ZAP by Checkmarx Scanning Report

Sites: https://telem-edge.smartscreen.microsoft.com https://data-edge.smartscreen.microsoft.com https://nav-edge.smartscreen.microsoft.com https://firefox-settings-attachments.cdn.mozilla.net https://readymadeui.com https://fonts.gstatic.com https://fonts.googleapis.com https://amarsolution.xyz

Generated on Mon, 2 Feb 2026 16:18:56

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	5
Informational	5

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP errors logged - see the zap.log file for details	2
Low	Warning		ZAP warnings logged - see the zap.log file for details	11
Info	Informational	http://amarsolution.xyz	Percentage of responses with status code 3xx	100 %
Info	Informational	http://amarsolution.xyz	Percentage of slow responses	11 %
Info	Informational	https://amarsolution.xyz	Percentage of responses with status code 2xx	57 %

Info	Informational	https://amarsolution.xyz	Percentage of responses with status code 3xx	10 %
Info	Exceeded Low	https://amarsolution.xyz	Percentage of responses with status code 4xx	31 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type application/javascript	22 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type application/json	11 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type image/svg+xml	11 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type text/css	11 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type text/html	44 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with method GET	100 %
Info	Informational	https://amarsolution.xyz	Count of total endpoints	9
Info	Exceeded Low	https://amarsolution.xyz	Percentage of slow responses	27 %
Info	Informational		Percentage of responses	100 %

		https://analytics.google.com	with status code 2xx	
Info	Informational	https://analytics.google.com	Percentage of slow responses	100 %
Info	Informational	https://api.rudderstack.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://api.rudderstack.com	Percentage of slow responses	8 %
Info	Informational	https://cdn.rudderlabs.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://cdn.rudderlabs.com	Percentage of slow responses	24 %
Info	Informational	https://cdn.usefathom.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://cdn.usefathom.com	Percentage of slow responses	68 %
Info	Informational	https://challenges.cloudflare.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://challenges.cloudflare.com	Percentage of slow responses	20 %
Info	Informational	https://data-edge.smartscreen.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://data-edge.smartscreen.microsoft.com	Percentage of endpoints with content type application/octet-stream	100 %
Info	Informational	https://data-edge.smartscreen.microsoft.com	Percentage of endpoints with method POST	100 %
Info	Informational	https://data-edge.smartscreen.microsoft.com	Count of total endpoints	2

Info	Informational	https://data-edge.smartscreen.microsoft.com	Percentage of slow responses	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of endpoints with content type text/plain	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of endpoints with method GET	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Count of total endpoints	2
Info	Informational	https://fonts.bunny.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://fonts.bunny.net	Percentage of slow responses	12 %
Info	Informational	https://fonts.googleapis.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://fonts.googleapis.com	Percentage of endpoints with content type text/css	100 %
Info	Informational	https://fonts.googleapis.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://fonts.googleapis.com	Count of total endpoints	1
Info	Informational	https://fonts.googleapis.com	Percentage of slow responses	100 %
Info	Informational		Percentage of	100 %

		https://fonts.gstatic.com	responses with status code 2xx	
Info	Informational	https://fonts.gstatic.com	Percentage of endpoints with content type font /woff2	100 %
Info	Informational	https://fonts.gstatic.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://fonts.gstatic.com	Count of total endpoints	1
Info	Informational	https://fonts.gstatic.com	Percentage of slow responses	6 %
Info	Informational	https://laracasts.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://laracasts.com	Percentage of slow responses	25 %
Info	Informational	https://laravel-news.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://laravel-news.com	Percentage of slow responses	48 %
Info	Informational	https://laravel.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://laravel.com	Percentage of slow responses	27 %
Info	Informational	https://laravelnews.s3.amazonaws.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://laravelnews.s3.amazonaws.com	Percentage of slow responses	100 %
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of responses with status code 2xx	100 %

Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of endpoints with method POST	100 %
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Count of total endpoints	1
Info	Informational	https://nav-edge.smartscreen.microsoft.com	Percentage of slow responses	66 %
Info	Informational	https://p.typekit.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://p.typekit.net	Percentage of slow responses	33 %
Info	Informational	https://picperf.io	Percentage of responses with status code 2xx	100 %
Info	Informational	https://picperf.io	Percentage of slow responses	20 %
Info	Informational	https://readymadeui.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://readymadeui.com	Percentage of endpoints with content type image/webp	100 %
Info	Informational	https://readymadeui.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://readymadeui.com	Count of total endpoints	1
Info	Informational	https://readymadeui.com	Percentage of slow responses	97 %

Info	Informational	https://stats.g.doubleclick.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://stats.g.doubleclick.net	Percentage of slow responses	100 %
Info	Informational	https://tag.clearbitscripts.com	Percentage of responses with status code 4xx	100 %
Info	Informational	https://tag.clearbitscripts.com	Percentage of slow responses	100 %
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Percentage of endpoints with method POST	100 %
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Count of total endpoints	1
Info	Informational	https://telem-edge.smartscreen.microsoft.com	Percentage of slow responses	50 %
Info	Informational	https://use.typekit.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://use.typekit.net	Percentage of slow responses	25 %
Info	Informational	https://www.google.com.bd	Percentage of responses with status code 2xx	100 %
Info	Informational	https://www.google.com.bd	Percentage of slow responses	50 %
Info	Informational	https://www.googletagmanager.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://www.googletagmanager.com	Percentage of slow responses	100 %

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Cross-Domain Misconfiguration	Medium	3
Private IP Disclosure	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	Systemic
Strict-Transport-Security Header Not Set	Low	Systemic
Timestamp Disclosure - Unix	Low	Systemic
X-Content-Type-Options Header Missing	Low	Systemic
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	3
Re-examine Cache-control Directives	Informational	5
Retrieved from Cache	Informational	3
User Agent Fuzzer	Informational	Systemic

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://amarsolution.xyz/
Node Name	https://amarsolution.xyz/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://amarsolution.xyz/robots.txt
Node Name	https://amarsolution.xyz/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://amarsolution.xyz/sitemap.xml
Node Name	https://amarsolution.xyz/sitemap.xml
Method	GET

Attack	
Evidence	
Other Info	
Instances	3
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/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://amarsolution.xyz/backend/main/api/user
Node Name	https://amarsolution.xyz/backend/main/api/user
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.googleapis.com/css2?family=Inter:wght@100..900&display=swap
Node Name	https://fonts.googleapis.com/css2 (display,family)
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Node Name	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Method	GET
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	3
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
CWE Id	[264]()
WASC Id	14
Plugin Id	[10098]()

Low	Private IP Disclosure
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	192.168.68.130:7600
Other Info	192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600 192.168.68.130:7600
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://datatracker.ietf.org/doc/html/rfc1918
CWE Id	[497]()
WASC Id	13
Plugin Id	[2]()

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://amarsolution.xyz/
Node Name	https://amarsolution.xyz/
Method	GET

Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
URL	https://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
URL	https://amarsolution.xyz/assets/index-f776b6eb.css
Node Name	https://amarsolution.xyz/assets/index-f776b6eb.css
Method	GET
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
URL	https://amarsolution.xyz/assets/login-beeda917.js
Node Name	https://amarsolution.xyz/assets/login-beeda917.js
Method	GET
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
URL	https://amarsolution.xyz/backend/main/api/user
Node Name	https://amarsolution.xyz/backend/main/api/user
Method	GET
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
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/
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://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://amarsolution.xyz/assets/index-f776b6eb.css
Node Name	https://amarsolution.xyz/assets/index-f776b6eb.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://amarsolution.xyz/assets/login-beeda917.js
Node Name	https://amarsolution.xyz/assets/login-beeda917.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Method	GET
Attack	
Evidence	
Other Info	
	https://fonts.gstatic.com/s/inter/v20

URL	/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Node Name	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3
Node Name	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3 ()({identity:{user:{locale},device:{id,customId,onlineIdTicket,family,locale,osVersion,browser:{internetExplorer},netJoinStatus,enterprise:{},cloudSku,architecture},caller:{locale,name,version},client:{version,data:{topTraffic,customSynchronousLookupUris,edgeSettings,customSettings}}},correlationId,debugInfo:{clientId}})
Method	POST
Attack	
Evidence	
Other Info	
URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3
Node Name	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3 ()({identity:{user:{locale},device:{id,customId,onlineIdTicket,family,locale,osVersion,browser:{internetExplorer},netJoinStatus,enterprise:{},cloudSku,architecture},caller:{locale,name,version},client:{version,data:{topTraffic,customSynchronousLookupUris,edgeSettings,customSettings}}},correlationId,debugInfo:{clientId}})
Method	POST
Attack	
Evidence	
Other Info	
URL	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
Node Name	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3 ()({userAgent,redirectChain:{source,chain:[]},identity:{user:{locale},device:{id,customId,onlineIdTicket,family,locale,osVersion,browser:{internetExplorer},netJoinStatus,enterprise:{},cloudSku,architecture},caller:{locale,name,version},client:{version,data:{topTraffic,customSynchronousLookupUris,edgeSettings,customSettings}}},config:{user:{uriReputation:{enforcedByPolicy,level}},device:{appControl:{level},appReputation:{enforcedByPolicy,level}}},destination:{uri,ip},type,forceServiceDetermination,correlatio...)
Method	POST
Attack	
Evidence	
Other Info	
URL	https://telem-edge.smartscreen.microsoft.com/api/browser/edge/telemetry/3
Node Name	https://telem-edge.smartscreen.microsoft.com/api/browser/edge/telemetry/3 ()({executionTime,random,samplingRates:{evaluateModel,serverCall},config:{user:{uriReputation:{enforcedByPolicy,level}},device:{appControl:{level},appReputation:{enforcedByPolicy,level}}},correlationId,identity:{user:{locale},device:{id,customId,onlineIdTicket,family,locale,osVersion,browser:{internetExplorer},netJoinStatus,enterprise:{},cloudSku,architecture},caller:{locale,name,version},client:{version,data:{topTraffic,customSynchronousLookupUris,edgeSettings,customSettings}}},userAgent,events:[{$type,nam...)

Method	POST
Attack	
Evidence	
Other Info	
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
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://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	1604231423
Other Info	1604231423, which evaluates to: 2020-11-01 17:50:23.
URL	https://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	1687547391
Other Info	1687547391, which evaluates to: 2023-06-24 01:09:51.
URL	https://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	1724754687
Other Info	1724754687, which evaluates to: 2024-08-27 16:31:27.
URL	https://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js

Method	GET
Attack	
Evidence	1768516095
Other Info	1768516095, which evaluates to: 2026-01-16 04:28:15.
URL	https://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	2005441023
Other Info	2005441023, which evaluates to: 2033-07-20 08:57:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Method	GET
Attack	
Evidence	1768266603
Other Info	1768266603, which evaluates to: 2026-01-13 07:10:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Method	GET
Attack	
Evidence	1765588203
Other Info	1765588203, which evaluates to: 2025-12-13 07:10:03.
Instances	Systemic
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
CWE Id	497
WASC 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://amarsolution.xyz/assets/index-e46c8535.js
Node	

Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://amarsolution.xyz/assets/index-f776b6eb.css
Node Name	https://amarsolution.xyz/assets/index-f776b6eb.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://amarsolution.xyz/assets/login-beeda917.js
Node Name	https://amarsolution.xyz/assets/login-beeda917.js
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3
Node Name	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/settings/3 ()({identity:{user:{locale},device:{id,customId,onlineIdTicket,family,locale,osVersion,browser:{internetExplorer},netJoinStatus,enterprise:{},cloudSku,architecture},caller:{locale,name,version},client:{version,data:{topTraffic,customSynchronousLookupUris,edgeSettings,customSettings}}},correlationId,debugInfo:{clientId}})
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3
Node Name	https://data-edge.smartscreen.microsoft.com/api/browser/edge/data/toptraffic/3 ()({identity:{user:{locale},device:{id,customId,onlineIdTicket,family,locale,osVersion,browser:{internetExplorer},netJoinStatus,enterprise:{},cloudSku,architecture},caller:{locale,name,version},client:{version,data:{topTraffic,customSynchronousLookupUris,edgeSettings,customSettings}}},correlationId,debugInfo:{clientId}})
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3
Node Name	https://nav-edge.smartscreen.microsoft.com/api/browser/edge/navigate/3 ()({userAgent,redirectChain:{source,chain:[]},identity:{user:{locale},device:{id,customId,onlineIdTicket,family,locale,osVersion,browser:{internetExplorer},netJoinStatus,enterprise:{},cloudSku,architecture},caller:{locale,name,version},client:{version,data:{topTraffic,customSynchronousLookupUris,edgeSettings,customSettings}}},config:{user:{uriReputation:{enforcedByPolicy,level}},device:{appControl:{level},appReputation:{enforcedByPolicy,level}}},destination:{uri,ip},type,forceServiceDetermination,correlatio...)
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
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
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://amarsolution.xyz/assets/index-e46c8535.js
Node Name	https://amarsolution.xyz/assets/index-e46c8535.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//redux.js.org/Errors?code=${e} for the full message or use the non-minified dev environment for full errors. `}var Cje=(()=>typ", see evidence field for the suspicious comment/snippet.
URL	https://amarsolution.xyz/assets/login-beeda917.js
Node Name	https://amarsolution.xyz/assets/login-beeda917.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.w3.org/2000/svg",fill:"#bbb",stroke:"#bbb",className:"w-[18px] h-[18px] absolute right-4 cursor-pointer",viewBox:"0 0 128 ", see evidence field for the suspicious comment/snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
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://amarsolution.xyz/
Node Name	https://amarsolution.xyz/
Method	GET
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-e46c8535.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://amarsolution.xyz/robots.txt
Node Name	https://amarsolution.xyz/robots.txt
Method	GET
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-e46c8535.js"></script>
Other	No links have been found while there are scripts, which is an indication that this is a modern

Info	web application.
URL	https://amarsolution.xyz/sitemap.xml
Node Name	https://amarsolution.xyz/sitemap.xml
Method	GET
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-e46c8535.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	3
Solution	This is an informational alert and so no changes are required.
Reference	
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://amarsolution.xyz/
Node Name	https://amarsolution.xyz/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://amarsolution.xyz/robots.txt
Node Name	https://amarsolution.xyz/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://amarsolution.xyz/sitemap.xml
Node Name	https://amarsolution.xyz/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48

Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
Instances	5
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/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/1d8c39b7-d6d6-4d19-adf9-31065d9e4f48
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ad5b0ea1-f347-497a-8ee6-bef5e0ff38b7
Method	GET

Attack	
Evidence	HIT
Other Info	
URL	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Node Name	https://fonts.gstatic.com/s/inter/v20/UcC73FwrK3iLTeHuS_nVMrMxCp50SjIa1ZL7W0I5nvwU.woff2
Method	GET
Attack	
Evidence	Age: 405932
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	3
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	525
WASC Id	
Plugin Id	10050

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://amarsolution.xyz/assets
Node Name	https://amarsolution.xyz/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://amarsolution.xyz/assets
Node Name	https://amarsolution.xyz/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
Other Info	
URL	https://amarsolution.xyz/assets
Node Name	https://amarsolution.xyz/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
Instances	Systemic
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104