ZAP by Checkmarx Scanning Report

Sites: https://192.192.51.193 http://192.192.51.193

Generated on , 25 5 2026 13:53:00

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	7
Informational	11

	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	Systemic
CSP: script-src unsafe-inline	Medium	Systemic
CSP: style-src unsafe-inline	Medium	Systemic
Application Error Disclosure	Low	1
Cookie No HttpOnly Flag	Low	Systemic
Cookie Without Secure Flag	Low	1
Cookie without SameSite Attribute	Low	Systemic
Information Disclosure - Debug Error Messages	Low	1
Private IP Disclosure	Low	2
Timestamp Disclosure - Unix	Low	3
Authentication Request Identified	Informational	7
Information Disclosure - Sensitive Information in URL	Informational	Systemic
Modern Web Application	Informational	Systemic
Re-examine Cache-control Directives	Informational	1
Session Management Response Identified	Informational	69
Tech Detected - Apache HTTP Server	Informational	2
Tech Detected - Bootstrap	Informational	2
Tech Detected - Font Awesome	Informational	2
Tech Detected - HSTS	Informational	2

Tech Detected - jQuery	Informational	2
User Controllable HTML Element Attribute (Potential XSS)	Informational	7

Alert Detail

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	http://192.192.51.193/
Node Name	http://192.192.51.193/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://192.192.51.193/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://192.192.51.193/sitemap.xml
Node Name	http://192.192.51.193/sitemap.xml
	GET

Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	http://192.192.51.193/sitemap.xml/
Node Name	http://192.192.51.193/sitemap.xml/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: script-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://192.192.51.193/
Node Name	http://192.192.51.193/

	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	script-src includes unsafe-inline.
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	script-src includes unsafe-inline.
URL	http://192.192.51.193/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	script-src includes unsafe-inline.
URL	http://192.192.51.193/sitemap.xml
Node Name	http://192.192.51.193/sitemap.xml
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	script-src includes unsafe-inline.
URL	http://192.192.51.193/sitemap.xml/
Node Name	http://192.192.51.193/sitemap.xml/
	GET

Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	script-src includes unsafe-inline.
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	script-src includes unsafe-inline.
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://192.192.51.193/
Node Name	http://192.192.51.193/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	style-src includes unsafe-inline.
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/

	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	style-src includes unsafe-inline.
URL	http://192.192.51.193/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	style-src includes unsafe-inline.
URL	http://192.192.51.193/sitemap.xml
Node Name	http://192.192.51.193/sitemap.xml
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	style-src includes unsafe-inline.
URL	http://192.192.51.193/sitemap.xml/
Node Name	http://192.192.51.193/sitemap.xml/
	GET
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	style-src includes unsafe-inline.
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
	default-src 'self'; script-src 'self' 'unsafe-inline' https://maps.googleapis.com https://maps.

Evidence	gstatic.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://maps.googleapis.com https://maps.gstatic.com https://*.googleapis.com https://*.gstatic.com https://*.google.com; font-src 'self' https://fonts.gstatic.com; connect-src 'self' https://maps.googleapis.com https://*.googleapis.com
Other Info	style-src includes unsafe-inline.
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Low	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://192.192.51.193/kurogo/error?code=internal&id=stats&page=index
Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	HTTP/1.0 500 Internal Server Error
Other Info	
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	550
WASC Id	13
Plugin Id	90022

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://192.192.51.193/admin/
Node Name	http://192.192.51.193/admin/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5

Other Info	
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	http://192.192.51.193/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	http://192.192.51.193/login/
Node Name	http://192.192.51.193/login/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	http://192.192.51.193/rest/
Node Name	http://192.192.51.193/rest/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
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 Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
Instances	1
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, 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	http://192.192.51.193/
Node Name	http://192.192.51.193/
	GET
Evidence	Set-Cookie: deviceClassification
Other Info	
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/

	GET
Evidence	Set-Cookie: visitID
Other Info	
URL	http://192.192.51.193/robots.txt
Node Name	http://192.192.51.193/robots.txt
	GET
Evidence	Set-Cookie: deviceClassification
Other Info	
URL	http://192.192.51.193/sitemap.xml
Node Name	http://192.192.51.193/sitemap.xml
	GET
Evidence	Set-Cookie: deviceClassification
Other Info	
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	Set-Cookie: visitID
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	**Information Disclosure - Debug Error Messages**

Description	The response appeared to contain common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages.
URL	http://192.192.51.193/kurogo/error?code=internal&id=stats&page=index
Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	Internal server error
Other Info	
Instances	1
Solution	Disable debugging messages before pushing to production.
Reference	
CWE Id	1295
WASC Id	13
Plugin Id	10023

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	http://192.192.51.193/device/compliant/min/?g=file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Node Name	http://192.192.51.193/device/compliant/min/ (g)
	GET
Evidence	10.1.9.34
Other Info	10.1.9.34 10.8.1.1 10.8.1.1
URL	http://192.192.51.193/min/?g=file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Node Name	http://192.192.51.193/min/ (g)
	GET
Evidence	10.1.9.34
Other Info	10.1.9.34 10.8.1.1 10.8.1.1
Instances	2
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	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	1779687459
Other Info	1779687459, which evaluates to: 2026-05-25 13:37:39.
URL	http://192.192.51.193/home/
Node Name	http://192.192.51.193/home/
	GET
Evidence	1779687459
Other Info	1779687459, which evaluates to: 2026-05-25 13:37:39.
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	1779687467
Other Info	1779687467, which evaluates to: 2026-05-25 13:37:47.
Instances	3
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

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	http://192.192.51.193/device/compliant/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5BstartOver%5D=1&code=server&id=login&page=login
Node Name	http://192.192.51.193/device/compliant/kurogo/error (args[agreeTerm],args[authority],args[loginPassword],args[loginUser],args[startOver],code,id,page)
	GET

Evidence	args[loginPassword]
Other Info	userParam=args[loginPassword] userValue=ZAP passwordParam=args[loginPassword] referer=http://192.192.51.193/device/compliant/login/login csrfToken=anticsrf
URL	http://192.192.51.193/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5Bid%5D=admin&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5Bpage%5D=index&args%5BstartOver%5D=1&code=server&id=login&page=login
Node Name	http://192.192.51.193/kurogo/error (args[agreeTerm],args[authority],args[id],args[loginPassword],args[loginUser],args[page],args[startOver],code,id,page)
	GET
Evidence	args[loginPassword]
Other Info	userParam=args[loginPassword] userValue=ZAP passwordParam=args[loginPassword] referer=http://192.192.51.193/login/login csrfToken=anticsrf
URL	http://192.192.51.193/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5BstartOver%5D=1&code=server&id=login&page=login
Node Name	http://192.192.51.193/kurogo/error (args[agreeTerm],args[authority],args[loginPassword],args[loginUser],args[startOver],code,id,page)
	GET
Evidence	args[loginPassword]
Other Info	userParam=args[loginPassword] userValue=ZAP passwordParam=args[loginPassword] referer=http://192.192.51.193/login/login csrfToken=anticsrf
URL	http://192.192.51.193/login/login?agreeTerm=1&authority=nou&loginPassword=ZAP&loginUser=ZAP&startOver=1
Node Name	http://192.192.51.193/login/login (agreeTerm,authority,loginPassword,loginUser,startOver)
	GET
Evidence	loginPassword
	userParam=loginPassword

Other Info	userValue=ZAP passwordParam=loginPassword referer=http://192.192.51.193/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5BstartOver%5D=1&code=server&id=login&page=login csrfToken=anticsrf
URL	http://192.192.51.193/device/compliant/login/login
Node Name	http://192.192.51.193/device/compliant/login/login ()(agreeTerm,anticsrf,authority,loginPassword,loginUser,startOver)
	POST
Evidence	loginPassword
Other Info	userParam=loginPassword userValue=ZAP passwordParam=loginPassword referer=http://192.192.51.193/device/compliant/login/login?authority=nou csrfToken=anticsrf
URL	http://192.192.51.193/login/login
Node Name	http://192.192.51.193/login/login ()(agreeTerm,anticsrf,authority,id,loginPassword,loginUser,page,startOver)
	POST
Evidence	loginPassword
Other Info	userParam=loginPassword userValue=ZAP passwordParam=loginPassword referer=http://192.192.51.193/login/login?authority=nou&id=admin&page=index csrfToken=anticsrf
URL	http://192.192.51.193/login/login
Node Name	http://192.192.51.193/login/login ()(agreeTerm,anticsrf,authority,loginPassword,loginUser,startOver)
	POST
Evidence	loginPassword
Other Info	userParam=loginPassword userValue=ZAP passwordParam=loginPassword referer=http://192.192.51.193/login/login?authority=nou csrfToken=anticsrf
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/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	**Information Disclosure - Sensitive Information in URL**
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	http://192.192.51.193/device/compliant/min/?g=file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Node Name	http://192.192.51.193/device/compliant/min/ (g)
	GET
Evidence	file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Other Info	The URL contains email address(es).
URL	http://192.192.51.193/device/compliant/min/?g=file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Node Name	http://192.192.51.193/device/compliant/min/ (g)
	GET
Evidence	file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Other Info	The URL contains email address(es).
URL	http://192.192.51.193/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5BstartOver%5D=1&code=server&id=login&page=login
Node Name	http://192.192.51.193/kurogo/error (args[agreeTerm],args[authority],args[loginPassword],args[loginUser],args[startOver],code,id,page)
	GET
Evidence	args[loginPassword]
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass args[loginPassword]
URL	http://192.192.51.193/min/?g=file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Node Name	http://192.192.51.193/min/ (g)
	GET
Evidence	file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Other Info	The URL contains email address(es).
URL	http://192.192.51.193/min/?g=file-/common/javascript/fontawesome-free@6.6.0.all.min.js

Node Name	http://192.192.51.193/min/ (g)
	GET
Evidence	file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Other Info	The URL contains email address(es).
URL	https://192.192.51.193/device/compliant/min/?g=file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Node Name	https://192.192.51.193/device/compliant/min/ (g)
	GET
Evidence	file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Other Info	The URL contains email address(es).
Instances	Systemic
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	598
WASC Id	13
Plugin Id	10024

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://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	<li class="d-flex align-items-start ms-2 me-auto my-3">
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://192.192.51.193/home/
Node Name	http://192.192.51.193/home/
	GET
Evidence	<li class="d-flex align-items-start ms-2 me-auto my-3">
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://192.192.51.193/kurogo/error?code=notfound&id=sitemap.xml&page=index

Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	<li class="d-flex align-items-start ms-2 me-auto my-3">
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://192.192.51.193/login/login?authority=nou
Node Name	http://192.192.51.193/login/login (authority)
	GET
Evidence	<li class="d-flex align-items-start ms-2 me-auto my-3">
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://192.192.51.193/people/
Node Name	http://192.192.51.193/people/
	GET
Evidence	<li class="d-flex align-items-start ms-2 me-auto my-3">
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	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	<li class="d-flex align-items-start ms-2 me-auto my-3">
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	Systemic
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**
	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,

Description	however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	max-age=0
Other Info	
Instances	1
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://192.192.51.193/
Node Name	http://192.192.51.193/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/about/about
Node Name	http://192.192.51.193/about/about
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/admin/
Node Name	http://192.192.51.193/admin/
	GET

Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:e6f53a77f1692ed32baa4220d6c522e5
URL	http://192.192.51.193/dashboard
Node Name	http://192.192.51.193/dashboard
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/dashboard/
Node Name	http://192.192.51.193/dashboard/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/depkind/index
Node Name	http://192.192.51.193/depkind/index
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/depys/index
Node Name	http://192.192.51.193/depys/index
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/device/compliant/about/about
Node Name	http://192.192.51.193/device/compliant/about/about
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/home/

Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	e6f53a77f1692ed32baa4220d6c522e5
Other Info	cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:visitID
URL	http://192.192.51.193/device/compliant/kurogo/error?args%5B_b%5D=%5B%5D&args%5Bcode%5D=02&args%5Bcode_name%5D=%EF%BC%88%E5%85%AC%E4%BD%88%E6%AC%84%EF%BC%89%E4%B8%80%E8%88%AC%E5%85%AC%E5%91%8A&code=server&id=qrybulletin&page=list
Node Name	http://192.192.51.193/device/compliant/kurogo/error (args[_b],args[code],args[code_name],code,id,page)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/kurogo/error?args%5B_b%5D=%5B%5D&args%5Bcode%5D=033&code=server&id=qryschoolmap&page=view
Node Name	http://192.192.51.193/device/compliant/kurogo/error (args[_b],args[code],code,id,page)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5BstartOver%5D=1&code=server&id=login&page=login
Node Name	http://192.192.51.193/device/compliant/kurogo/error (args[agreeTerm],args[authority],args[loginPassword],args[loginUser],args[startOver],code,id,page)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/kurogo/error?code=server&id=depkind&page=index
Node Name	http://192.192.51.193/device/compliant/kurogo/error (code,id,page)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/login/login?authority=nou
Node	

Name	http://192.192.51.193/device/compliant/login/login (authority)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/preferences/
Node Name	http://192.192.51.193/device/compliant/preferences/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/qrybulletin/
Node Name	http://192.192.51.193/device/compliant/qrybulletin/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/qrycalendar/
Node Name	http://192.192.51.193/device/compliant/qrycalendar/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/qrycontact/
Node Name	http://192.192.51.193/device/compliant/qrycontact/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/qrynews/
Node Name	http://192.192.51.193/device/compliant/qrynews/
	GET
Evidence	visitID
Other	

Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/qryrecruit/
Node Name	http://192.192.51.193/device/compliant/qryrecruit/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/qryroadmap/
Node Name	http://192.192.51.193/device/compliant/qryroadmap/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/qryschoolmap/
Node Name	http://192.192.51.193/device/compliant/qryschoolmap/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/device/compliant/schoolsystem/
Node Name	http://192.192.51.193/device/compliant/schoolsystem/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://192.192.51.193/home
Node Name	http://192.192.51.193/home
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/home/
Node Name	http://192.192.51.193/home/
	GET

Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:visitID
URL	http://192.192.51.193/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5Bid%5D=admin&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5Bpage%5D=index&args%5BstartOver%5D=1&code=server&id=login&page=login
Node Name	http://192.192.51.193/kurogo/error (args[agreeTerm],args[authority],args[id],args[loginPassword],args[loginUser],args[page],args[startOver],code,id,page)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/kurogo/error?args%5BagreeTerm%5D=1&args%5Bauthority%5D=nou&args%5BloginPassword%5D=ZAP&args%5BloginUser%5D=ZAP&args%5BstartOver%5D=1&code=server&id=login&page=login
Node Name	http://192.192.51.193/kurogo/error (args[agreeTerm],args[authority],args[loginPassword],args[loginUser],args[startOver],code,id,page)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	http://192.192.51.193/kurogo/error (code,id,page)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:visitID
URL	http://192.192.51.193/login
Node Name	http://192.192.51.193/login
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/login/

Node Name	http://192.192.51.193/login/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:e6f53a77f1692ed32baa4220d6c522e5
URL	http://192.192.51.193/login/?id=admin&page=index
Node Name	http://192.192.51.193/login/ (id,page)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/login/forgotpassword?_b=%5B%7B%22t%22%3A%22%5Cu767b%5Cu5165%22%2C%22lt%22%3A%22%5Cu767b%5Cu5165%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%2C%7B%22t%22%3A%22%5Cu767b%5Cu5165%22%2C%22lt%22%3A%22%5Cu767b%5Cu5165%22%2C%22p%22%3A%22login%22%2C%22a%22%3A%22authority%3Dnou%22%7D%5D
Node Name	http://192.192.51.193/login/forgotpassword (_b)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/login/login?agreeTerm=1&authority=nou&loginPassword=ZAP&loginUser=ZAP&startOver=1
Node Name	http://192.192.51.193/login/login (agreeTerm,authority,loginPassword,loginUser,startOver)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/login/login?authority=nou
Node Name	http://192.192.51.193/login/login (authority)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/login/login?authority=nou&id=admin&page=index

Node Name	http://192.192.51.193/login/login (authority,id,page)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/login/login?id=dashboard&page=index
Node Name	http://192.192.51.193/login/login (id,page)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/people/
Node Name	http://192.192.51.193/people/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:visitID
URL	http://192.192.51.193/people/group?_b=%5B%7B%22t%22%3A%22%5Cu806f%5Cu7d61%5Cu8cc7%5Cu8a0a%22%2C%22lt%22%3A%22%5Cu806f%5Cu7d61%5Cu8cc7%5Cu8a0a%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D&group=group1
Node Name	http://192.192.51.193/people/group (_b,group)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/preferences
Node Name	http://192.192.51.193/preferences
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/preferences/

Node Name	http://192.192.51.193/preferences/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/qrybulletin
Node Name	http://192.192.51.193/qrybulletin
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qrybulletin/
Node Name	http://192.192.51.193/qrybulletin/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qrycalendar
Node Name	http://192.192.51.193/qrycalendar
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qrycalendar/
Node Name	http://192.192.51.193/qrycalendar/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/qrycontact
Node Name	http://192.192.51.193/qrycontact
	GET

Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qrycontact/
Node Name	http://192.192.51.193/qrycontact/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qrycourse/index
Node Name	http://192.192.51.193/qrycourse/index
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qrynews
Node Name	http://192.192.51.193/qrynews
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qrynews/
Node Name	http://192.192.51.193/qrynews/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/qryrecruit
Node Name	http://192.192.51.193/qryrecruit
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qryrecruit/
Node	

Name	http://192.192.51.193/qryrecruit/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/qryroadmap
Node Name	http://192.192.51.193/qryroadmap
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qryroadmap/
Node Name	http://192.192.51.193/qryroadmap/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/qryroadmap/view?_b=%5B%5D&code=011
Node Name	http://192.192.51.193/qryroadmap/view (_b,code)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qryschoolmap
Node Name	http://192.192.51.193/qryschoolmap
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/qryschoolmap/
Node Name	http://192.192.51.193/qryschoolmap/
	GET
Evidence	deviceClassification

Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/qryschoolmap/view?_b=%5B%5D&code=000
Node Name	http://192.192.51.193/qryschoolmap/view (_b,code)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/rest/
Node Name	http://192.192.51.193/rest/
	GET
Evidence	e6f53a77f1692ed32baa4220d6c522e5
Other Info	cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:apiDeviceClassification
URL	http://192.192.51.193/robots.txt
Node Name	http://192.192.51.193/robots.txt
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/schoolsystem
Node Name	http://192.192.51.193/schoolsystem
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/schoolsystem/
Node Name	http://192.192.51.193/schoolsystem/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://192.192.51.193/sitemap.xml
Node	

Name	http://192.192.51.193/sitemap.xml
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/sitemap.xml/
Node Name	http://192.192.51.193/sitemap.xml/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/sitemap.xml/index
Node Name	http://192.192.51.193/sitemap.xml/index
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/stats/
Node Name	http://192.192.51.193/stats/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/stats/index
Node Name	http://192.192.51.193/stats/index
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	e6f53a77f1692ed32baa4220d6c522e5
Other	cookie:e6f53a77f1692ed32baa4220d6c522e5

Info	cookie:visitID
URL	http://192.192.51.193/login/login
Node Name	http://192.192.51.193/login/login ()(agreeTerm,anticsrf,authority,id,loginPassword,loginUser, page,startOver)
	POST
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://192.192.51.193/login/login
Node Name	http://192.192.51.193/login/login ()(agreeTerm,anticsrf,authority,loginPassword,loginUser, startOver)
	POST
Evidence	deviceClassification
Other Info	cookie:deviceClassification
Instances	69
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	**Tech Detected - Apache HTTP Server**
Description	The following "Web servers" technology was identified: Apache HTTP Server. Described as: Apache is a free and open-source cross-platform web server software.
URL	http://192.192.51.193/sitemap.xml/
Node Name	http://192.192.51.193/sitemap.xml/
	GET
Evidence	Apache
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	Apache
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*

Instances	2
Solution	
Reference	https://httpd.apache.org/
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Bootstrap**
Description	The following "UI frameworks" technology was identified: Bootstrap. Described as: Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components.
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	<link href="/device/compliant/min/g=file-/common/css/bootstrap@5.3.3.min.css
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 5.3.3
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	<link href="/device/compliant/min/g=file-/common/css/bootstrap@5.3.3.min.css
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 5.3.3
Instances	2
Solution	
Reference	https://getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Font Awesome**
Description	The following "Font scripts" technology was identified: Font Awesome. Described as: Font Awesome is a font and icon toolkit based on CSS and Less.
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/

	GET
Evidence	fontawesome-free@6.6.0
Other Info	The following version(s) is/are associated with the identified tech: 6.6.0
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	fontawesome-free@6.6.0
Other Info	The following version(s) is/are associated with the identified tech: 6.6.0
Instances	2
Solution	
Reference	https://fontawesome.com/
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - HSTS**
Description	The following "Security" technology was identified: HSTS. Described as: HTTP Strict Transport Security (HSTS) informs browsers that the site should only be accessed using HTTPS.
URL	http://192.192.51.193/robots.txt
Node Name	http://192.192.51.193/robots.txt
	GET
Evidence	Strict-Transport-Security
Other Info	
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	Strict-Transport-Security
Other Info	
Instances	2
Solution	
Reference	https://www.rfc-editor.org/rfc/rfc6797#section-6.1
CWE Id	

WASC Id	13
Plugin Id	10004

Informational	Tech Detected - jQuery
Description	The following "JavaScript libraries" technology was identified: jQuery. Described as: jQuery is a JavaScript library which is a free, open-source software designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax.
URL	http://192.192.51.193/device/compliant/home/
Node Name	http://192.192.51.193/device/compliant/home/
	GET
Evidence	/jquery-3.7.1.
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 3.7.1
URL	https://192.192.51.193/device/compliant/home/
Node Name	https://192.192.51.193/device/compliant/home/
	GET
Evidence	/jquery-3.7.1.
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 3.7.1
Instances	2
Solution	
Reference	https://jquery.com
CWE Id	
WASC Id	13
Plugin Id	10004

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://192.192.51.193/device/compliant/login/login?authority=nou
Node Name	http://192.192.51.193/device/compliant/login/login (authority)
	GET
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://192.192.51.193/device/compliant/login/login?authority=nou appears to include user input in: a(n) [input] tag [value] attribute The user input found was: authority=nou The user-controlled value was: nou
URL	http://192.192.51.193/login/login?agreeTerm=1&authority=nou&loginPassword=ZAP&loginUser=ZAP&startOver=1
Node Name	http://192.192.51.193/login/login (agreeTerm,authority,loginPassword,loginUser,startOver)
	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://192.192.51.193/login/login?agreeTerm=1&authority=nou&loginPassword=ZAP&loginUser=ZAP&startOver=1 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: agreeTerm=1 The user-controlled value was: ie=edge,chrome=1
URL	http://192.192.51.193/login/login?agreeTerm=1&authority=nou&loginPassword=ZAP&loginUser=ZAP&startOver=1
Node Name	http://192.192.51.193/login/login (agreeTerm,authority,loginPassword,loginUser,startOver)
	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://192.192.51.193/login/login?agreeTerm=1&authority=nou&loginPassword=ZAP&loginUser=ZAP&startOver=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: authority=nou The user-controlled value was:

	nou
URL	http://192.192.51.193/login/login?authority=nou
Node Name	http://192.192.51.193/login/login (authority)
	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://192.192.51.193/login/login?authority=nou appears to include user input in: a(n) [input] tag [value] attribute The user input found was: authority=nou The user-controlled value was: nou
URL	http://192.192.51.193/login/login?authority=nou&id=admin&page=index
Node Name	http://192.192.51.193/login/login (authority,id,page)
	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://192.192.51.193/login/login?authority=nou&id=admin&page=index appears to include user input in: a(n) [input] tag [value] attribute The user input found was: authority=nou The user-controlled value was: nou
URL	http://192.192.51.193/login/login?authority=nou&id=admin&page=index
Node Name	http://192.192.51.193/login/login (authority,id,page)
	GET
Evidence	
	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://192.192.51.193/login/login?authority=nou&id=admin&page=index

Other Info	appears to include user input in: a(n) [input] tag [value] attribute The user input found was: id=admin The user-controlled value was: admin
URL	http://192.192.51.193/login/login?authority=nou&id=admin&page=index
Node Name	http://192.192.51.193/login/login (authority,id,page)
	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://192.192.51.193/login/login?authority=nou&id=admin&page=index appears to include user input in: a(n) [input] tag [value] attribute The user input found was: page=index The user-controlled value was: index
Instances	7
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