Summary of netvibes.dk [Desktop Version] Website Security Test

FINAL GRADE

A+

DNS

SERVER IP
93.191.156.196

REVERSE DNS
linux306.unoeuro.com

CLIENT
Desktop Browser

INFO

DATE OF TEST
February 7th 2022, 23:19

SERVER LOCATION
Skibby

Software Security Test	EU GDPR Compliance Test	PCI DSS Compliance Test	Content Security Policy Test	HTTP Headers Security Test
NO ISSUES FOUND	NO ISSUES FOUND	NO ISSUES FOUND	NO MAJOR ISSUES FOUND	NO ISSUES FOUND

Web Server Security Test

HTTP RESPONSE
200

HTTP VERSIONS
HTTP/1.1 HTTP/2

NPN
N/A

ALPN
H2

CONTENT ENCODING
None

SERVER SIGNATURE
Apache

WAF
Mod_Security2

LOCATION
N/A

HTTP METHODS ENABLED

GET HEAD OPTIONS DELETE PUT TRACK CUSTOM

HTTP REDIRECTS

1. http://netvibes.dk/
2. https://netvibes.dk/

Web 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 was found on the website. Good configuration

WEBSITE SECURITY

Website CMS and its components could not have been reliably fingerprinted.
Ensure that they are up2date. Information

TLS ENCRYPTION

HTTPS encryption is present on the web server. Good configuration

COOKIE PROTECTION

No cookies with personal or tracking information seem to be sent. Information

COOKIE DISCLAIMER

No third-party cookies or cookies with 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 they are 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 Test

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

MISSING OPTIONAL HTTP HEADERS

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

SERVER

Web server does not disclose its version. Good configuration

Raw HTTP Header

Server: Apache

STRICT-TRANSPORT-SECURITY

The header is properly set. Good configuration

Raw HTTP Header

strict-transport-security: max-age=31536000; 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 value is not consistent with Content-Security-Policy. Information

The header is properly set. Good configuration

Raw HTTP Header

x-frame-options: sameorigin

X-CONTENT-TYPE-OPTIONS

The header is properly set. Good configuration

Raw HTTP Header

x-content-type-options: nosniff

PERMISSIONS-POLICY

The header is properly set. Good configuration

Raw HTTP Header

Permissions-Policy: geolocation=self

REFERRER-POLICY

The header is properly set. Good configuration

Raw HTTP Header

referrer-policy: no-referrer

Content Security Policy Test

CONTENT-SECURITY-POLICY

Some directives have values that are too permissive. Misconfiguration or weakness

The header is not consistent with other headers. Information

Content-Security Policy is enforced. Good configuration

Raw HTTP Header

Content-Security-Policy: default-src 'self' data: ; frame-ancestors 'none'

Directives

Name	Description

Name	Description
default-src	The default-src directive serves as a fallback for the other fetch directives. `*` - resources can be loaded from any source, which is inherently risky. `'unsafe-inline'` - allowing inline code execution can be dangerous, as it can often be exploited by intruders. `'unsafe-eval'` - using eval makes it possible to execute malicious code.
frame-ancestors	Restricts the URLs which can embed the resource using frame, iframe, object, or embed.

CONTENT-SECURITY-POLICY-REPORT-ONLY

The header was not sent by the server. Information

Cookies Privacy and Security Analysis

No cookies were sent by the web application. Good configuration

External Content Privacy and Security Analysis

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 HTTP Requests	Failed HTTP Requests
8	0

cdn-cookieyes.com

https://cdn-cookieyes.com/client_data/11b01f5f80bdb61110fcc6d0/script.js

www.googletagmanager.com

https://www.googletagmanager.com/gtag/js?id=UA-198623725-1

https://www.googletagmanager.com/gtm.js?id=GTM-N4993WK

www.google-analytics.com

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

https://www.google-analytics.com/j/collect?v=1&_v=j96&aip=1&a=116686186&t=pageview&_s=1&dl=https%3A%2F%2Fnetvib…

stats.g.doubleclick.net

https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j96&tid=UA-198623725-1&cid=1569382534.1644272334&ji…

www.google.ca

https://www.google.ca/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j96&tid=UA-198623725-1&cid=1569382534.164…

www.google.com

https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j96&tid=UA-198623725-1&cid=1569382534.1…