Summary of allthegear.org.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
July 17th 2022, 19:30

SERVER LOCATION
Farmington 🇺🇸

Software Security Test	EU GDPR Compliance Test	PCI DSS Compliance Test	Content Security Policy Test	Headers Security Test
5 ISSUES FOUND	1 ISSUE FOUND	3 ISSUES FOUND	MISSING	NO MAJOR 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
No WAF detected

LOCATION
A2 Hosting, Inc.

HTTP METHODS ENABLED
✓ GET ✓ HEAD

Web Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities

6	5	9

FINGERPRINTED CMS & VULNERABILITIES

Magento

CMS version is unknown. Make sure the CMS is up2date. Current most recent version is **2.4.4**.

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

jQuery 1.12.4

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities.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-2020-11022	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 Mobile

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **1.4.5**.

CVSSv3.1 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
6.2 Medium	Not Assigned, see 2 references: • https://snyk.io/vuln/SNYK-JS-JQUERYMOBILE-174599 • https://www.cybersecurity-help.cz/vdb/SB2019050912	CWE-79 — Cross-site scripting

jQuery UI 1.10.4

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities.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-IDCVE	Vulnerability TypeType
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

Lodash 1.8.2

The component is outdated. No known security vulnerabilities found. Update to the most recent version **4.17.21**.

RequireJS 2.1.11

The component is outdated. No known security vulnerabilities found. Update to the most recent version **2.3.6**.

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 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

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 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/7.4.30

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

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

X-Frame-Options is not consistent with Content-Security-Policy-Report-Only. Information

The header is not consistent with other headers. Information

Content-Security Policy is enforced. Good configuration

Raw HTTP Header

```
Content-Security-Policy-Report-Only: font-src *.yotpo.com *.googleapis.com *.gstatic.com data: 'self' ; form-action geostag.cardinalcommerce.com
geo.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.com centinelapistag.cardinalcommerce.com
centinelapi.cardinalcommerce.com secure.authorize.net test.authorize.net pilot-payflowlink.paypal.com *.amazon.com *.amazon.co.uk
*.amazon.co.jp *.amazon.jp *.amazon.it *.amazon.fr *.amazon.es *.amazon.de *.yotpo.com 'self' ; frame-ancestors 'self'; frame-src
geostag.cardinalcommerce.com geo.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.com
centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com secure.authorize.net test.authorize.net www.paypal.com
```

www.sandbox.paypal.com pilot-payflowlink.paypal.com player.vimeo.com assets.braintreegateway.com *.amazon.com *.amazon.co.uk *.amazon.co.jp *.amazon.jp *.amazon.it *.amazon.fr *.amazon.es *.amazon.de *.payments-amazon.com *.payments-amazon.co.uk *.payments-amazon.co.jp *.payments-amazon.jp *.payments-amazon.it *.payments-amazon.fr *.payments-amazon.es *.payments-amazon.de cdn.dnky.co webchat.dotdigital.com *.yotpo.com 'self' ; img-src widgets.magentocommerce.com data: www.googleadservices.com www.google-analytics.com t.paypal.com www.paypal.com www.paypalobjects.com fpdbs.paypal.com fpdbs.sandbox.paypal.com *.vimeocdn.com s.ytimg.com validator.swagger.io d3sbl0c71oxeok.cloudfront.net dhkkzdfmpzvap.cloudfront.net d2bpzs5y44q6e0.cloudfront.net d37shgu97oizpd.cloudfront.net d1zlqll3enr74n.cloudfront.net d1jynp0fpwn93a.cloudfront.net d2cb3tokgpwh3v.cloudfront.net d1re8bfxx3pw6e.cloudfront.net d35u8xwkxs8vpe.cloudfront.net d13s9xffygp5o.cloudfront.net d388nbw0dwi1jm.cloudfront.net d11p2vtu3dppaw.cloudfront.net d3r89hiip86hka.cloudfront.net dc7snq0c8ipyk.cloudfront.net d5c7kvljggzso.cloudfront.net d2h8yg3ypfzua1.cloudfront.net d1b556x7apj5fb.cloudfront.net draz1ib3z71v2.cloudfront.net dr6hdp4s5yzfc.cloudfront.net d2bomicxw8p7ii.cloudfront.net d3aypcdgvjnnam.cloudfront.net d2a3iuf10348gy.cloudfront.net d23yuld0pofhhw.cloudfront.net *.ssl-images-amazon.com *.ssl-images-amazon.co.uk *.ssl-images-amazon.co.jp *.ssl-images-amazon.jp *.ssl-images-amazon.it *.ssl-images-amazon.fr *.ssl-images-amazon.es *.ssl-images-amazon.de *.media-amazon.com *.media-amazon.co.uk *.media-amazon.co.jp *.media-amazon.jp *.media-amazon.it *.media-amazon.fr *.media-amazon.es *.media-amazon.de *.yotpo.com data: 'self' ; script-src assets.adobedtm.com geostag.cardinalcommerce.com 1eafstag.cardinalcommerce.com geoapi.cardinalcommerce.com 1eafapi.cardinalcommerce.com songbird.cardinalcommerce.com includestest.ccdc02.com www.googleadservices.com www.google-analytics.com secure.authorize.net test.authorize.net www.paypal.com www.sandbox.paypal.com www.paypalobjects.com t.paypal.com s.ytimg.com video.google.com vimeo.com www.vimeo.com *.vimeocdn.com js.authorize.net jstest.authorize.net cdn-scripts.signifyd.com www.youtube.com js.braintreegateway.com *.payments-amazon.com *.payments-amazon.co.uk *.payments-amazon.co.jp *.payments-amazon.jp *.payments-amazon.it *.payments-amazon.fr *.payments-amazon.es *.payments-amazon.de r1-t.trackedlink.net r2-t.trackedlink.net r3-t.trackedlink.net r1.trackedweb.net r2.trackedweb.net r3.trackedweb.net static.trackedweb.net cdn.dnky.co api.comapi.com webchat.dotdigital.com *.yotpo.com 'self' ; style-src getfirebug.com cdn.dnky.co webchat.dotdigital.com *.yotpo.com *.googleapis.com 'self' ; object-src 'self' ; media-src 'self' ; manifest-src 'self' ; connect-src geostag.cardinalcommerce.com geo.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.com centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com www.sandbox.paypal.com payments.sandbox.braintree-api.com origin-analytics-sand.sandbox.braintree-api.com assets.braintreegateway.com *.amazon.com *.amazon.co.uk *.amazon.co.jp *.amazon.jp *.amazon.it *.amazon.fr *.amazon.es *.amazon.de *.amazonpay.com *.amazonpay.co.uk *.amazonpay.co.jp *.amazonpay.jp *.amazonpay.it *.amazonpay.fr *.amazonpay.es *.amazonpay.de mws.amazonservices.com mws.amazonservices.co.uk mws.amazonservices.co.jp mws.amazonservices.jp mws.amazonservices.it mws.amazonservices.fr mws.amazonservices.es mws.amazonservices.de r1-t.trackedlink.net r2-t.trackedlink.net r3-t.trackedlink.net r1.trackedweb.net r2.trackedweb.net r3.trackedweb.net static.trackedweb.net api.comapi.com webchat.dotdigital.com *.yotpo.com 'self' ; child-src http: blob: 'self' ; default-src 'self' ; base-uri 'self' ;

Directives

Name	Description
font-src	Restricts the URLs from which font resources may be loaded. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.

Name	Description
form-action	Restricts the URLs which can be used as the target of a form submissions from a given context. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
frame-ancestors	Restricts the URLs which can embed the resource using frame, iframe, object, or embed.
frame-src	Restricts the URLs which may be loaded into nested browsing contexts (frames). 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
img-src	Restricts the URLs from which image resources may be loaded. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
script-src	Restricts the locations from which scripts may be executed. '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.
style-src	Restricts the locations from which style may be applied to a Document. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
object-src	Restricts the URLs from which plugin content may be loaded. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
media-src	Restricts the URLs from which video, audio, and associated text track resources may be loaded. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
manifest-src	Restricts the URLs from which application manifests may be loaded. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
connect-src	Controls requests which transmit or receive data from other origins using script interfaces. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.
child-src	Governs the creation of nested browsing contexts (e.g. frames) and Worker execution contexts. https: - allows any connections over the specified protocol; it’s recommended to strengthen this restriction by specifying the domains from which resources are allowed to be loaded. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.

Name	Description
default-src	The default-src directive serves as a fallback for the other fetch directives. '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.
base-uri	Restricts the URLs which can be used in a Document's base element. 'unsafe-inline' - allowing inline code execution can be dangerous, as it can often be exploited by intruders.

Cookies Privacy and Security Analysis

All cookies sent by the web application have secure flags and attributes. Good configuration

COOKIE: PHPSESSID

The cookie has Secure, HttpOnly and SameSite attributes set. Good configuration

Raw HTTP Header

set-cookie: PHPSESSID=1d8f68c6369465ec4ed83faa8ac0142d; expires=Sun, 17-Jul-2022 19:27:26 GMT; Max-Age=3600; path=/; domain=allthegear.org.uk; ; ; =

Attributes

Name	Value	Description
expires	Sun, 17-Jul-2022 19:27:26 GMT	Sets the maximum lifetime of the cookie using a date.
max-age	3600	Sets the maximum lifetime of the cookie using a time in seconds.
path	/	Sets the path of the application where the cookie should be sent.
domain	allthegear.org.uk	Sets the domains where browsers should send this cookie too.
secure	✓	Prevents browsers to send this cookie over an insecure connection.
httponly	✓	Prevents client-side scripts to access the cookie by telling browsers to only transmit the cookie over HTTP(S).
samesite	Lax	Prevents CSRF attacks by not sending the cookies when the request comes from another website.

External Content Privacy and Security Analysis

No external content found on tested page. Information