



Site: <https://outbound.nccu.edu.tw>

Generated on , 20 10 2026 11:25:37

ZAP Version: 2.17.0

ZAP by [Checkmarx](#)

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	2
Low	4
Informational	4

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP warnings logged - see the zap.log file for details	1
	Informational	https://outbound.nccu.edu.tw	Percentage of responses with status code 2xx	28 %
	Informational	https://outbound.nccu.edu.tw	Percentage of responses with status code 3xx	38 %
	Informational	https://outbound.nccu.edu.tw	Percentage of responses with status code 4xx	32 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type application/pdf	16 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type application/vnd.oasis.opendocument.text	1 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type image/jpeg	1 %

	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type image/png	8 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type text/css	21 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type text/html	23 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type text/javascript	26 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with content type text/plain	1 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with method GET	97 %
	Informational	https://outbound.nccu.edu.tw	Percentage of endpoints with method POST	2 %
	Informational	https://outbound.nccu.edu.tw	Count of total endpoints	93
	Informational	https://outbound.nccu.edu.tw	Percentage of slow responses	58 %

	Risk Level	Number of Instances
Vulnerable JS Library	High	1
Content Security Policy (CSP) Header Not Set	Medium	5
Sub Resource Integrity Attribute Missing	Medium	Systemic
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3
Cookie No HttpOnly Flag	Low	Systemic
Cookie Without Secure Flag	Low	Systemic
Cross-Domain JavaScript Source File Inclusion	Low	Systemic
Information Disclosure - Suspicious Comments	Informational	3
Modern Web Application	Informational	Systemic
Re-examine Cache-control Directives	Informational	Systemic
Session Management Response Identified	Informational	50

Alert Detail

High	Vulnerable JS Library
Description	The identified library appears to be vulnerable.

URL	https://outbound.nccu.edu.tw/enrolment/vendor/handlebars/4.7.7/handlebars.runtime.js
Node Name	https://outbound.nccu.edu.tw/enrolment/vendor/handlebars/4.7.7/handlebars.runtime.js
	GET
Evidence	<pre>/*! @license handlebars v4.7.7</pre> The identified library handlebars, version 4.7.7 is vulnerable. CVE-2026-33937 CVE-2026-33939 CVE-2026-33916 CVE-2026-33938 CVE-2026-33940 CVE-2026-33941 https://github.com/handlebars-lang/handlebars.js/commit/68d8df5a88e0a26fe9e6084c5c6aae67b07da2 https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-9cx6-37pm-9jff https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-3mf8-83xf-c92r https://github.com/handlebars-lang/handlebars.js/releases/tag/v4.7.9 https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-7rx3-28cr-v5wh https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-2qvq-rjwj-gvw9 https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-xhpf-hc6g-r9c6 https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-442j-39wm-28r2 https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-2w6w-674q-4c4q https://github.com/handlebars-lang/handlebars.js/security/advisories/GHSA-xjpf-3mr7-gcpf
Other Info	
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/2021/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	1395
WASC Id	
Plugin Id	10003

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://outbound.nccu.edu.tw/enrolment/login
Node Name	https://outbound.nccu.edu.tw/enrolment/login

	GET
Evidence	
Other Info	
URL	https://outbound.nccu.edu.tw/enrolment/user/forget-password
Node Name	https://outbound.nccu.edu.tw/enrolment/user/forget-password
	GET
Evidence	
Other Info	
URL	https://outbound.nccu.edu.tw/page/\${%7Bdata%7D
Node Name	https://outbound.nccu.edu.tw/page/\${data}
	GET
Evidence	
Other Info	
URL	https://outbound.nccu.edu.tw/sitemap.xml
Node Name	https://outbound.nccu.edu.tw/sitemap.xml
	GET
Evidence	
Other Info	
URL	https://outbound.nccu.edu.tw/%E5%9C%B0%E5%8D%80%E6%9C%89%E4%B8%8D%E5%90%8C%E5%AD%B8%E5%88%B6%E8%88%87%E8%A1%8C%E6%94%BF%E6%9C%9F%E7%A8%8B%E7%BC%8C%E5%9B%A0%E6%AD%A4%E5%8F%AF%E5%9C%A8%E5%9C%8B%E5%90%88%E8%99%95%E7%B6%B2%E9%A0%81
Node Name	https://outbound.nccu.edu.tw/
	GET
Evidence	
Other Info	
Instances	5
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	https://outbound.nccu.edu.tw/page/11
Node Name	https://outbound.nccu.edu.tw/page/11
	GET
Evidence	<script nonce="wh2TASmbtWGjbzWn1fjkoZAI6Gohw0Xi" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/page/12
Node Name	https://outbound.nccu.edu.tw/page/12
	GET
Evidence	<script nonce="MFaqxZ3A6m3V1rG6R9HgXVdMeYV0wzIX" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/page/7
Node Name	https://outbound.nccu.edu.tw/page/7
	GET
Evidence	<script nonce="Jq0EVparlViNQJXfAJPAslaqE5vad4Y8" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/post/40
Node Name	https://outbound.nccu.edu.tw/post/40
	GET
Evidence	<script nonce="ZeyKaMoWbStbidKgeHbihhpJQZh9dUFv" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/sitemap.xml

Node Name	https://outbound.nccu.edu.tw/sitemap.xml
	GET
Evidence	<script nonce="Zx603FmYAFBGwnlwPsWOx6vazx3tkQCx" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
Instances	Systemic
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	https://outbound.nccu.edu.tw/enrolment/
Node Name	https://outbound.nccu.edu.tw/enrolment/
	GET
Evidence	
Other Info	Location header URI length: 44 [https://outbound.nccu.edu.tw/enrolment/login]. Predicted response size: 344. Response Body Length: 422.
URL	https://outbound.nccu.edu.tw/enrolment/login
Node Name	https://outbound.nccu.edu.tw/enrolment/login ()(_token,captcha,password,uid)
	POST
Evidence	
Other Info	Location header URI length: 44 [https://outbound.nccu.edu.tw/enrolment/login]. Predicted response size: 344. Response Body Length: 422.
URL	https://outbound.nccu.edu.tw/enrolment/user/forget-password
Node Name	https://outbound.nccu.edu.tw/enrolment/user/forget-password ()(_token,uid)
	POST
Evidence	
	Location header URI length: 59 [https://outbound.nccu.edu.tw/enrolment/user/forget-password].

Other Info	Predicted response size: 359. Response Body Length: 482.
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	https://outbound.nccu.edu.tw/
Node Name	https://outbound.nccu.edu.tw/
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://outbound.nccu.edu.tw/page/11
Node Name	https://outbound.nccu.edu.tw/page/11
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://outbound.nccu.edu.tw/page/12
Node Name	https://outbound.nccu.edu.tw/page/12
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://outbound.nccu.edu.tw/page/7
Node Name	https://outbound.nccu.edu.tw/page/7
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other	

Info	
URL	https://outbound.nccu.edu.tw/post/40
Node Name	https://outbound.nccu.edu.tw/post/40
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	Systemic
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	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://outbound.nccu.edu.tw/
Node Name	https://outbound.nccu.edu.tw/
	GET
Evidence	Set-Cookie: _session
Other Info	
URL	https://outbound.nccu.edu.tw/page/11
Node Name	https://outbound.nccu.edu.tw/page/11
	GET
Evidence	Set-Cookie: _session
Other Info	
URL	https://outbound.nccu.edu.tw/page/12
Node Name	https://outbound.nccu.edu.tw/page/12
	GET
Evidence	Set-Cookie: _session
Other Info	
URL	https://outbound.nccu.edu.tw/page/7
Node Name	https://outbound.nccu.edu.tw/page/7

	GET
Evidence	Set-Cookie: _session
Other Info	
URL	https://outbound.nccu.edu.tw/post/40
Node Name	https://outbound.nccu.edu.tw/post/40
	GET
Evidence	Set-Cookie: _session
Other Info	
Instances	Systemic
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	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://outbound.nccu.edu.tw/
Node Name	https://outbound.nccu.edu.tw/
	GET
Evidence	<script nonce="V6arO9uQfIfANPui6Y6ssQKF1oOHILha" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/
Node Name	https://outbound.nccu.edu.tw/
	GET
Evidence	<script nonce="bQZwpePJ6YZOBjjKPyV50m5AWIXU7DV7" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/page/11
Node Name	https://outbound.nccu.edu.tw/page/11
	GET

Evidence	<script nonce="wh2TASmbtWGjbzWn1fjkoZAI6Gohw0Xi" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/page/7
Node Name	https://outbound.nccu.edu.tw/page/7
	GET
Evidence	<script nonce="Jq0EVparlViNQJXfAJPAslaqE5vad4Y8" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
URL	https://outbound.nccu.edu.tw/sitemap.xml
Node Name	https://outbound.nccu.edu.tw/sitemap.xml
	GET
Evidence	<script nonce="Zx603FmYAFBGwnlwPsWOx6vazx3tkQCx" async src="https://www.googletagmanager.com/gtag/js?id=G-0LF8XHL8CH"></script>
Other Info	
Instances	Systemic
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	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://outbound.nccu.edu.tw/enrolment/js/jquery.tagsinput-revisited.js
Node Name	https://outbound.nccu.edu.tw/enrolment/js/jquery.tagsinput-revisited.js
	GET
Evidence	// If a user types a delimiter c
Other Info	The following pattern was used: \bUSER\b and was detected 3 times, the first in likely comment: "// If a user types a delimiter create a new tag", see evidence field for the suspicious comment/snippet.
URL	https://outbound.nccu.edu.tw/enrolment/vendor/handlebars/4.7.7/handlebars.runtime.js
Node Name	https://outbound.nccu.edu.tw/enrolment/vendor/handlebars/4.7.7/handlebars.runtime.js
	GET

Evidence	OTHERWISE, ARISING FROM, OUT OF OR IN CONNE
Other Info	The following pattern was used: \bFROM\b and was detected 5 times, the first in likely comment: "/*! @license handlebars v4.7.7 Copyright (C) 2011-2019 by Yehuda Katz Permission is hereby granted, free of charge, to any", see evidence field for the suspicious comment/snippet.
URL	https://outbound.nccu.edu.tw/enrolment/vendor/handlebars/4.7.7/handlebars.runtime.js
Node Name	https://outbound.nccu.edu.tw/enrolment/vendor/handlebars/4.7.7/handlebars.runtime.js
	GET
Evidence	issue under safari where we can't directly s
Other Info	The following pattern was used: \bWHERE\b and was detected in likely comment: "// Work around issue under safari where we can't directly set the column value", see evidence field for the suspicious comment/snippet.
Instances	3
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	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	https://outbound.nccu.edu.tw/page/11
Node Name	https://outbound.nccu.edu.tw/page/11
	GET
Evidence	 <i class="fa fa-caret-right fa-fw arrow first-level-arrow"></i>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://outbound.nccu.edu.tw/page/12
Node Name	https://outbound.nccu.edu.tw/page/12
	GET
Evidence	 <i class="fa fa-caret-right fa-fw arrow first-level-arrow"></i>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://outbound.nccu.edu.tw/page/7

Node Name	https://outbound.nccu.edu.tw/page/7
	GET
Evidence	 <i class="fa fa-caret-right fa-fw arrow first-level-arrow"></i>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://outbound.nccu.edu.tw/post/40
Node Name	https://outbound.nccu.edu.tw/post/40
	GET
Evidence	 <i class="fa fa-caret-right fa-fw arrow first-level-arrow"></i>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	https://outbound.nccu.edu.tw/sitemap.xml
Node Name	https://outbound.nccu.edu.tw/sitemap.xml
	GET
Evidence	 <i class="fa fa-caret-right fa-fw arrow first-level-arrow"></i>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
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
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://outbound.nccu.edu.tw/
Node Name	https://outbound.nccu.edu.tw/
	GET
Evidence	no-cache, private
Other Info	
URL	https://outbound.nccu.edu.tw/page/11
Node	

Name	https://outbound.nccu.edu.tw/page/11
	GET
Evidence	no-cache, private
Other Info	
URL	https://outbound.nccu.edu.tw/page/7
Node Name	https://outbound.nccu.edu.tw/page/7
	GET
Evidence	no-cache, private
Other Info	
URL	https://outbound.nccu.edu.tw/post/40
Node Name	https://outbound.nccu.edu.tw/post/40
	GET
Evidence	no-cache, private
Other Info	
URL	https://outbound.nccu.edu.tw/robots.txt
Node Name	https://outbound.nccu.edu.tw/robots.txt
	GET
Evidence	
Other Info	
Instances	Systemic
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	https://outbound.nccu.edu.tw/
Node Name	https://outbound.nccu.edu.tw/
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/enrolment/
Node Name	https://outbound.nccu.edu.tw/enrolment/
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/enrolment/login
Node Name	https://outbound.nccu.edu.tw/enrolment/login
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/enrolment/user/forget-password
Node Name	https://outbound.nccu.edu.tw/enrolment/user/forget-password
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/06fa21cb-c5f3-4b3c-b52c-4f802f707ee4
Node Name	https://outbound.nccu.edu.tw/media/files/06fa21cb-c5f3-4b3c-b52c-4f802f707ee4
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/28c640bf-e21c-49c4-b517-0ac7005b64fc
Node Name	https://outbound.nccu.edu.tw/media/files/28c640bf-e21c-49c4-b517-0ac7005b64fc

	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/38d2255b-f4cb-4136-a4b6-61f218fe280c
Node Name	https://outbound.nccu.edu.tw/media/files/38d2255b-f4cb-4136-a4b6-61f218fe280c
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/3ea13799-2dec-472d-b714-36c0fde350d3
Node Name	https://outbound.nccu.edu.tw/media/files/3ea13799-2dec-472d-b714-36c0fde350d3
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/49780a9b-4996-4a52-ab04-a269cf282685
Node Name	https://outbound.nccu.edu.tw/media/files/49780a9b-4996-4a52-ab04-a269cf282685
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/6073ebf1-2c58-4bc2-a6ff-21f596a03fde
Node Name	https://outbound.nccu.edu.tw/media/files/6073ebf1-2c58-4bc2-a6ff-21f596a03fde
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/77f81fe4-0b38-4577-acf6-4e3728390f4b
Node Name	https://outbound.nccu.edu.tw/media/files/77f81fe4-0b38-4577-acf6-4e3728390f4b
	GET

Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/80c15f9d-3b21-400d-b6fc-2cd09c3c1510
Node Name	https://outbound.nccu.edu.tw/media/files/80c15f9d-3b21-400d-b6fc-2cd09c3c1510
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/a950ad8b-cb06-4201-87fc-cf8ed89d31ff
Node Name	https://outbound.nccu.edu.tw/media/files/a950ad8b-cb06-4201-87fc-cf8ed89d31ff
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/b02b908d-e76f-4d0e-9618-1afe497b54f3
Node Name	https://outbound.nccu.edu.tw/media/files/b02b908d-e76f-4d0e-9618-1afe497b54f3
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/c9d4ca9c-c23c-47a8-8cfb-b16cbfec167d
Node Name	https://outbound.nccu.edu.tw/media/files/c9d4ca9c-c23c-47a8-8cfb-b16cbfec167d
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/cbce4d5a-d8bc-44e4-ae22-7af2d246bb24
Node Name	https://outbound.nccu.edu.tw/media/files/cbce4d5a-d8bc-44e4-ae22-7af2d246bb24
	GET
Evidence	_session
Other	cookie:_session

Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/d1136f8f-133a-44fa-a071-4bb782603015
Node Name	https://outbound.nccu.edu.tw/media/files/d1136f8f-133a-44fa-a071-4bb782603015
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/d7dfef11-ea3-4c10-80bb-90df66b8ca6c
Node Name	https://outbound.nccu.edu.tw/media/files/d7dfef11-ea3-4c10-80bb-90df66b8ca6c
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/ea2cfd0b-ee9b-4c9c-94fc-de20fdc3ffd8
Node Name	https://outbound.nccu.edu.tw/media/files/ea2cfd0b-ee9b-4c9c-94fc-de20fdc3ffd8
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/f353edca-d805-48ac-a6c9-9f66cf925c9e
Node Name	https://outbound.nccu.edu.tw/media/files/f353edca-d805-48ac-a6c9-9f66cf925c9e
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/f79594b0-eb50-4812-b563-90c015d2597c
Node Name	https://outbound.nccu.edu.tw/media/files/f79594b0-eb50-4812-b563-90c015d2597c
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/\$%7Bdata%7D

Node Name	https://outbound.nccu.edu.tw/page/\${data}
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/11
Node Name	https://outbound.nccu.edu.tw/page/11
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/12
Node Name	https://outbound.nccu.edu.tw/page/12
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/15
Node Name	https://outbound.nccu.edu.tw/page/15
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/3
Node Name	https://outbound.nccu.edu.tw/page/3
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/6
Node Name	https://outbound.nccu.edu.tw/page/6
	GET

Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/7
Node Name	https://outbound.nccu.edu.tw/page/7
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/8
Node Name	https://outbound.nccu.edu.tw/page/8
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/post/40
Node Name	https://outbound.nccu.edu.tw/post/40
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/post/48
Node Name	https://outbound.nccu.edu.tw/post/48
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/post/75
Node Name	https://outbound.nccu.edu.tw/post/75
	GET
Evidence	_session

Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/search?query=ZAP
Node Name	https://outbound.nccu.edu.tw/search (query)
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/enrolment/login
Node Name	https://outbound.nccu.edu.tw/enrolment/login ()(_token,captcha,password,uid)
	POST
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/enrolment/user/forget-password
Node Name	https://outbound.nccu.edu.tw/enrolment/user/forget-password ()(_token,uid)
	POST
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/enrolment/login
Node Name	https://outbound.nccu.edu.tw/enrolment/login
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/06fa21cb-c5f3-4b3c-b52c-4f802f707ee4
Node Name	https://outbound.nccu.edu.tw/media/files/06fa21cb-c5f3-4b3c-b52c-4f802f707ee4
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/2ac5a2af-d2aa-4b3f-aa3d-68a146c4616e

Node Name	https://outbound.nccu.edu.tw/media/files/2ac5a2af-d2aa-4b3f-aa3d-68a146c4616e
	GET
Evidence	_session
Other Info	cookie:_session
URL	https://outbound.nccu.edu.tw/media/files/2ac5a2af-d2aa-4b3f-aa3d-68a146c4616e
Node Name	https://outbound.nccu.edu.tw/media/files/2ac5a2af-d2aa-4b3f-aa3d-68a146c4616e
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/3ea13799-2dec-472d-b714-36c0fde350d3
Node Name	https://outbound.nccu.edu.tw/media/files/3ea13799-2dec-472d-b714-36c0fde350d3
	GET
Evidence	_session
Other Info	cookie:_session
URL	https://outbound.nccu.edu.tw/media/files/3ea13799-2dec-472d-b714-36c0fde350d3
Node Name	https://outbound.nccu.edu.tw/media/files/3ea13799-2dec-472d-b714-36c0fde350d3
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/4969ffd4-31e3-4bb1-a2b8-a3618eb141ce
Node Name	https://outbound.nccu.edu.tw/media/files/4969ffd4-31e3-4bb1-a2b8-a3618eb141ce
	GET
Evidence	_session
Other Info	cookie:_session
URL	https://outbound.nccu.edu.tw/media/files/4969ffd4-31e3-4bb1-a2b8-a3618eb141ce
Node Name	https://outbound.nccu.edu.tw/media/files/4969ffd4-31e3-4bb1-a2b8-a3618eb141ce
	GET
Evidence	XSRF-TOKEN

Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/cbce4d5a-d8bc-44e4-ae22-7af2d246bb24
Node Name	https://outbound.nccu.edu.tw/media/files/cbce4d5a-d8bc-44e4-ae22-7af2d246bb24
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/ea2cfd0b-ee9b-4c9c-94fc-de20fdc3ffd8
Node Name	https://outbound.nccu.edu.tw/media/files/ea2cfd0b-ee9b-4c9c-94fc-de20fdc3ffd8
	GET
Evidence	_session
Other Info	cookie:_session
URL	https://outbound.nccu.edu.tw/media/files/ea2cfd0b-ee9b-4c9c-94fc-de20fdc3ffd8
Node Name	https://outbound.nccu.edu.tw/media/files/ea2cfd0b-ee9b-4c9c-94fc-de20fdc3ffd8
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/media/files/f353edca-d805-48ac-a6c9-9f66cf925c9e
Node Name	https://outbound.nccu.edu.tw/media/files/f353edca-d805-48ac-a6c9-9f66cf925c9e
	GET
Evidence	_session
Other Info	cookie:_session
URL	https://outbound.nccu.edu.tw/media/files/f353edca-d805-48ac-a6c9-9f66cf925c9e
Node Name	https://outbound.nccu.edu.tw/media/files/f353edca-d805-48ac-a6c9-9f66cf925c9e
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/\${data}
Node Name	https://outbound.nccu.edu.tw/page/\${data}
	GET

Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
URL	https://outbound.nccu.edu.tw/page/6
Node Name	https://outbound.nccu.edu.tw/page/6
	GET
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
Instances	50
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