ZAP by Checkmarx Scanning Report

Sites: https://cdn.jsdelivr.net https://android.clients.google.com https://140.119.221.102 http://140.119.221.102

Generated on , 21 4 2026 10:46:43

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

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

	Risk Level	Number of Instances
CSP: script-src unsafe-inline	Medium	Systemic
CSP: style-src unsafe-inline	Medium	Systemic
Sub Resource Integrity Attribute Missing	Medium	Systemic
Cookie No HttpOnly Flag	Low	1
Cookie without SameSite Attribute	Low	Systemic
Cross-Domain JavaScript Source File Inclusion	Low	2
!authhelper.session-detect.name!	Informational	5
!wappalyzer.alert.name.prefix!	Informational	1
Modern Web Application	Informational	Systemic
Session Management Response Identified	Informational	22
Tech Detected - Apache HTTP Server	Informational	2
Tech Detected - Bootstrap	Informational	1
Tech Detected - Google Maps	Informational	1
Tech Detected - HSTS	Informational	2
Tech Detected - jQuery	Informational	1
Tech Detected - jsDelivr	Informational	2
User Controllable HTML Element Attribute (Potential XSS)	Informational	4

Alert Detail

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://140.119.221.102/
Node Name	http://140.119.221.102/
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other Info	script-src includes unsafe-inline.
URL	http://140.119.221.102/device/compliant/nami/index
Node Name	http://140.119.221.102/device/compliant/nami/index
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other Info	script-src includes unsafe-inline.
URL	http://140.119.221.102/device/compliant/timetable/index
Node Name	http://140.119.221.102/device/compliant/timetable/index
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other Info	script-src includes unsafe-inline.
URL	http://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET

Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other Info	script-src includes unsafe-inline.
URL	http://140.119.221.102/sitemap.xml
Node Name	http://140.119.221.102/sitemap.xml
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
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://140.119.221.102/
Node Name	http://140.119.221.102/
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other	

Info	style-src includes unsafe-inline.
URL	http://140.119.221.102/device/compliant/nami/index
Node Name	http://140.119.221.102/device/compliant/nami/index
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other Info	style-src includes unsafe-inline.
URL	http://140.119.221.102/device/compliant/timetable/index
Node Name	http://140.119.221.102/device/compliant/timetable/index
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other Info	style-src includes unsafe-inline.
URL	http://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
Other Info	style-src includes unsafe-inline.
URL	http://140.119.221.102/sitemap.xml
Node Name	http://140.119.221.102/sitemap.xml
	GET
Evidence	default-src 'self' ; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net maps.google.com ; style-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net fonts.googleapis.com ; img-src 'self' data: *.gstatic.com *.googleapis.com *.google.com ; font-src 'self' https://cdn.jsdelivr.net fonts.gstatic.com ; connect-src 'self' *.googleapis.com https://cdn.jsdelivr.net ; frame-src 'self' ; media-src 'self' ; object-src 'none' ; base-uri 'self' ; form-action 'self' https://webapp.nccu.edu.tw ; frame-ancestors 'self' ;
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

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://140.119.221.102/device/compliant/library/index
Node Name	http://140.119.221.102/device/compliant/library/index
	GET
Evidence	<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet" media="all" type="text/css"/>
Other Info	
URL	http://140.119.221.102/device/compliant/nccu-news/index
Node Name	http://140.119.221.102/device/compliant/nccu-news/index
	GET
Evidence	<link href="https://cdn.jsdelivr.net/npm/@fortawesome/fontawesome-free@6.0.0/css/all.min.css" rel="stylesheet" media="all" type="text/css"/>
Other Info	
URL	http://140.119.221.102/device/compliant/nccu-news/index
Node Name	http://140.119.221.102/device/compliant/nccu-news/index
	GET
Evidence	<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet" media="all" type="text/css"/>
Other Info	
URL	http://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET

Evidence	<link href="https://cdn.jsdelivr.net/npm/@fortawesome/fontawesome-free@6.0.0/css/all.min.css" rel="stylesheet" media="all" type="text/css"/>
Other Info	
URL	http://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET
Evidence	<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet" media="all" type="text/css"/>
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

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://140.119.221.102/device/compliant/home/
Node Name	http://140.119.221.102/device/compliant/home/
	GET
Evidence	Set-Cookie: 9a413b28155ba831d19c5bf733947006
Other Info	
Instances	1
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 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://140.119.221.102/
Node Name	http://140.119.221.102/
	GET

Evidence	Set-Cookie: deviceClassification
Other Info	
URL	http://140.119.221.102/device/compliant/home/
Node Name	http://140.119.221.102/device/compliant/home/
	GET
Evidence	Set-Cookie: 9a413b28155ba831d19c5bf733947006
Other Info	
URL	http://140.119.221.102/device/compliant/nccu-news/index
Node Name	http://140.119.221.102/device/compliant/nccu-news/index
	GET
Evidence	Set-Cookie: visitID
Other Info	
URL	http://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET
Evidence	Set-Cookie: visitID
Other Info	
URL	http://140.119.221.102/sitemap.xml
Node Name	http://140.119.221.102/sitemap.xml
	GET
Evidence	Set-Cookie: deviceClassification
Other Info	
Instances	Systemic
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://140.119.221.102/device/compliant/map/index

Node Name	http://140.119.221.102/device/compliant/map/index
	GET
Evidence	<script src="http://maps.google.com/maps/api/js?sensor=true&key=AIzaSyCACefBMK8t6ZVduOKGSkN7C-Js3D2oVV8" type="text/javascript"></script>
Other Info	
URL	http://140.119.221.102/map/
Node Name	http://140.119.221.102/map/
	GET
Evidence	<script src="http://maps.google.com/maps/api/js?sensor=true&key=AIzaSyCACefBMK8t6ZVduOKGSkN7C-Js3D2oVV8" type="text/javascript"></script>
Other Info	
Instances	2
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

Informational	**!authhelper.session-detect.name!**
Description	!authhelper.session-detect.desc!
URL	http://140.119.221.102/device/compliant/home/
Node Name	http://140.119.221.102/device/compliant/home/
	GET
Evidence	9a413b28155ba831d19c5bf733947006
Other Info	cookie:9a413b28155ba831d19c5bf733947006 cookie:visitID
URL	http://140.119.221.102/device/compliant/nccu-news/index
Node Name	http://140.119.221.102/device/compliant/nccu-news/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index

	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://140.119.221.102/home/help?_b=%5B%7B%22t%22%3A%22%5Cu5bb6%5Cu76ee%5Cu9304%22%2C%22lt%22%3A%22%5Cu5bb6%5Cu76ee%5Cu9304%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D
Node Name	http://140.119.221.102/home/help (_b)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	http://140.119.221.102/kurogo/error (code,id,page)
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
Instances	5
Solution	!authhelper.session-detect.soln!
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informational	**!wappalyzer.alert.name.prefix!**
Description	!wappalyzer.alert.desc!!wappalyzer.alert.desc.extended!
URL	http://140.119.221.102/links/
Node Name	http://140.119.221.102/links/
	GET
Evidence	<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css
Other Info	!wappalyzer.alert.otherinfo.cpe! !wappalyzer.alert.otherinfo.version!
Instances	1
Solution	
Reference	https://getbootstrap.com
CWE Id	

WASC Id	13
Plugin Id	10004

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://140.119.221.102/device/compliant/home/
Node Name	http://140.119.221.102/device/compliant/home/
	GET
Evidence	
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://140.119.221.102/device/compliant/library/index
Node Name	http://140.119.221.102/device/compliant/library/index
	GET
Evidence	
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://140.119.221.102/device/compliant/nccu-news/index
Node Name	http://140.119.221.102/device/compliant/nccu-news/index
	GET
Evidence	
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://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET
Evidence	
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://140.119.221.102/home/
Node Name	http://140.119.221.102/home/
	GET
Evidence	
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	**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://140.119.221.102/
Node Name	http://140.119.221.102/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/about/
Node Name	http://140.119.221.102/about/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/calendar/
Node Name	http://140.119.221.102/calendar/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/device/compliant/about-app/index
Node Name	http://140.119.221.102/device/compliant/about-app/index
	GET
Evidence	visitID
Other Info	cookie:visitID
	http://140.119.221.102/device/compliant/about-app/view?_b=%5B%7B%22t%22%3A%22%

URL	5Cu95dc%5Cu65bc%5Cu884c%5Cu52d5%5Cu653f%5Cu5927%22%2C%22lt%22%3A%22%5Cu95dc%5Cu65bc%5Cu884c%5Cu52d5%5Cu653f%5Cu5927%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D&feed=privacy
Node Name	http://140.119.221.102/device/compliant/about-app/view (_b,feed)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://140.119.221.102/device/compliant/emergency-contacts/index
Node Name	http://140.119.221.102/device/compliant/emergency-contacts/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://140.119.221.102/device/compliant/login/login?authority=nccu&id=activity&page=index
Node Name	http://140.119.221.102/device/compliant/login/login (authority,id,page)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://140.119.221.102/device/compliant/map/bookmarks?_b=%5B%7B%22t%22%3A%22%5Cu6821%5Cu5712%5Cu5730%5Cu5716%22%2C%22lt%22%3A%22%5Cu6821%5Cu5712%5Cu5730%5Cu5716%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D
Node Name	http://140.119.221.102/device/compliant/map/bookmarks (_b)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://140.119.221.102/device/compliant/map/index?_b=%5B%5D&group=maps&listview=1
Node Name	http://140.119.221.102/device/compliant/map/index (_b,group,listview)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	http://140.119.221.102/fullweb/
Node	

Name	http://140.119.221.102/fullweb/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/kurogo/
Node Name	http://140.119.221.102/kurogo/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/links/
Node Name	http://140.119.221.102/links/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/login/
Node Name	http://140.119.221.102/login/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/map/
Node Name	http://140.119.221.102/map/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/news/
Node Name	http://140.119.221.102/news/
	GET

Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/people/
Node Name	http://140.119.221.102/people/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
URL	http://140.119.221.102/sitemap.xml
Node Name	http://140.119.221.102/sitemap.xml
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/sitemap.xml/
Node Name	http://140.119.221.102/sitemap.xml/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/sitemap.xml/index
Node Name	http://140.119.221.102/sitemap.xml/index
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/sites/
Node Name	http://140.119.221.102/sites/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/social/

Node Name	http://140.119.221.102/social/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	http://140.119.221.102/video/
Node Name	http://140.119.221.102/video/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification cookie:visitID
Instances	22
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://140.119.221.102/device/compliant/min/?config=home&g=file-/common/javascript/lib/jquery-cycle2/jquery.cycle2.center.min.js
Node Name	http://140.119.221.102/device/compliant/min/ (config,g)
	GET
Evidence	Apache
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*
URL	http://140.119.221.102/robots.txt
Node Name	http://140.119.221.102/robots.txt
	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://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET
Evidence	<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.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: 5.3.0
Instances	1
Solution	
Reference	https://getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - Google Maps
Description	The following "Maps" technology was identified: Google Maps. Described as: Google Maps is a web mapping service. It offers satellite imagery, aerial photography, street maps, 360° interactive panoramic views of streets, real-time traffic conditions, and route planning for traveling by foot, car, bicycle and air, or public transportation.
URL	http://140.119.221.102/device/compliant/map/index
Node Name	http://140.119.221.102/device/compliant/map/index
	GET
Evidence	//maps.google.com/maps/api/js
Other Info	
Instances	1
Solution	
Reference	https://maps.google.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://140.119.221.102/device/compliant/min/?config=home&g=file-/common/javascript/lib/jquery-cycle2/jquery.cycle2.center.min.js
Node Name	http://140.119.221.102/device/compliant/min/ (config,g)
	GET
Evidence	Strict-Transport-Security
Other Info	
URL	http://140.119.221.102/robots.txt
Node Name	http://140.119.221.102/robots.txt
	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://140.119.221.102/device/compliant/home/
Node Name	http://140.119.221.102/device/compliant/home/
	GET
Evidence	/jquery-3.7.1.
Other	The following CPE is associated with the identified tech: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*

Info	The following version(s) is/are associated with the identified tech: 3.7.1
Instances	1
Solution	
Reference	https://jquery.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - jsDelivr**
Description	The following "CDN" technology was identified: jsDelivr. Described as: JSDelivr is a free public CDN for open-source projects. It can serve web files directly from the npm registry and GitHub repositories without any configuration.
URL	http://140.119.221.102/device/compliant/transportation/index
Node Name	http://140.119.221.102/device/compliant/transportation/index
	GET
Evidence	
Other Info	
URL	http://140.119.221.102/links/
Node Name	http://140.119.221.102/links/
	GET
Evidence	
Other Info	
Instances	2
Solution	
Reference	https://www.jsdelivr.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://140.119.221.102/device/compliant/login/login?authority=nccu&id=activity&page=index
Node Name	http://140.119.221.102/device/compliant/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://140.119.221.102/device/compliant/login/login?authority=nccu&id=activity&page=index appears to include user input in: a(n) [input] tag [value] attribute The user input found was: authority=nccu The user-controlled value was: nccu
URL	http://140.119.221.102/device/compliant/login/login?authority=nccu&id=activity&page=index
Node Name	http://140.119.221.102/device/compliant/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://140.119.221.102/device/compliant/login/login?authority=nccu&id=activity&page=index appears to include user input in: a(n) [input] tag [value] attribute The user input found was: id=activity The user-controlled value was: activity
URL	http://140.119.221.102/device/compliant/login/login?authority=nccu&id=activity&page=index
Node Name	http://140.119.221.102/device/compliant/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://140.119.221.102/device/compliant/login/login?authority=nccu&id=activity&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
URL	http://140.119.221.102/device/compliant/map/index?_b=%5B%5D&group=maps&listview=1
Node Name	http://140.119.221.102/device/compliant/map/index (_b,group,listview)
	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://140.119.221.102/device/compliant/map/index?_b=%5B%5D&group=maps&listview=1 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: listview=1 The user-controlled value was: ie=edge,chrome=1
Instances	4
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