ZAP by Checkmarx Scanning Report

Sites: https://data-edge.smartscreen.microsoft.com https://telem-edge.smartscreen.microsoft.com https://copilot.microsoft.com https://nav-edge.smartscreen.microsoft.com https://firefox-settings-attachments.cdn.mozilla.net https://firefox.settings.services.mozilla.com https://www.gstatic.com https://fonts.gstatic.com https://fonts.googleapis.com https://www.google.com https://cdn.jsdelivr.net https://softsadi.com https://amarsolution.xyz

Generated on Mon, 2 Feb 2026 16:05:43

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	9
Informational	7

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP errors logged - see the zap.log file for details	8
Low	Warning		ZAP warnings logged - see the zap.log file for details	25
Info	Informational	http://amarsolution.xyz	Percentage of responses with status code 3xx	100 %
Info	Informational	http://amarsolution.xyz	Percentage of slow responses	75 %
Info	Informational	http://softsadi.com	Percentage of responses	100 %

			with status code 3xx	
Info	Informational	https://amarsolution.xyz	Percentage of responses with status code 2xx	64 %
Info	Informational	https://amarsolution.xyz	Percentage of responses with status code 3xx	9 %
Info	Informational	https://amarsolution.xyz	Percentage of responses with status code 4xx	26 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type application /javascript	14 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type image /svg+xml	14 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type text /css	14 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with content type text /html	57 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with method GET	100 %
Info	Informational	https://amarsolution.xyz	Count of total endpoints	7
Info	Informational	https://amarsolution.xyz	Percentage of slow responses	16 %
Info	Informational		Percentage of	100 %

		https://cdn.jsdelivr.net	responses with status code 2xx	
Info	Informational	https://cdn.jsdelivr.net	Percentage of endpoints with content type application/javascript	100 %
Info	Informational	https://cdn.jsdelivr.net	Percentage of endpoints with method GET	100 %
Info	Informational	https://cdn.jsdelivr.net	Count of total endpoints	1
Info	Informational	https://cdn.jsdelivr.net	Percentage of slow responses	5 %
Info	Informational	https://copilot.microsoft.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://copilot.microsoft.com	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://copilot.microsoft.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://copilot.microsoft.com	Count of total endpoints	1
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 %
			Percentage of endpoints	

Info	Informational	https://data-edge.smartscreen.microsoft.com	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	3
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of endpoints with content type application /json	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Count of total endpoints	1
Info	Informational	https://fonts.googleapis.com	Percentage of responses with status code 2xx	100 %
			Percentage of endpoints	

Info	Informational	https://fonts.googleapis.com	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	https://fonts.gstatic.com	Percentage of responses with status code 2xx	100 %
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	2
Info	Informational	https://fonts.gstatic.com	Percentage of slow responses	14 %
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://readymadeui.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://readymadeui.com	Percentage of slow responses	93 %
Info	Informational	https://softsadi.com	Percentage of responses with status code 2xx	40 %
Info	Informational	https://softsadi.com	Percentage of responses with status code 3xx	24 %
Info	Exceeded Low	https://softsadi.com	Percentage of responses with status code 4xx	34 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type application/javascript	26 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type application/octet-stream	2 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type image/jpeg	7 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type image/png	7 %
			Percentage of	

Info	Informational	https://softsadi.com	endpoints with content type image /webp	2 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type text /css	31 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type text /html	17 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type text /plain	2 %
Info	Informational	https://softsadi.com	Percentage of endpoints with content type text /xml	2 %
Info	Informational	https://softsadi.com	Percentage of endpoints with method GET	95 %
Info	Informational	https://softsadi.com	Percentage of endpoints with method POST	4 %
Info	Informational	https://softsadi.com	Count of total endpoints	41
Info	Informational	https://softsadi.com	Percentage of slow responses	2 %
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	33 %
Info	Informational	https://www.google.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://www.google.com	Percentage of endpoints with content type text /javascript	100 %
Info	Informational	https://www.google.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://www.google.com	Count of total endpoints	1
Info	Informational	https://www.google.com	Percentage of slow responses	100 %
Info	Informational	https://www.gstatic.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://www.gstatic.com	Percentage of endpoints with content type text /javascript	100 %
Info	Informational	https://www.gstatic.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://www.gstatic.com	Count of total endpoints	1
Info	Informational	https://www.gstatic.com	Percentage of slow responses	15 %

Alerts

Name	Risk Level	Number of Instances

Content Security Policy (CSP) Header Not Set	Medium	6
Cross-Domain Misconfiguration	Medium	6
Sub Resource Integrity Attribute Missing	Medium	Systemic
Vulnerable JS Library	Medium	2
Big Redirect Detected (Potential Sensitive Information Leak)	Low	4
Cookie No HttpOnly Flag	Low	Systemic
Cookie with SameSite Attribute None	Low	Systemic
Cross-Domain JavaScript Source File Inclusion	Low	4
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	10
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	5
Modern Web Application	Informational	3
Re-examine Cache-control Directives	Informational	Systemic
Retrieved from Cache	Informational	Systemic
Session Management Response Identified	Informational	11
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	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://softsadi.com/password/reset
Node Name	https://softsadi.com/password/reset
Method	GET
Attack	
Evidence	
Other Info	
URL	https://softsadi.com/tags
Node Name	https://softsadi.com/tags
Method	GET
Attack	
Evidence	
Other Info	
Instances	6
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://cdn.jsdelivr.net/npm/canvas-confetti@1.5.1/dist/confetti.browser.min.js
Node Name	https://cdn.jsdelivr.net/npm/canvas-confetti@1.5.1/dist/confetti.browser.min.js
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://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Node Name	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset (_expected)
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=DM+Sans:wght@400;500;700&family=Manrope:wght@300;400;500;600;700&display=swap
Node Name	https://fonts.googleapis.com/css2 (display,family,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/dmsans/v17/rP2Yp2ywxg089UriI5-g4vlH9VoD8Cmcqbu0-K6z8GXhnU0.woff2
Node Name	https://fonts.gstatic.com/s/dmsans/v17/rP2Yp2ywxg089UriI5-g4vlH9VoD8Cmcqbu0-K6z8GXhnU0.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.
URL	https://fonts.gstatic.com/s/manrope/v20/xn7gYHE41ni1AdIRggexSg.woff2
Node Name	https://fonts.gstatic.com/s/manrope/v20/xn7gYHE41ni1AdIRggexSg.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.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
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	6
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

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://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/canvas-confetti@1.5.1/dist/confetti.browser.min.js"></script>
Other	The following hash was calculated (using base64 encoding of the output of the hash

Info	algorithm: SHA-384) for the script in question sha384-0DP0MDbig+ZDZ9nB+hxK0onRr5KVsL0nGdTEFh1XVBS7HRf4AHMW2i+bOKH+8qkK
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	The following hash was calculated (using base64 encoding of the output of the hash algorithm: SHA-384) for the script in question sha384-BIHhXUU45B8iCYiXnanE62QGsfvyf9auiUsA2kbhGnnf0jIDwfYJA5NC9VYyXWXH
Instances	Systemic
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

Medium	**Vulnerable JS Library**
Description	The identified library appears to be vulnerable.
URL	https://softsadi.com/loginasset/assets/js/bootstrap.min.js
Node Name	https://softsadi.com/loginasset/assets/js/bootstrap.min.js
Method	GET
Attack	
Evidence	* Bootstrap v4.0.0
Other Info	The identified library bootstrap, version 4.0.0 is vulnerable. CVE-2018-14041 CVE-2019-8331 CVE-2018-14040 CVE-2018-14042 https://github.com/twbs/bootstrap/issues/28236 https://github.com/advisories/GHSA-pj7m-g53m-7638 https://github.com/twbs/bootstrap/issues/20184 https://github.com/advisories/GHSA-9v3m-8fp8-mj99
URL	https://softsadi.com/loginasset/assets/js/jquery-2.2.0.min.js

Node Name	https://softsadi.com/loginasset/assets/js/jquery-2.2.0.min.js
Method	GET
Attack	
Evidence	jquery-2.2.0.min.js
Other Info	The identified library jquery, version 2.2.0 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Instances	2
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	1395
WASC Id	
Plugin Id	10003

Low	**Big Redirect Detected (Potential Sensitive Information Leak)**
Description	The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	https://softsadi.com/
Node Name	https://softsadi.com/
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 25 [https://softsadi.com/home]. Predicted response size: 325. Response Body Length: 346.
URL	https://softsadi.com/home
Node Name	https://softsadi.com/home
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 26 [https://softsadi.com/login]. Predicted response size: 326. Response Body Length: 350.
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login ()(_token,email,password)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 26 [https://softsadi.com/login]. Predicted response size: 326. Response Body Length: 350.

URL	https://softsadi.com/reset-password
Node Name	https://softsadi.com/reset-password ()(_token,phone)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 35 [https://softsadi.com/password/reset]. Predicted response size: 335. Response Body Length: 386.
Instances	4
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	201
WASC Id	13
Plugin Id	10044

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://softsadi.com/
Node Name	https://softsadi.com/
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://softsadi.com/home
Node Name	https://softsadi.com/home
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	Systemic
Solution	Ensure that the HttpOnly flag is set for all cookies.

Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie with SameSite Attribute None**
Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://copilot.microsoft.com/c/api/user/eligibility
Node Name	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	Set-Cookie: __cf_bm
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	Set-Cookie: amarsolution_session
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	Systemic
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET

Attack	
Evidence	<script src="https://cdn.jsdelivr.net/npm/canvas-confetti@1.5.1/dist/confetti.browser.min.js"></script>
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	
Instances	4
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

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
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-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/robots.txt
Node Name	https://amarsolution.xyz/robots.txt
Method	GET
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
URL	https://amarsolution.xyz/sitemap.xml
Node Name	https://amarsolution.xyz/sitemap.xml
Method	GET
Attack	
Evidence	nginx/1.24.0 (Ubuntu)

Other Info	
URL	https://amarsolution.xyz/vite.svg
Node Name	https://amarsolution.xyz/vite.svg
Method	GET
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
URL	https://softsadi.com/v2-asset/css/bootstrap.min.css
Node Name	https://softsadi.com/v2-asset/css/bootstrap.min.css
Method	GET
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
URL	https://softsadi.com/v2-asset/css/fontawesome/css/fontawesome.min.css
Node Name	https://softsadi.com/v2-asset/css/fontawesome/css/fontawesome.min.css
Method	GET
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
URL	https://softsadi.com/v2-asset/css/magnific-popup.css
Node Name	https://softsadi.com/v2-asset/css/magnific-popup.css
Method	GET
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
URL	https://softsadi.com/v2-asset/css/responsive.css
Node Name	https://softsadi.com/v2-asset/css/responsive.css
Method	GET
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
URL	https://softsadi.com/v2-asset/css/style.css
Node Name	https://softsadi.com/v2-asset/css/style.css
Method	GET

Attack	
Evidence	nginx/1.18.0 (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/vite.svg
Node Name	https://amarsolution.xyz/vite.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://copilot.microsoft.com/c/api/user/eligibility
Node Name	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET

Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/896a8080-1cd7-439f-8e89-977d206ec79b
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/896a8080-1cd7-439f-8e89-977d206ec79b
Method	GET
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/dmsans/v17/rP2Yp2ywxg089UriI5-g4vlH9VoD8Cmcqbu0-K6z8GXhnU0.woff2
Node Name	https://fonts.gstatic.com/s/dmsans/v17/rP2Yp2ywxg089UriI5-g4vlH9VoD8Cmcqbu0-K6z8GXhnU0.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://fonts.gstatic.com/s/manrope/v20/xn7gYHE41ni1AdIRggexSg.woff2
Node Name	https://fonts.gstatic.com/s/manrope/v20/xn7gYHE41ni1AdIRggexSg.woff2
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://softsadi.com/v2-asset/css/bootstrap.min.css
Node Name	https://softsadi.com/v2-asset/css/bootstrap.min.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://softsadi.com/v2-asset/css/magnific-popup.css
Node Name	https://softsadi.com/v2-asset/css/magnific-popup.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://softsadi.com/v2-asset/css/owl-carousel/owl.carousel.min.css
Node Name	https://softsadi.com/v2-asset/css/owl-carousel/owl.carousel.min.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://softsadi.com/v2-asset/css/responsive.css
Node Name	https://softsadi.com/v2-asset/css/responsive.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://softsadi.com/v2-asset/css/style.css
Node Name	https://softsadi.com/v2-asset/css/style.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.google.com/recaptcha/api.js
Node Name	https://www.google.com/recaptcha/api.js
Method	GET

Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
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
	https://telem-edge.smartscreen.microsoft.com/api/browser/edge/telemetry/3 ()

Node Name	({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://copilot.microsoft.com/c/api/user/eligibility
Node Name	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	1770026439
Other Info	1770026439, which evaluates to: 2026-02-02 16:00:39.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
Method	GET
Attack	
Evidence	1765588203
Other Info	1765588203, which evaluates to: 2025-12-13 07:10:03.
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
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/896a8080-1cd7-439f-8e89-977d206ec79b
Node	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists

Name	/896a8080-1cd7-439f-8e89-977d206ec79b
Method	GET
Attack	
Evidence	1765588203
Other Info	1765588203, which evaluates to: 2025-12-13 07:10:03.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-26 04:36:33.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 11:37:29.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 07:23:13.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 10:16:33.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET

Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 14:17:21.
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/vite.svg
Node Name	https://amarsolution.xyz/vite.svg
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://copilot.microsoft.com/c/api/user/eligibility

Node Name	https://copilot.microsoft.com/c/api/user/eligibility
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/12943580-a81c-4c79-bdeb-686df660f244
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
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/4ad2159b-3349-40e5-83b5-902fb2959d1c
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
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/896a8080-1cd7-439f-8e89-977d206ec79b
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/896a8080-1cd7-439f-8e89-977d206ec79b
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	10
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	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login ()(_token,email,password)

Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://softsadi.com/login csrfToken=_token
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

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://softsadi.com/loginasset/assets/js/jquery-2.2.0.min.js
Node Name	https://softsadi.com/loginasset/assets/js/jquery-2.2.0.min.js
Method	GET
Attack	
Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected in likely comment: "//,rb={},sb={},tb="*/".concat("*"),ub=d.createElement("a");ub.href=ib.href;function vb(a){return function(b,c){"string"!=typeof ", see evidence field for the suspicious comment/snippet.
URL	https://softsadi.com/v2-asset/js/bootstrap.min.js
Node Name	https://softsadi.com/v2-asset/js/bootstrap.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//popper.js.org)");let e=this._element;"parent"===this._config.reference?e=t:c(this._config.reference)?e=h(this._config.referenc", see evidence field for the suspicious comment/snippet.
URL	https://softsadi.com/v2-asset/js/jquery.min.js
Node Name	https://softsadi.com/v2-asset/js/jquery.min.js
Method	GET
Attack	
Evidence	username

Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//, Rt={},Mt={},It="*/".concat("*"),Wt=E.createElement("a");function Ft(o){return function(e,t) {"string"!=typeof e&&(t=e,e="*");v", see evidence field for the suspicious comment/snippet.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "//google.com/recaptcha/admin/migrate" target="_blank">Take action. ')),F)>>2&29)>=7&&(F^73)<20&&Kf.call(this,BV,k),F)&&", see evidence field for the suspicious comment/snippet.
Instances	5
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 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/sitemap.xml
Node Name	https://amarsolution.xyz/sitemap.xml
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.
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://copilot.microsoft.com/c/api/user/eligibility
Node Name	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244

Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/896a8080-1cd7-439f-8e89-977d206ec79b
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/896a8080-1cd7-439f-8e89-977d206ec79b
Method	GET
Attack	
Evidence	public, max-age=3600
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Node Name	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset (_expected)
Method	GET
Attack	
Evidence	max-age=3600
Other Info	
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://softsadi.com/robots.txt
Node Name	https://softsadi.com/robots.txt
Method	GET
Attack	

Evidence	
Other Info	
URL	https://softsadi.com/sitemap.xml
Node Name	https://softsadi.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
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://cdn.jsdelivr.net/npm/canvas-confetti@1.5.1/dist/confetti.browser.min.js
Node Name	https://cdn.jsdelivr.net/npm/canvas-confetti@1.5.1/dist/confetti.browser.min.js
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/12943580-a81c-4c79-bdeb-686df660f244
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c

Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/4ad2159b-3349-40e5-83b5-902fb2959d1c
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/896a8080-1cd7-439f-8e89-977d206ec79b
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/896a8080-1cd7-439f-8e89-977d206ec79b
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset?_expected=1750871406038
Node Name	https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/mfcdm-origins-list/changeset (_expected)
Method	GET
Attack	
Evidence	HIT
Other Info	
URL	https://fonts.gstatic.com/s/dmsans/v17/rP2Yp2ywxg089UriI5-g4vlH9VoD8Cmcqbu0-K6z8GXhnU0.woff2
Node Name	https://fonts.gstatic.com/s/dmsans/v17/rP2Yp2ywxg089UriI5-g4vlH9VoD8Cmcqbu0-K6z8GXhnU0.woff2
Method	GET
Attack	
Evidence	Age: 283972
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://fonts.gstatic.com/s/manrope/v20/xn7gYHE41ni1AdIRggexSg.woff2
Node Name	https://fonts.gstatic.com/s/manrope/v20/xn7gYHE41ni1AdIRggexSg.woff2
Method	GET
Attack	
Evidence	Age: 293641
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET

Attack	
Evidence	Age: 534034
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 534091
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 534111
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 534123
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Node Name	https://www.gstatic.com/recaptcha/releases/N67nZn4AqZkNcbeMu4prBgzg/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 534137
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	Systemic
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	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://copilot.microsoft.com/c/api/user/eligibility
Node Name	https://copilot.microsoft.com/c/api/user/eligibility
Method	GET
Attack	
Evidence	__cf_bm
Other Info	cookie:__cf_bm
URL	https://softsadi.com/
Node Name	https://softsadi.com/
Method	GET
Attack	
Evidence	amarsolution_session
Other Info	cookie:amarsolution_session cookie:XSRF-TOKEN
URL	https://softsadi.com/home
Node Name	https://softsadi.com/home
Method	GET
Attack	
Evidence	amarsolution_session
Other Info	cookie:amarsolution_session cookie:XSRF-TOKEN
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login
Method	GET
Attack	
Evidence	amarsolution_session
Other Info	cookie:amarsolution_session cookie:XSRF-TOKEN

URL	https://softsadi.com/password/reset
Node Name	https://softsadi.com/password/reset
Method	GET
Attack	
Evidence	amarsolution_session
Other Info	cookie:amarsolution_session cookie:XSRF-TOKEN
URL	https://softsadi.com/login
Node Name	https://softsadi.com/login ()(_token,email,password)
Method	POST
Attack	
Evidence	amarsolution_session
Other Info	cookie:amarsolution_session cookie:XSRF-TOKEN
URL	https://softsadi.com/reset-password
Node Name	https://softsadi.com/reset-password ()(_token,phone)
Method	POST
Attack	
Evidence	amarsolution_session
Other Info	cookie:amarsolution_session cookie:XSRF-TOKEN
URL	https://softsadi.com/
Node Name	https://softsadi.com/
Method	GET
Attack	
Evidence	amarsolution_session
Other Info	cookie:amarsolution_session
URL	https://softsadi.com/
Node Name	https://softsadi.com/
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://softsadi.com/home
Node Name	https://softsadi.com/home
Method	GET
Attack	

Evidence	amarsolution_session
Other Info	cookie:amarsolution_session
URL	https://softsadi.com/home
Node Name	https://softsadi.com/home
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
Instances	11
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

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	

URL	https://amarsolution.xyz/assets
Node Name	https://amarsolution.xyz/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://amarsolution.xyz/assets
Node Name	https://amarsolution.xyz/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://softsadi.com/
Node Name	https://softsadi.com/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://softsadi.com/
Node Name	https://softsadi.com/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://softsadi.com/
Node Name	https://softsadi.com/
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