Summary of anonform.com [Desktop Version] Website Security Test

FINAL GRADE

A+

DNS

SERVER IP
51.195.41.240

REVERSE DNS
web1.anonform.com

CLIENT
Desktop Browser

INFO

DATE OF TEST
February 23rd 2021, 15:13

SERVER LOCATION
London 🇬🇧

Web Server Security Test

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

CONTENT ENCODING	SERVER SIGNATURE	WAF	LOCATION
BR	ANON	Custom	N/A

HTTP METHODS ENABLED

✓ GET ✓ POST ✓ HEAD

Software Security Test

FINGERPRINTED CMS & VULNERABILITIES

No CMS were fingerprinted on the website. Information

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

No components were fingerprinted on the website. Information

GDPR Compliance Test

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

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 Compliance Test

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

All HTTP headers related to security and privacy are properly set and configured. Good configuration

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin Public-Key-Pins Public-Key-Pins-Report-Only Expect-CT Permissions-Policy

SERVER

Web server does not disclose its version. Good configuration

Raw HTTP Header

Server: ANON

STRICT-TRANSPORT-SECURITY

The header is properly set. Good configuration

Raw HTTP Header

Strict-Transport-Security: max-age=63072000; 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 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 Test

CONTENT-SECURITY-POLICY

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

Some directives have value considered as unsafe. Information

Content-Security Policy is enforced. Good configuration

Raw HTTP Header

Content-Security-Policy: default-src 'self'; connect-src 'self' ; img-src 'self' https://ps.w.org https://www.google.com https://embedwistia-a.akamaihd.net data:; media-src 'self' data:; script-src 'self' https://www.googletagmanager.com https://browser-update.org https://www.google-analytics.com 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; frame-src 'self' data:; manifest-src 'self';

Directives

Name	Description
default-src	Sets the list of sources where browser is allowed to get every resource from, if not specified in another directive.
connect-src	Sets the list of servers that browser is allowed to connect to, for instance with WebSockets.
img-src	Sets the list of sources where browser is allowed to get images from.
media-src	Sets the list of sources where browser is allowed to get media (e.g. video, or audio).
script-src	Sets the list of sources where browser is allowed to get scripts from.

Name	Description
style-src	Sets the list of sources where browser is allowed to get style sheets from.
font-src	Sets the list of sources where browser is allowed to get fonts from.
frame-src	Deprecated and replaced by "child-src" parameter. Sets the list of sources that can be included in frames or iframes.
manifest-src	Sets the list of sources where browser is allowed to get application manifest from.

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. Good configuration

External Content Security Test

EXTERNAL CONTENT ON HOMEPAGE

External web content (e.g. images, video, CSS or JavaScript) can improve website loading time. However, the external content can also put privacy of website visitors at risk given that some information about them is transmitted to the third parties operating the external resources, sometimes even without proper HTTPS encryption or user consent.

External Requests	Failed Requests
19	0

c0.wp.com

https://c0.wp.com/c/5.6.2/wp-includes/js/jquery/jquery-migrate.min.js

https://c0.wp.com/p/jetpack/9.4/_inc/build/photon/photon.min.js

https://c0.wp.com/c/5.6.2/wp-includes/js/wp-embed.min.js

https://c0.wp.com/p/jetpack/9.4/_inc/build/widgets/eu-cookie-law/eu-cookie-law.min.js

https://c0.wp.com/c/5.6.2/wp-includes/js/jquery/jquery.min.js

www.googletagmanager.com

https://www.googletagmanager.com/gtag/js?id=UA-189811076-1

stats.wp.com

https://stats.wp.com/e-202108.js

www.google-analytics.com

https://www.google-analytics.com/analytics.js

https://www.google-analytics.com/plugins/ua/linkid.js

pixel.wp.com

https://pixel.wp.com/g.gif?v=ext&j=1%3A9.4&blog=189463143&post=40&tz=2&srv=anonform.com&ho…

fonts.gstatic.com

https://fonts.gstatic.com/s/ptsans/v12/jizaRExUiTo99u79D0yEww.woff

https://fonts.gstatic.com/s/ptsans/v12/jizfRExUiTo99u79B_mh0OCtKw.woff

https://fonts.gstatic.com/s/ptsans/v12/jizdRExUiTo99u79D0e8fOydIRUb.woff

i1.wp.com

https://i1.wp.com/anonform.com/wp-content/uploads/2020/12/secure-mail.jpg?resize=1230%2C500&

https://i1.wp.com/anonform.com/wp-content/uploads/2021/01/consultant.jpg?resize=330%2C240&ssl=1

browser-update.org

https://browser-update.org/update.min.js

https://browser-update.org/update.show.min.js

i0.wp.com

https://i0.wp.com/anonform.com/wp-content/uploads/2020/12/secure-website.jpg?resize=330%2C240…

i2.wp.com

https://i2.wp.com/anonform.com/wp-content/uploads/2021/01/whistleblower.jpg?resize=330%2C240&s…