Summary of ehr-online.co.uk [Desktop Version] Website Security Test

YOUR FINAL SCORE

C

DNS

SERVER IP
68.66.247.187

REVERSE DNS
68.66.247.187.static.a2webhosting.c…

CLIENT
Desktop Browser

INFO

DATE OF TEST
June 20th 2022, 21:28

SERVER LOCATION
Farmington

Software Security Test	EU GDPR Compliance Test	PCI DSS Compliance Test	Content Security Policy Test	HTTP Headers Security Test
1 ISSUE FOUND	3 ISSUES FOUND	3 ISSUES FOUND	MISSING	NO MAJOR ISSUES FOUND

This test was made **34 days ago** and may be outdated

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
No WAF detected

LOCATION
A2 Hosting, Inc.

HTTP METHODS ENABLED

GET POST HEAD OPTIONS DELETE PUT TRACK CUSTOM

HTTP REDIRECTS

1. https://ehr-online.co.uk/
2. https://ehr-online.co.uk/interface/login/login.php?site=default

Web Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities
2	1	6

FINGERPRINTED CMS & VULNERABILITIES

LibreHealth EHR

CMS version is unknown. Make sure the CMS is up2date.

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

jQuery 1.4.3

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **3.6.0**.

CVSSv3.1 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.5 Medium	CVE-2020-7656	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2020-11022	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 — Cross-site scripting
5.3 Medium	Not Assigned, see 4 references: • http://www.openwall.com/lists/oss-security/2013/01/31/3 • http://blog.jquery.com/2011/09/01/jquery-1-6-3-released/ • https://bugs.jquery.com/ticket/9521 • https://www.cybersecurity-help.cz/vdb/SB2011060701	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

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 not found on the website or is not easily accessible. — Misconfiguration or weakness

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Website CMS or its components are outdated and contain publicly known security vulnerabilities.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 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 Permissions-Policy

SERVER

Web server does not disclose its version. Good configuration

Raw HTTP Header

Server: Apache

X-POWERED-BY

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

Raw HTTP Header

x-powered-by: PHP/7.4.29

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-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

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 Privacy and Security Analysis

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

COOKIE: LIBREHEALTHEHR

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

Raw HTTP Header

set-cookie: LibreHealthEHR=4de1fb93dcb0c34f964dcda4a3b89b9e; path=/

Attributes

Name	Value	Description
path	/	Sets the path of the application where the cookie should be sent.

External Content Privacy and Security Analysis

No external content found on tested page. Information