



Site: <http://120.97.66.25>

Generated on , 20 10 2026 18:20:40

ZAP Version: 2.17.0

ZAP by [Checkmarx](#)

Summary of Alerts

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

Insights

Level	Reason	Site	Description	Statistic
Informational	Informational	http://120.97.66.25	Percentage of responses with status code 2xx	67 %
Informational	Informational	http://120.97.66.25	Percentage of responses with status code 3xx	10 %
Informational	Informational	http://120.97.66.25	Percentage of responses with status code 4xx	22 %
Informational	Informational	http://120.97.66.25	Percentage of endpoints with content type application/manifest+json	4 %
Informational	Informational	http://120.97.66.25	Percentage of endpoints with content type application/pdf	4 %
Informational	Informational	http://120.97.66.25	Percentage of endpoints with content type image/png	4 %
Informational	Informational	http://120.97.66.25	Percentage of endpoints with content type text/css	8 %

	Informational	http://120.97.66.25	Percentage of endpoints with content type text/html	26 %
	Informational	http://120.97.66.25	Percentage of endpoints with content type text/javascript	47 %
	Informational	http://120.97.66.25	Percentage of endpoints with content type text/plain	4 %
	Informational	http://120.97.66.25	Percentage of endpoints with method GET	91 %
	Informational	http://120.97.66.25	Percentage of endpoints with method POST	8 %
	Informational	http://120.97.66.25	Count of total endpoints	23
	Informational	http://120.97.66.25	Percentage of slow responses	30 %

	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	1
Sub Resource Integrity Attribute Missing	Medium	3
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3
Cookie No HttpOnly Flag	Low	Systemic
Modern Web Application	Informational	3
Session Management Response Identified	Informational	7
User Controllable HTML Element Attribute (Potential XSS)	Informational	1

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://120.97.66.25/sitemap.xml
Node Name	http://120.97.66.25/sitemap.xml

	GET
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	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://120.97.66.25/login
Node Name	http://120.97.66.25/login
	GET
Evidence	<link href="https://fonts.bunny.net/css?family=figtree:400,500,600&display=swap" rel="stylesheet" />
Other Info	
URL	http://120.97.66.25/mima/forget?source=forgot
Node Name	http://120.97.66.25/mima/forget (source)
	GET
Evidence	<link href="https://fonts.bunny.net/css?family=figtree:400,500,600&display=swap" rel="stylesheet" />
Other Info	
URL	http://120.97.66.25/sitemap.xml
Node Name	http://120.97.66.25/sitemap.xml
	GET
Evidence	<link href="https://fonts.bunny.net/css?family=figtree:400,500,600&display=swap" rel="stylesheet" />
Other	

Info	
Instances	3
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Defenses/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

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://120.97.66.25/
Node Name	http://120.97.66.25/
	GET
Evidence	
Other Info	Location header URI length: 25 [http://120.97.66.25/login]. Predicted response size: 325. Response Body Length: 346.
URL	http://120.97.66.25/login
Node Name	http://120.97.66.25/login ()(_token,captcha,captcha_key,mima,uid)
	POST
Evidence	
Other Info	Location header URI length: 25 [http://120.97.66.25/login]. Predicted response size: 325. Response Body Length: 346.
URL	http://120.97.66.25/mima/forget
Node Name	http://120.97.66.25/mima/forget ()(_token,captcha,captcha_key,email,source)
	POST
Evidence	
Other Info	Location header URI length: 45 [http://120.97.66.25/mima/forget?source=forgot]. Predicted response size: 345. Response Body Length: 426.
Instances	3
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://120.97.66.25/
Node Name	http://120.97.66.25/
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.97.66.25/login
Node Name	http://120.97.66.25/login
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.97.66.25/mima/forget?source=forgot
Node Name	http://120.97.66.25/mima/forget (source)
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.97.66.25/login
Node Name	http://120.97.66.25/login ()(_token,captcha,captcha_key,mima,uid)
	POST
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.97.66.25/mima/forget
Node Name	http://120.97.66.25/mima/forget ()(_token,captcha,captcha_key,email,source)
	POST
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

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	http://120.97.66.25/login
Node Name	http://120.97.66.25/login
	GET
Evidence	<code> <i class="fa-solid fa-arrow-up"></i> </code>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://120.97.66.25/mima/forget?source=forgot
Node Name	http://120.97.66.25/mima/forget (source)
	GET
Evidence	<code> <i class="fa-solid fa-arrow-up"></i> </code>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://120.97.66.25/sitemap.xml
Node Name	http://120.97.66.25/sitemap.xml
	GET
Evidence	<code> <i class="fa-solid fa-arrow-up"></i> </code>

Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	3
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	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://120.97.66.25/
Node Name	http://120.97.66.25/
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:smartexam-ai-session
URL	http://120.97.66.25/example
Node Name	http://120.97.66.25/example
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:smartexam-ai-session
URL	http://120.97.66.25/login
Node Name	http://120.97.66.25/login
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:smartexam-ai-session
URL	http://120.97.66.25/mima/forget?source=forgot
Node Name	http://120.97.66.25/mima/forget (source)
	GET
Evidence	XSRF-TOKEN

Other Info	cookie:XSRF-TOKEN cookie:smartexam-ai-session
URL	http://120.97.66.25/login
Node Name	http://120.97.66.25/login ()(_token,captcha,captcha_key,mima,uid)
	POST
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:smartexam-ai-session
URL	http://120.97.66.25/mima/forget
Node Name	http://120.97.66.25/mima/forget ()(_token,captcha,captcha_key,email,source)
	POST
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:smartexam-ai-session
URL	http://120.97.66.25/
Node Name	http://120.97.66.25/
	GET
Evidence	smartexam-ai-session
Other Info	cookie:smartexam-ai-session
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 Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://120.97.66.25/mima/forget?source=forgot
Node Name	http://120.97.66.25/mima/forget (source)
	GET
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://120.97.66.25/mima/forget?source=forgot appears to include user input in: a(n) [input] tag [value] attribute The user input found was: source=forgot The user-controlled value was: forgot
Instances	1
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031