Summary of www.links.hr [Desktop Version] Website Security Test

links.hr was tested 2 times during the last 12 months.

Tested on:	Sep 6th, 2022 13:32:33 GMT+2
Server IP:	168.119.143.57
Reverse DNS:	static.57.143.119.168.clients.your-server.de
Location:	Leawood 🇺🇸
Client:	Desktop Version

Your final score

A
B
C
F

F

Software Security Test

4 ISSUES FOUND

EU GDPR Compliance Test

2 ISSUES FOUND

PCI DSS Compliance Test

3 ISSUES FOUND

Content Security Policy Test

MISSING

HTTP Headers Security Test

NO MAJOR ISSUES FOUND

Discovered Subdomains

Tested URL	Protocol/Port	Certificate(s)	Tested on	Compliances	Grade
links.hr	HTTP / 80	❓	Not tested yet		❓
links.hr	HTTPS / 443	🌊	Feb 27th, 2019 07:45:41 GMT+1		F
support.links.hr	HTTP / 80	❓	Not tested yet		❓
support.links.hr	HTTPS / 443	🌊	Not tested yet		❓

SHOW 26 MORE

Web Server Security Test

HTTP RESPONSE	HTTP VERSIONS	NPN	ALPN
200	HTTP/1.0 HTTP/1.1 HTTP/2	N/A	H2

CONTENT ENCODING	SERVER SIGNATURE	WAF	LOCATION
None	Microsoft-IIS/10.0	No WAF detected	N/A

HTTP METHODS ENABLED

✓ GET   ✓ HEAD   ✓ OPTIONS   ✓ DELETE   ✓ CONNECT   ✓ TRACE   ✓ TRACK   ✓ CUSTOM

Web Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities
5	4	9

Fingerprinted CMS & Vulnerabilities

> No CMS were fingerprinted on the website.   Information

Fingerprinted CMS Components & Vulnerabilities

jQuery   1.10.2

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **3.6.1**.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.5 Medium	CVE-2020-11022	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 - Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-400 - Prototype pollution
4.1 Medium	CVE-2020-11023	CWE-79 - Cross-site scripting

jQuery UI   1.10.3

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **1.13.2**.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.5 Medium	CVE-2021-41184	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41182	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41183	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2016-7103	CWE-79 - Cross-site scripting
4.1 Medium	CVE-2022-31160	CWE-79 - Cross-site scripting

Modernizr   2.8.3

The component is outdated. No known security vulnerabilities found. Update to the most recent version **3.11.8**.

Core-js   3.0.0

The component is outdated. No known security vulnerabilities found. Update to the most recent version **3.25.0**.

Hammer.js   2.0.8

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

GDPR Compliance Test

If the website processes or stores personal data of the 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 or its components are outdated and contain publicly known security vulnerabilities.   Misconfiguration or weakness

TLS ENCRYPTION

HTTPS encryption is present on the web server.   Good configuration

COOKIE PROTECTION

Cookies with personal or tracking information are sent without Secure flag.   Misconfiguration or weakness

COOKIE DISCLAIMER

Third-party cookies or cookies with tracking information are sent, cookie disclaimer was found on the website.   Good configuration

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 or its components seem to be outdated. Check for available updates.   Misconfiguration or weakness

REQUIREMENT 6.5

Fingerprinted website CMS or its components contain publicly known vulnerabilities (Ref. PCI DSS 6.5.1-6.5.10).

Misconfiguration or weakness

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

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

Misconfiguration or weakness

MISSING REQUIRED HTTP HEADERS

Strict-Transport-Security   X-Content-Type-Options

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin   Permissions-Policy

SERVER

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

Misconfiguration or weakness

Server

Server: Microsoft-IIS/10.0

X-ASPNET-VERSION

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

X-AspNet-Version

x-aspnet-version: 4.0.30319

X-FRAME-OPTIONS

The header is properly set.   Good configuration

X-Frame-Options

x-frame-options: SAMEORIGIN

Content Security Policy Test

CONTENT-SECURITY-POLICY

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

CONTENT-SECURITY-POLICY

The header was not sent by the server.   Information

Cookies Privacy and Security Analysis

Some cookies have missing secure flags or attributes.	Misconfiguration or weakness

COOKIE: NOP.CUSTOMER

The cookie has HttpOnly attribute set.	Good configuration

The cookie is missing Secure and SameSite flag. Make sure it does not store sensitive information.	Misconfiguration or weakness

Raw HTTP Header

set-cookie: Nop.customer=e815c8e2-9984-491b-b61a-b9da2e8ccc66; expires=Wed, 06-Sep-2023 11:28:21 GMT; path=/; HttpOnly

Directives

Name	Value	Description
expires	Wed, 06-Sep-2023 11:28:21 GMT	Sets the maximum lifetime of the cookie using a date.
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).

COOKIE: __REQUESTVERIFICATIONTOKEN

The cookie has HttpOnly attribute set.	Good configuration

The cookie is missing Secure and SameSite flag. Make sure it does not store sensitive information.

Misconfiguration or weakness

Raw HTTP Header

set-cookie:

__RequestVerificationToken=npVfkVW_OXOd3C12miX9AGEkMIXal3sZvyTdoHRpJG9Qw6_8BnltrBUVzdYGmHUTdqxrGYp11LVpuy9Q5F5gEy_PeE4dV0EH

xLJ248JgFFQ1; path=/; HttpOnly

Directives

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).

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

<div style="text-align:center">

28

0

</div>

clickvox.links.hr

https://clickvox.links.hr/site-contact/main.css

https://clickvox.links.hr/site-contact/main.js

https://clickvox.links.hr/api/customerChat/availableAgentCount

cdn.midas-network.com

https://cdn.midas-network.com/MidasPixel/IndexAsync/35a72d17-497d-4808-849b-04ea36abae6b

www.positivessl.com

https://www.positivessl.com/images/seals/positivessl_trust_seal_sm_124x32.png

www.google-analytics.com

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

https://www.google-analytics.com/j/collect?v=1&_v=j96&a=1660653759&t=pageview&_s=1&dl=https%

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

https://www.google-analytics.com/collect?v=1&_v=j96&a=1660653759&t=event&ni=1&_s=2&dl=ht

connect.facebook.net

https://connect.facebook.net/en_US/fbevents.js

https://connect.facebook.net/signals/config/597046670501261?v=2.9.79&r=stable

www.googletagmanager.com

https://www.googletagmanager.com/gtm.js?id=GTM-KJ9378Z

s-eu-1.pushpushgo.com

https://s-eu-1.pushpushgo.com/js/61012cd804b7f5abc12634fc.js

https://s-eu-1.pushpushgo.com/scripts/6307585bea9c73823ecd1642/sentry.js

https://s-eu-1.pushpushgo.com/scripts/6307585bea9c73823ecd1642/plugin-push.js

https://s-eu-1.pushpushgo.com/scripts/6307585bea9c73823ecd1642/plugin-beacon.js

https://s-eu-1.pushpushgo.com/scripts/6307585bea9c73823ecd1642/plugin-geolocation.js

www.redditstatic.com

https://www.redditstatic.com/ads/pixel.js

chimpstatic.com

https://chimpstatic.com/mcjs-connected/js/users/6ca3c77b6a4d20cf7f9756697/cf828b203d92e1ed9f7960805.js

static.hotjar.com

https://static.hotjar.com/c/hotjar-1974920.js?sv=7

stats.g.doubleclick.net

https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j96&tid=UA-1498380-1&cid=95

alb.reddit.com

https://alb.reddit.com/rp.gif?ts=1662463715928&id=t2_3wcw41mp&event=PageVisit&m.itemCount=&m.val

script.hotjar.com

https://script.hotjar.com/modules.d5eb3c97b67a0b8958ff.js

www.facebook.com

https://www.facebook.com/tr/?id=597046670501261&ev=PageView&dl=https%3A%2F%2Fwww.links.hr%2Fhr%2Fregi

https://www.facebook.com/tr/?id=597046670501261&ev=Microdata&dl=https%3A%2F%2Fwww.links.hr%2Fhr%2Fregi

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-149838

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-14983

vars.hotjar.com

https://vars.hotjar.com/box-1ada912494ba7fc7aca15fcef1c2a7ae.html