pins for other subdomains of your website.

X-FRAME-OPTIONS

The header is properly set. **Good configuration**

Raw HTTP Header

X-Frame-Options: SAMEORIGIN

Directives

Name	Description
SAMEORIGIN	Allows browsers to display this content in a frame from the same origin than itself.

X-XSS-PROTECTION

The header is properly set. **Good configuration**

Raw HTTP Header

X-XSS-Protection: 1; mode=block

Directives

Name	Description
1	Forces browsers to enable heuristic protection against reflected XSS attacks.
mode=block	Forces browsers to block server's response when heuristic protection detects an XSS.

X-CONTENT-TYPE-OPTIONS

The header is properly set. Good configuration

Raw HTTP Header

X-Content-Type-Options: nosniff

Directives

Name	Description
nosniff	Disables browser ability to detect content type by analyzing it and allows to prevent XSS for example.

CONTENT-SECURITY-POLICY

Content-Security Policy is enforced. Good configuration

Some directives have values that are too permissive, like wildcards. Information

Some directives have value considered as unsafe. Information

Raw HTTP Header

Content-Security-Policy: default-src 'self'; connect-src ##RPL0## font-src ##RPL1## child-src ##RPL2## img-src ##RPL3## media-src ##RPL4## object-src ##RPL5## script-src 'self' ##RPL6## ##RPL7## style-src 'self' 'unsafe-inline'

Directives

Name	Description
default-src	Sets the list of sources where browsers are allowed to get every resource from, if not specified in another directive.
connect-src	Sets the list of servers that browsers are allowed to connect to, for instance with WebSockets.
font-src	Sets the list of sources where browsers are allowed to get fonts from.
child-src	Sets the list of sources that can be included in frames or iframes.
img-src	Sets the list of sources where browsers are allowed to get images from.
media-src	Sets the list of sources where browsers are allowed to get media from, such as videos, audio...
object-src	Sets the list of sources where browsers are allowed to get plugin content from.
script-src	Sets the list of sources where browsers are allowed to get scripts from.
style-src	Sets the list of sources where browsers are allowed to get style sheets from.

Cookies Security Analysis

COOKIE: "YACHT"

The cookie has the following attributes set: Secure attribute; HttpOnly attribute. Good configuration

Raw HTTP Cookie

Set-Cookie: Yacht=SessionId=55045213D64D4A1D87B04D01786FB85B; path=/; ##RPL0## Secure

Attributes

Name	Value	Description
path	/	Sets the path of the application where the cookie should be sent.
httponly	✓	Prevents client-side scripts to access the cookie by telling browsers to only transmit the cookie over HTTP(S).
secure	✓	Prevents browsers to send this cookie over an insecure connection.