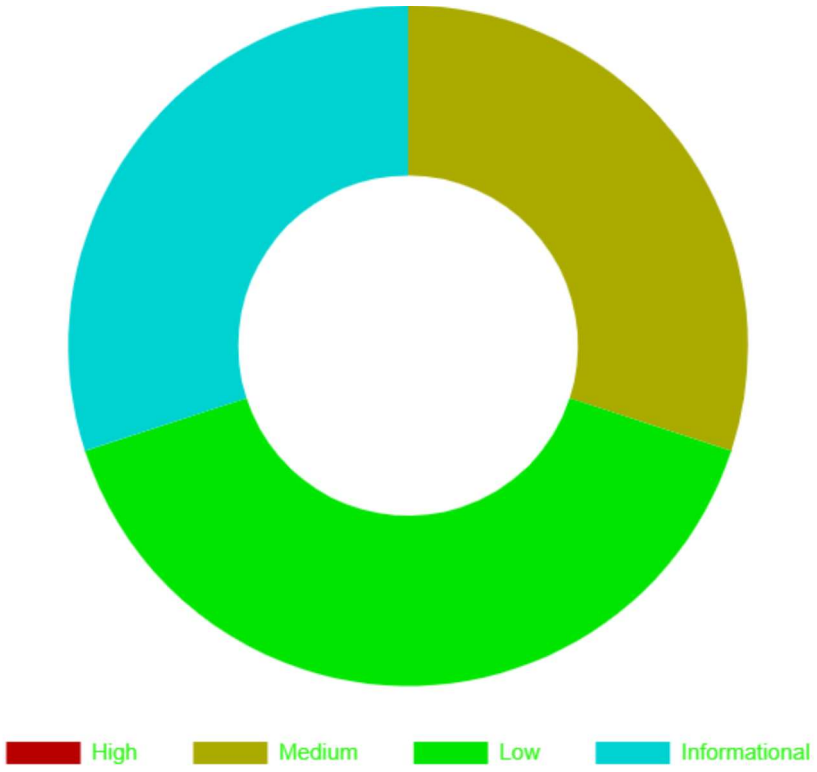
ZAP by Checkmarx Scanning Report

Generated on Mon, 4 May 2026 13:27:19

ZAP Version: 2.17.0

ZAP by Checkmarx



Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	4
Informational	3

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP warnings logged - see the zap.log file for details	4
Info	Informational	https://vertechie.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://vertechie.com	Percentage of endpoints with content type application/javascript	14 %
Info	Informational	https://vertechie.com	Percentage of endpoints with content type text/css	14 %
Info	Informational	https://vertechie.com	Percentage of endpoints with content type text/html	71 %
Info	Informational	https://vertechie.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://vertechie.com	Count of total endpoints	7
Info	Informational	https://vertechie.com	Percentage of slow responses	100 %

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	5
Missing Anti-clickjacking Header	Medium	5
Sub Resource Integrity Attribute Missing	Medium	5
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	Systemic
Strict-Transport-Security Header Not Set	Low	Systemic
Timestamp Disclosure - Unix	Low	1

X-Content-Type-Options Header Missing	Low	Systemic
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	5
Re-examine Cache-control Directives	Informational	4

Passing Rules

Name	Rule Type	Threshold	Strength
Script Active Scan Rules	Active	MEDIUM	MEDIUM
Private IP Disclosure	Passive	MEDIUM	-
Session ID in URL Rewrite	Passive	MEDIUM	-
Script Served From Malicious Domain (polyfill)	Passive	MEDIUM	-
ZAP is Out of Date	Passive	MEDIUM	-
Insecure JSF ViewState	Passive	MEDIUM	-
Java Serialization Object	Passive	MEDIUM	-
Vulnerable JS Library (Powered by Retire.js)	Passive	MEDIUM	-
In Page Banner Information Leak	Passive	MEDIUM	-
Charset Mismatch	Passive	MEDIUM	-
Cookie No HttpOnly Flag	Passive	MEDIUM	-
Cookie Without Secure Flag	Passive	MEDIUM	-
Cross-Domain JavaScript Source File Inclusion	Passive	MEDIUM	-
Content-Type Header Missing	Passive	MEDIUM	-
Application Error Disclosure	Passive	MEDIUM	-
Information Disclosure - Debug Error Messages	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in URL	Passive	MEDIUM	-

Information Disclosure - Sensitive Information in HTTP Referrer Header	Passive	MEDIUM	-
Off-site Redirect	Passive	MEDIUM	-
Cookie Poisoning	Passive	MEDIUM	-
User Controllable Charset	Passive	MEDIUM	-
User Controllable HTML Element Attribute (Potential XSS)	Passive	MEDIUM	-
Loosely Scoped Cookie	Passive	MEDIUM	-
Viewstate	Passive	MEDIUM	-
Directory Browsing	Passive	MEDIUM	-
Heartbleed OpenSSL Vulnerability (Indicative)	Passive	MEDIUM	-
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Passive	MEDIUM	-
X-Backend-Server Header Information Leak	Passive	MEDIUM	-
Secure Pages Include Mixed Content	Passive	MEDIUM	-
HTTP to HTTPS Insecure Transition in Form Post	Passive	MEDIUM	-
HTTPS to HTTP Insecure Transition in Form Post	Passive	MEDIUM	-
User Controllable JavaScript Event (XSS)	Passive	MEDIUM	-
Big Redirect Detected (Potential Sensitive Information Leak)	Passive	MEDIUM	-
Retrieved from Cache	Passive	MEDIUM	-
X-ChromeLogger-Data (XCOLD) Header Information Leak	Passive	MEDIUM	-
Cookie without SameSite Attribute	Passive	MEDIUM	-
CSP	Passive	MEDIUM	-
X-Debug-Token Information Leak	Passive	MEDIUM	-
Username Hash Found	Passive	MEDIUM	-
X-AspNet-Version Response Header	Passive	MEDIUM	-

PII Disclosure	Passive	MEDIUM	-
Script Passive Scan Rules	Passive	MEDIUM	-
Stats Passive Scan Rule	Passive	MEDIUM	-
Absence of Anti-CSRF Tokens	Passive	MEDIUM	-
Hash Disclosure	Passive	MEDIUM	-
Cross-Domain Misconfiguration	Passive	MEDIUM	-
Weak Authentication Method	Passive	MEDIUM	-
Reverse Tabnabbing	Passive	MEDIUM	-

Sites

https://vertechie.com

HTTP Response Code	Number of Responses
200 OK	14

No Authentication Statistics Found

Parameter Name	Type	Flags	Times Used	# Values

Alert Detail

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

URL	https://vertechie.com/
Node Name	https://vertechie.com/
Method	GET
Parameter	
Attack	
Evidence	
Show/hide Request and Response	
Request Header-size:	

228 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/contact

Node Name	https://vertechie.com/contact
Method	GET
Parameter	
Attack	
Evidence	
Show/hide Request and Response	

Request Header-size: 292 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size

: 929 bytes.

URL https://vertechie.com/favicon.svg

Node Name https://vertechie.com/favicon.svg

Method GET

Parameter

Attack

Evidence

Show/hide Request and Response

Request Head

er
-
si
ze
:
27
2
by
te
s.

Re
qu
es
t
Bo
dy
-
si
ze
:
0
by
te
s.

Re
sp
on
se
He
ad
er
-
si
ze
:
24
7
by
te
s.

Re
sp
on
se
Bo
dy
-
si
ze
:
92
9
by
te
s.

URL	https://vertechie.com/robots.txt
Node Name	https://vertechie.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Show/hide Request and Response	
Request Header-size: 238	

bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/sitemap.xml

Node https://vertechie.com/sitemap.xml

Name

Method GET

Parameter

Attack

Evidence

Show/hide Request and Response

Request Header-size: 239 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/

	https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
Tags	CWE-693 OWASP_2021_A05 OWASP_2017_A06 POLICY_QA_STD = POLICY_PENTEST = SYSTEMIC
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://vertechie.com/
Node Name	https://vertechie.com/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	

Show/hide Request and Response

Request Header-size: 228 bytes.

Request Body-size: 0 bytes.

Response Header-size

: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/contact

Node Name https://vertechie.com/contact

Method GET

Parameter x-frame-options

Attack

Evidence

Show/hideRe

quest and Response

Request Header-size: 292 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body - size: 929 bytes.	
URL	https://vertechie.com/favicon.svg
Node Name	https://vertechie.com/favicon.svg
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Show/hide Request and Resp	

onse

Request Header-size: 272 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body

- size: 929 bytes.	
URL	https://vertechie.com/robots.txt
Node Name	https://vertechie.com/robots.txt
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Show/hide Request and Response	
Request	

t
He
ad
er
-
si
ze
:
23
8
by
te
s.

Re
qu
es
t
Bo
dy
-
si
ze
:
0
by
te
s.

Re
sp
on
se
He
ad
er
-
si
ze
:
24
7
by
te
s.

Re
sp
on
se
Bo
dy
-
si
ze
:
92
9
by

tes.	
URL	https://vertechie.com/sitemap.xml
Node Name	https://vertechie.com/sitemap.xml
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Show/hide Request and Response	
Request Header-size	

: 239 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

Instances 5

	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.
Solution	If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
Tags	OWASP_2021_A05 POLICY_QA_STD = POLICY_PENTEST = CWE-1021 SYSTEMIC WSTG-v42-CLNT-09 OWASP_2017_A06
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Sub Resource Integrity Attribute Missing**
Description	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL	https://vertechie.com/
Node Name	https://vertechie.com/
Method	GET
Parameter	

Attack

Evidence

```
<link href="https://fonts.googleapis.com/css2?
family=Inter:wght@300;400;500;600;700&display=swap" rel="stylesheet"
/>
```

Show/hide Request and Response

Request Header-size: 228 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/contact

Node Name https://vertechie.com/contact

Method GET

Parameter

Attack

Evidence

```
<link href="https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;600;700&display=swap" rel="stylesheet" />
```

Show/hide Request and Response

Request Header-size: 292 bytes.

Request Body-size: 0 bytes.

Response

Header-size: 247 bytes.	
ResponseBody-size: 929 bytes.	
URL	https://vertechie.com/favicon.svg
NodeName	https://vertechie.com/favicon.svg
Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;600;700&display=swap" rel="stylesheet" />

Show/hide Request and Response

Request Header-size: 272 bytes.

Request Body-size: 0 bytes.

Response Header-size

: 247 bytes.	
Response Body-size: 929 bytes.	
URL	https://vertechie.com/robots.txt
Node Name	https://vertechie.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;600;700&display=swap" rel="stylesheet" />
Show/hide Re	

quest and Response

Request Header-size: 238 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body - size: 929 bytes.

URL https://vertechie.com/sitemap.xml

Node Name https://vertechie.com/sitemap.xml

Method GET

Parameter

Attack

Evidence <link href="https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;600;700&display=swap" rel="stylesheet" />

Show/hide Request and Resp

onse

Request Header-size: 239 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body

- size: 929 bytes.	
Instances	5
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
Tags	CWE-345 OWASP_2021_A05 POLICY_QA_STD = POLICY_PENTEST = SYSTEMIC OWASP_2017_A06 POLICY_DEV_STD =
CWE Id	345
WASC Id	15
Plugin Id	90003

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://vertechie.com/
Node Name	https://vertechie.com/
Method	GET

Parameter	
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Show/hide Request and Response	
Request Header-size: 228 bytes.	
Request Body-si	

ze: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/assets/index-DXqeRgIr.css

Node Name https://vertechie.com/assets/index-DXqeRgIr.css

Method GET

Parameter

Attack

Evidence nginx/1.24.0 (Ubuntu)

Show/hide Request and Response

Request Header-size: 286 bytes.

Request Body-size: 0 bytes.

Response Header-size: 246 bytes.

Response Body-size: 921 bytes.

URL https://vertechie.com/favicon.svg

Node Name https://vertechie.com/favicon.svg

Method GET

Parameter

Attack

Evidence: nginx/1.24.0 (Ubuntu)

Show/hide Request and Response

Request Header-size: 272 bytes.

Request Body-size: 0 bytes.

Response

Header-size: 247 bytes.	
ResponseBody-size: 929 bytes.	
URL	https://vertechie.com/robots.txt
NodeName	https://vertechie.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0 (Ubuntu)

Show/hide Request and Response

Request Header-size: 238 bytes.

Request Body-size: 0 bytes.

Response Header-size

: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/sitemap.xml

Node Name https://vertechie.com/sitemap.xml

Method GET

Parameter

Attack

Evidence nginx/1.24.0 (Ubuntu)

Show/hide Re

quest and Response

Request Header-size: 239 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body - size: 929 bytes.	
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
Tags	OWASP_2021_A05 POLICY_QA_STD = POLICY_PENTEST = SYSTEMIC OWASP_2017_A06 WSTG-v42-INFO-02 CWE-497
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://vertechie.com/

Node Name	https://vertechie.com/
Method	GET
Parameter	
Attack	
Evidence	
Show/hide Request and Response	

Request Header-size: 228 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size

: 929 bytes.

URL https://vertechie.com/assets/index-DXqeRgIr.css

Node Name https://vertechie.com/assets/index-DXqeRgIr.css

Method GET

Parameter

Attack

Evidence

Show/hide Request and Response

Request Head

er
-
si
ze
:
28
6
by
te
s.

Re
qu
es
t
Bo
dy
-
si
ze
:
0
by
te
s.

Re
sp
on
se
He
ad
er
-
si
ze
:
24
6
by
te
s.

Re
sp
on
se
Bo
dy
-
si
ze
:
92
1
by
te
s.

URL	https://vertechie.com/favicon.svg
Node Name	https://vertechie.com/favicon.svg
Method	GET
Parameter	
Attack	
Evidence	
Show/hide Request and Response	
Request Header-size: 272	

bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/robots.txt

Node https://vertechie.com/robots.txt

Name

Method GET

Parameter

Attack

Evidence

Show/hide Request and Response

Request Header-size: 238 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/sitemap.xml

Node Name https://vertechie.com/sitemap.xml

Method GET

Parameter

Attack

Evidence

Show/hide Request and Response

Request Header-size: 239 bytes.

Request

Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
Tags	OWASP_2021_A05 OWASP_2017_A06

	POLICY_QA_STD = POLICY_PENTEST = SYSTEMIC CWE-319
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://vertechie.com/assets/index-CI9erZ_f.js
Node Name	https://vertechie.com/assets/index-CI9erZ_f.js
Method	GET
Parameter	
Attack	
Evidence	1540483477
Show/hideReques	

t
an
d
Re
sp
on
se

Re
qu
es
t
He
ad
er
-
si
ze
:
29
6
by
te
s.

Re
qu
es
t
Bo
dy
-
si
ze
:
0
by
te
s.

Re
sp
on
se
He
ad
er
-
si
ze
:
26
5
by
te
s.

Response Body - size: 846,526 bytes.	
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
Tags	OWASP_2021_A01 OWASP_2017_A03 POLICY_PENTEST = CWE-497 SYSTEMIC
CWE Id	497
WASP Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://vertechie.com/
Node	https://vertechie.com/

Name	
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Show/hide Request and Response	
Request Header-size: 228 bytes.	

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/assets/index-DXqeRgIr.css

Node Name https://vertechie.com/assets/index-DXqeRgIr.css

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Show/hide Request and Response	
Request Header-size: 286 bytes.	
Request	

Body-size: 0 bytes.

ResponseHeader-size: 246 bytes.

ResponseBody-size: 921 bytes.

URL https://vertechie.com/favicon.svg

NodeName https://vertechie.com/favicon.svg

Method GET

Para x-content-type-options

meter

Attack

Evidence

Show/hide Request and Response

Request Header-size: 272 bytes.

Request Body-size: 0

bytes.

ResponseHeader-size: 247 bytes.

ResponseBody-size: 929 bytes.

URL https://vertechie.com/robots.txt

NodeName https://vertechie.com/robots.txt

Method GET

Parameter x-content-type-options

Atta

ck

Ev
id
en
ce

Sh
ow
/
hi
de
Re
qu
es
t
an
d
Re
sp
on
se

Re
qu
es
t
He
ad
er
-
si
ze
:
23
8
by
te
s.

Re
qu
es
t
Bo
dy
-
si
ze
:
0
by
te
s.

Re
sp

onseHeader-size:	247 bytes.
ResponseBody-size:	929 bytes.
URL	https://vertechie.com/sitemap.xml
NodeName	https://vertechie.com/sitemap.xml
Method	GET
Parameter	x-content-type-options
Attack	

Evidence

Show/hide Request and Response

Request Header-size: 239 bytes.

Request Body-size: 0 bytes.

Response

Header-size: 247 bytes.

ResponseBody-size: 929 bytes.

Instances	Systemic
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
Tags	CWE-693 OWASP_2021_A05 OWASP_2017_A06 POLICY_QA_STD = POLICY_PENTEST = SYSTEMIC
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://vertechie.com/assets/index-CI9erZ_f.js
Node Name	https://vertechie.com/assets/index-CI9erZ_f.js
Method	GET
Parameter	
Attack	
Evidence	select
Show/hide Request and Response	
Request	

Header-size: 296 bytes.

Request Body-size: 0 bytes.

Response Header-size: 265 bytes.

Response Body-size: 846,526

bytes.	
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
Tags	OWASP_2021_A01 WSTG-v42-INFO-05 OWASP_2017_A03 POLICY_PENTEST = CWE-615
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://vertechie.com/
Node Name	https://vertechie.com/
Method	GET
Parameter	

Attack

Evidence

```
<script type="module" crossorigin src="/assets/index-CI9erZ_f.js">
</script>
```

Show/hide Request and Response

Request Header-size: 228 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/contact

Node Name https://vertechie.com/contact

Method GET

Parameter

Attack

Evidence

```
<script type="module" crossorigin src="/assets/index-CI9erZ_f.js">
</script>
```

Show/hide Request and Response

Request Header-size: 292 bytes.

Request Body-size: 0 bytes.

Response

Header-size: 247 bytes.	
ResponseBody-size: 929 bytes.	
URL	https://vertechie.com/favicon.svg
NodeName	https://vertechie.com/favicon.svg
Method	GET
Parameter	
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-CI9erZ_f.js"></script>

Show/hide Request and Response

Request Header-size: 272 bytes.

Request Body-size: 0 bytes.

Response Header-size

: 247 bytes.	
Response Body-size: 929 bytes.	
URL	https://vertechie.com/robots.txt
Node Name	https://vertechie.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-CI9erZ_f.js"></script>
Show/hideRe	

quest and Response

Request Header-size: 238 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.	
URL	https://vertechie.com/sitemap.xml
Node Name	https://vertechie.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-CI9erZ_f.js"></script>
Show/hide Request and Resp	

onse

Request Header-size: 239 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body

- size: 929 bytes.	
Instances	5
Solution	This is an informational alert and so no changes are required.
Reference	
Tags	POLICY_QA_STD = POLICY_PENTEST = SYSTEMIC POLICY_DEV_STD =
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://vertechie.com/
Node Name	https://vertechie.com/
Method	GET
Parame	cache-control

ter

Attack

Evidence

Show/hide Request and Response

Request Header-size: 228 bytes.

Request Body-size: 0 by

	tes.
	Response Header-size: 247 bytes.
	Response Body-size: 929 bytes.
URL	https://vertechie.com/contact
Node Name	https://vertechie.com/contact
Method	GET
Parameter	cache-control

Attack

Evidence

Show/hide Request and Response

Request Header-size: 292 bytes.

Request Body-size: 0 bytes.

Response Header-size: 247 bytes.

Response Body-size: 929 bytes.

URL https://vertechie.com/robots.txt

Node Name https://vertechie.com/robots.txt

Method GET

Parameter cache-control

Attack

Evidence

Show/hide Request and Response

Request Header-size: 238 bytes.

Request Body-size: 0 bytes.

Response

Header-size: 247 bytes.	
ResponseBody-size: 929 bytes.	
URL	https://vertechie.com/sitemap.xml
NodeName	https://vertechie.com/sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	

Show/hide Request and Response

Request Header-size: 239 bytes.

Request Body-size: 0 bytes.

Response Header-size

	: 247 bytes. Response Body-size: 929 bytes.
Instances	4
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
Tags	WSTG-v42-ATHN-06 CWE-525 POLICY_PENTEST = SYSTEMIC
CWE Id	525
WASC Id	13
Plugin Id	10015

Report by ZAP