ZAP by Checkmarx Scanning Report

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

Generated on Mon, 2 Feb 2026 11:25:08

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

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

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP warnings logged - see the zap.log file for details	2
Info	Informational	http://software.akaarserver.xyz	Percentage of responses with status code 2xx	50 %
Info	Informational	http://software.akaarserver.xyz	Percentage of responses with status code 3xx	42 %
Info	Informational	http://software.akaarserver.xyz	Percentage of responses with status code 4xx	7 %
Info	Informational	http://software.akaarserver.xyz	Percentage of endpoints with content type text/html	100 %
			Percentage of	

Info	Informational	http://software.akaarserver.xyz	endpoints with method GET	100 %
Info	Informational	http://software.akaarserver.xyz	Count of total endpoints	2
Info	Informational	https://cdn.jsdelivr.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://cdn.jsdelivr.net	Percentage of slow responses	50 %
Info	Informational	https://fonts.googleapis.com	Percentage of responses with status code 2xx	100 %
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 slow responses	50 %
Info	Informational	https://software.akaarserver.xyz	Percentage of responses with status code 2xx	93 %
Info	Informational	https://software.akaarserver.xyz	Percentage of responses with status code 3xx	5 %
Info	Informational	https://software.akaarserver.xyz	Percentage of responses with status code 4xx	1 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type application/xml	2 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type image/jpeg	2 %

Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type image /png	12 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type text /css	33 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type text /html	17 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type text /javascript	28 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with content type text /plain	2 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with method GET	94 %
Info	Informational	https://software.akaarserver.xyz	Percentage of endpoints with method POST	5 %
Info	Informational	https://software.akaarserver.xyz	Count of total endpoints	39
Info	Informational	https://software.akaarserver.xyz	Percentage of slow responses	2 %
Info	Informational	https://www.google.com	Percentage of responses with status code 2xx	100 %
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 slow responses	50 %

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	4
HTTP to HTTPS Insecure Transition in Form Post	Medium	1
Missing Anti-clickjacking Header	Medium	3
Sub Resource Integrity Attribute Missing	Medium	Systemic
Vulnerable JS Library	Medium	2
Big Redirect Detected (Potential Sensitive Information Leak)	Low	7
Cookie No HttpOnly Flag	Low	Systemic
Cross-Domain JavaScript Source File Inclusion	Low	8
Strict-Transport-Security Header Not Set	Low	Systemic
X-Content-Type-Options Header Missing	Low	Systemic
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	3
Re-examine Cache-control Directives	Informational	4
Session Management Response Identified	Informational	7
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	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/login

Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/password/reset
Node Name	https://software.akaarserver.xyz/password/reset
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/tags
Node Name	https://software.akaarserver.xyz/tags
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
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	**HTTP to HTTPS Insecure Transition in Form Post**
Description	This check looks for insecure HTTP pages that host HTTPS forms. The issue is that an insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	https://software.akaarserver.xyz/login
	The response to the following request over HTTP included an HTTPS form tag action

Other Info	attribute value: http://software.akaarserver.xyz The context was: <form class="login-form" action="https://software.akaarserver.xyz/login" method="POST"> <input type="hidden" name="_token" value="Y9r7i9YcfcKkF3gDRf1VzkwTKt8piBtg78M3qZjm"> <label for="user-id">Email or Username</label> <input name="email" value="" class="input-text " placeholder="Username or Email" required="required" autofocus id=" user-id"> <label for="password" >Password</label> <input type="password" name="password" class="input-text" placeholder="Password" required="required" autocomplete="current-password" id=" password"> <label for="remember"> <input class="form-check-input" type="checkbox" value=" 1" type="checkbox" id="remember">Remember Me </label> <button type="submit" class="ams-btn primary-btn my-3">Log in</button> </form>
Instances	1
Solution	Use HTTPS for landing pages that host secure forms.
Reference	
CWE Id	319
WASC Id	15
Plugin Id	10041

Medium	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/password/reset
Node Name	https://software.akaarserver.xyz/password/reset
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

Solution	If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Sub Resource Integrity Attribute Missing**
Description	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
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	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	
URL	https://software.akaarserver.xyz/login

Node Name	https://software.akaarserver.xyz/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://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	
URL	https://software.akaarserver.xyz/password/reset
Node Name	https://software.akaarserver.xyz/password/reset
Method	GET
Attack	
Evidence	<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Open+Sans:400,300,600,700,800%7CPoppins:400,500,700,800,900%7CRoboto:100,300,400,400i,500,700">
Other Info	
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://software.akaarserver.xyz/loginasset/assets/js/bootstrap.min.js
Node Name	https://software.akaarserver.xyz/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://software.akaarserver.xyz/loginasset/assets/js/jquery-2.2.0.min.js
Node Name	https://software.akaarserver.xyz/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	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 33 [https://software.akaarserver.xyz/]. Predicted response size: 333. Response Body Length: 818.
URL	http://software.akaarserver.xyz/robots.txt
Node	

Name	http://software.akaarserver.xyz/robots.txt
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 43 [https://software.akaarserver.xyz/robots.txt]. Predicted response size: 343. Response Body Length: 818.
URL	http://software.akaarserver.xyz/sitemap.xml
Node Name	http://software.akaarserver.xyz/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 44 [https://software.akaarserver.xyz/sitemap.xml]. Predicted response size: 344. Response Body Length: 818.
URL	https://software.akaarserver.xyz/
Node Name	https://software.akaarserver.xyz/
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 37 [https://software.akaarserver.xyz/home]. Predicted response size: 337. Response Body Length: 394.
URL	https://software.akaarserver.xyz/home
Node Name	https://software.akaarserver.xyz/home
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 38 [https://software.akaarserver.xyz/login]. Predicted response size: 338. Response Body Length: 398.
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login ()(_token,email,password)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 38 [https://software.akaarserver.xyz/login]. Predicted response size: 338. Response Body Length: 398.
URL	https://software.akaarserver.xyz/reset-password
Node Name	https://software.akaarserver.xyz/reset-password ()(_token,phone)
Method	POST
Attack	
Evidence	
Other	Location header URI length: 47 [https://software.akaarserver.xyz/password/reset]. Predicted

Info	response size: 347. Response Body Length: 434.
Instances	7
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	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://software.akaarserver.xyz/
Node Name	https://software.akaarserver.xyz/
Method	GET
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://software.akaarserver.xyz/home
Node Name	https://software.akaarserver.xyz/home
Method	GET
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://software.akaarserver.xyz/password/reset

Node Name	https://software.akaarserver.xyz/password/reset
Method	GET
Attack	
Evidence	set-cookie: XSRF-TOKEN
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login ()(_token,email,password)
Method	POST
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	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
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	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	

Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
URL	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/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://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	<script src="https://www.google.com/recaptcha/api.js" async defer></script>
Other Info	
Instances	8

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	**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/css/animate.min.css
Node Name	https://software.akaarserver.xyz/v2-asset/css/animate.min.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/v2-asset/css/magnific-popup.css
Node Name	https://software.akaarserver.xyz/v2-asset/css/magnific-popup.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://software.akaarserver.xyz/v2-asset/css/owl-carousel/owl.carousel.min.css
Node Name	https://software.akaarserver.xyz/v2-asset/css/owl-carousel/owl.carousel.min.css

Method	GET
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	**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	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
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/css/animate.min.css
Node Name	https://software.akaarserver.xyz/v2-asset/css/animate.min.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://software.akaarserver.xyz/v2-asset/css/magnific-popup.css
Node Name	https://software.akaarserver.xyz/v2-asset/css/magnific-popup.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://software.akaarserver.xyz/v2-asset/css/owl-carousel/owl.carousel.min.css
Node Name	https://software.akaarserver.xyz/v2-asset/css/owl-carousel/owl.carousel.min.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.
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	**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://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login ()(_token,email,password)
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://software.akaarserver.xyz/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://software.akaarserver.xyz/loginasset/assets/js/jquery-2.2.0.min.js
Node Name	https://software.akaarserver.xyz/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://software.akaarserver.xyz/v2-asset/js/bootstrap.min.js
Node Name	https://software.akaarserver.xyz/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://software.akaarserver.xyz/v2-asset/js/jquery.min.js
Node Name	https://software.akaarserver.xyz/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.

Instances	3
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	**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/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://software.akaarserver.xyz/password/reset
Node Name	https://software.akaarserver.xyz/password/reset
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	4

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

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	http://software.akaarserver.xyz
Node Name	http://software.akaarserver.xyz
Method	GET
Attack	
Evidence	amarsolution_akaarserver_session
Other Info	cookie:amarsolution_akaarserver_session cookie:XSRF-TOKEN
URL	https://software.akaarserver.xyz/
Node Name	https://software.akaarserver.xyz/
Method	GET
Attack	
Evidence	amarsolution_akaarserver_session
Other Info	cookie:amarsolution_akaarserver_session cookie:XSRF-TOKEN
URL	https://software.akaarserver.xyz/home
Node Name	https://software.akaarserver.xyz/home
Method	GET
Attack	
Evidence	amarsolution_akaarserver_session
Other Info	cookie:amarsolution_akaarserver_session cookie:XSRF-TOKEN
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login
Method	GET
Attack	
Evidence	amarsolution_akaarserver_session
Other Info	cookie:amarsolution_akaarserver_session cookie:XSRF-TOKEN

URL	https://software.akaarserver.xyz/password/reset
Node Name	https://software.akaarserver.xyz/password/reset
Method	GET
Attack	
Evidence	amarsolution_akaarserver_session
Other Info	cookie:amarsolution_akaarserver_session cookie:XSRF-TOKEN
URL	https://software.akaarserver.xyz/login
Node Name	https://software.akaarserver.xyz/login ()(_token,email,password)
Method	POST
Attack	
Evidence	amarsolution_akaarserver_session
Other Info	cookie:amarsolution_akaarserver_session cookie:XSRF-TOKEN
URL	https://software.akaarserver.xyz/reset-password
Node Name	https://software.akaarserver.xyz/reset-password ()(_token,phone)
Method	POST
Attack	
Evidence	amarsolution_akaarserver_session
Other Info	cookie:amarsolution_akaarserver_session cookie:XSRF-TOKEN
Instances	7
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	http://software.akaarserver.xyz/robots.txt
Node Name	http://software.akaarserver.xyz/robots.txt
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://software.akaarserver.xyz/robots.txt
Node Name	http://software.akaarserver.xyz/robots.txt

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://software.akaarserver.xyz/robots.txt
Node Name	http://software.akaarserver.xyz/robots.txt
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://software.akaarserver.xyz/sitemap.xml
Node Name	http://software.akaarserver.xyz/sitemap.xml
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://software.akaarserver.xyz/sitemap.xml
Node Name	http://software.akaarserver.xyz/sitemap.xml
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