Summary of nismphp-env.eba-ytbpbyww.us-ea... [Desktop Version] Website Security Test

FINAL GRADE

C

DNS

SERVER IP
18.209.2.175

REVERSE DNS
ec2-18-209-2-175.compute-1.amazo...

CLIENT
Desktop Browser

INFO

DATE OF TEST
June 7th 2021, 01:07

SERVER LOCATION
Mount Hope

Software Security Test	GDPR Compliance Test	PCI DSS Compliance Test	Content Security Policy Test	Headers Security Test
2 ISSUES FOUND	3 ISSUES FOUND	3 ISSUES FOUND	MISSING	NO MAJOR ISSUES FOUND

Web Server Security Test

HTTP RESPONSE
200 OK

HTTP VERSIONS
HTTP/1.0 HTTP/1.1

NPN
N/A

ALPN
N/A

CONTENT ENCODING
None

SERVER SIGNATURE
Apache

WAF
No WAF detected

LOCATION
Massachusetts Institute of Technology

HTTP METHODS ENABLED
✓ GET ✓ POST ✓ HEAD ✓ OPTIONS ✓ DELETE ✓ PUT ✓ TRACK ✓ CUSTOM

Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities

2	2	11

FINGERPRINTED CMS & VULNERABILITIES

No CMS were fingerprinted on the website. Information

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

jQuery 1.8.3

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities.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

CVSSv3.0 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	CVE-2012-6708	CWE-79 — Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-400 — Prototype pollution
4.2 Medium	CVE-2020-11023	CWE-79 — Cross-site scripting

Bootstrap 2.2.2

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **5.0.1**.

CVSSv3.0 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.5 Medium	CVE-2018-14040	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14042	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14041	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20677	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20676	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Website CMS or its components are outdated and contain publicly known security vulnerabilities.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 missing or has known security weaknesses or misconfigurations. Misconfiguration or weakness

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 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 REQUIRED HTTP HEADERS

X-Frame-Options X-XSS-Protection X-Content-Type-Options

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin Expect-CT Permissions-Policy

SERVER

Web server does not disclose its version. Good configuration

Raw HTTP Header

```
Server: Apache
```

Content Security Policy Test

CONTENT-SECURITY-POLICY

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

Cookies Security Test

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
1	0

ajax.googleapis.com

http://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js