ZAP by Checkmarx Scanning Report

Sites: https://amarsolution.xyz https://software.akaarserver.xyz

Generated on Mon, 2 Feb 2026 17:51:49

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	3
Informational	3

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP errors logged - see the zap.log file for details	4
Info	Informational	http://amarsolution.xyz	Percentage of responses with status code 3xx	100 %
Info	Informational	http://amarsolution.xyz	Percentage of slow responses	100 %
Info	Informational	http://software.akaarserver.xyz	Percentage of responses with status code 3xx	100 %
Info	Informational	https://amarsolution.xyz	Percentage of responses with status code 2xx	14 %
Info	Informational	https://amarsolution.xyz	Percentage of responses with status code 4xx	85 %
			Percentage of	

Info	Informational	https://amarsolution.xyz	endpoints with content type application /json	100 %
Info	Informational	https://amarsolution.xyz	Percentage of endpoints with method POST	100 %
Info	Informational	https://amarsolution.xyz	Count of total endpoints	1
Info	Informational	https://amarsolution.xyz	Percentage of slow responses	87 %
Info	Informational	https://software.akaarserver.xyz	Percentage of responses with status code 2xx	20 %
Info	Informational	https://software.akaarserver.xyz	Percentage of responses with status code 4xx	79 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type application /json	20 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type application /xml	20 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type image /jpeg	20 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type text /html	20 %
Info	Informational		Percentage of endpoints with	20 %

		https://software.akaarserver.xyz	content type text /plain	
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with method GET	100 %
Info	Informational	https://software.akaarserver.xyz	Count of total endpoints	5
Info	Informational	https://software.akaarserver.xyz	Percentage of slow responses	2 %

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	1
Cross-Domain Misconfiguration	Medium	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1
Strict-Transport-Security Header Not Set	Low	3
X-Content-Type-Options Header Missing	Low	4
Authentication Request Identified	Informational	1
Re-examine Cache-control Directives	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://software.akaarserver.xyz/tags
Node Name	https://software.akaarserver.xyz/tags
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
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/login
Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
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	1
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	**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/backend/main/api/login
Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
Attack	
Evidence	nginx/1.24.0 (Ubuntu)
Other Info	
Instances	1

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://software.akaarserver.xyz/robots.txt
Node Name	https://software.akaarserver.xyz/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/sitemap.xml
Node Name	https://software.akaarserver.xyz/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/v2-asset/images/shapes/404.jpg
Node Name	https://software.akaarserver.xyz/v2-asset/images/shapes/404.jpg
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
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	**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://software.akaarserver.xyz/api/v5/products?category_id=17930
Node Name	https://software.akaarserver.xyz/api/v5/products (category_id)
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://software.akaarserver.xyz/robots.txt
Node Name	https://software.akaarserver.xyz/robots.txt
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://software.akaarserver.xyz/sitemap.xml
Node Name	https://software.akaarserver.xyz/sitemap.xml
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://software.akaarserver.xyz/v2-asset/images/shapes/404.jpg
Node Name	https://software.akaarserver.xyz/v2-asset/images/shapes/404.jpg
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.
Instances	4

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://amarsolution.xyz/backend/main/api/login
Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=admin@gmail.com passwordParam=password
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	**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://software.akaarserver.xyz/api/v5/products?category_id=17930
Node Name	https://software.akaarserver.xyz/api/v5/products (category_id)
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://software.akaarserver.xyz/robots.txt
Node Name	https://software.akaarserver.xyz/robots.txt
Method	GET

Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/sitemap.xml
Node Name	https://software.akaarserver.xyz/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
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	**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://software.akaarserver.xyz/api/v5/products?category_id=17930
Node Name	https://software.akaarserver.xyz/api/v5/products (category_id)
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/api/v5/products?category_id=17930
Node Name	https://software.akaarserver.xyz/api/v5/products (category_id)
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/api/v5/products?category_id=17930
Node Name	https://software.akaarserver.xyz/api/v5/products (category_id)
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/api/v5/products?category_id=17930
Node Name	https://software.akaarserver.xyz/api/v5/products (category_id)
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/api/v5/products?category_id=17930
Node Name	https://software.akaarserver.xyz/api/v5/products (category_id)
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://amarsolution.xyz/backend/main/api/login
Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://amarsolution.xyz/backend/main/api/login
Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://amarsolution.xyz/backend/main/api/login
Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://amarsolution.xyz/backend/main/api/login

Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://amarsolution.xyz/backend/main/api/login
Node Name	https://amarsolution.xyz/backend/main/api/login ()({email,password})
Method	POST
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	
Instances	Systemic
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104