ZAP Scanning Report - https://www.alumni.ntu.edu.tw

Automated report generated by OWASP ZAP Automation Framework

Site: https://www.alumni.ntu.edu.tw

Generated on Tue, 10 Nov 2026 02:38:00

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	1
Informational	6
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	Systemic
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Multiple X-Frame-Options Header Entries	Medium	Systemic
Vulnerable JS Library	Medium	1
Secure Pages Include Mixed Content	Low	1
Information Disclosure - Sensitive Information in URL	Informational	1
Information Disclosure - Suspicious Comments	Informational	7
Modern Web Application	Informational	Systemic
Re-examine Cache-control Directives	Informational	Systemic
Session Management Response Identified	Informational	12
User Controllable HTML Element Attribute (Potential XSS)	Informational	2

Alert Detail

Medium	Absence of Anti-CSRF Tokens
	No Anti-CSRF tokens were found in a HTML submission form.

Description	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	<form action="/Home/Login" autocomplete="off" data-parsley-validate="" id="frmLogin" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 3: "__X-XSRFVerificationToken" "acct" "aua8" "captcha" "showpwd"].
URL	https://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	<form action="/SiteSearch" autocomplete="off" class="d-flex searchBar" method="post" onsubmit="return checkData()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "__X-XSRFVerificationToken" "Search_keyword"].
URL	https://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	<form action="/SiteSearch" autocomplete="off" class="d-none d-flex w-100" id="searchfrm" method="post" onsubmit="return checkData()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "__X-XSRFVerificationToken" "Search_keyword"].

URL	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Node Name	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Method	GET
Attack	
Evidence	<form action="/SiteSearch" autocomplete="off" class="d-flex searchBar" method="post" onsubmit="return checkData()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "__X-XSRFVerificationToken" "Search_keyword"].
URL	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Node Name	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Method	GET
Attack	
Evidence	<form action="/SiteSearch" autocomplete="off" class="d-none d-flex w-100" id="searchfrm" method="post" onsubmit="return checkData()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "__X-XSRFVerificationToken" "Search_keyword"].
Instances	Systemic
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

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://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.alumni.ntu.edu.tw/About/About?LangCode=tw
Node Name	https://www.alumni.ntu.edu.tw/About/About (LangCode)
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000419
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000419
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation

Node Name	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
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	**Multiple X-Frame-Options Header Entries**
Description	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
URL	https://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.alumni.ntu.edu.tw/About/About?LangCode=tw
Node Name	https://www.alumni.ntu.edu.tw/About/About (LangCode)
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000403
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000403
Method	GET
Attack	
Evidence	
Other Info	

URL	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Node Name	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
Solution	Ensure only a single X-Frame-Options header is present in the response.
Reference	https://datatracker.ietf.org/doc/html/rfc7034
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Vulnerable JS Library**
Description	The identified library appears to be vulnerable.
URL	https://www.alumni.ntu.edu.tw/lib/cdnjs/select2/v3.5.0/select2.min.js
Node Name	https://www.alumni.ntu.edu.tw/lib/cdnjs/select2/v3.5.0/select2.min.js
Method	GET
Attack	
Evidence	3.5.0/select2.min.js
Other Info	The identified library select2, version 3.5.0 is vulnerable. CVE-2016-10744 https://github.com/advisories/GHSA-rf66-hmqf-q3fc https://nvd.nist.gov/vuln/detail/CVE-2016-10744 https://github.com/select2/select2/issues/4587 https://github.com/snipe/snipe-it/pull/6831/commits/5848d9a10c7d62c73ff6a3858edfae96a429402a https://github.com/snipe/snipe-it/pull/6831 https://github.com/select2/select2
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

CWE Id	1395
WASC Id	
Plugin Id	10003

Low	**Secure Pages Include Mixed Content**
Description	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.
URL	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000330
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000330
Method	GET
Attack	
Evidence	http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg
Other Info	tag=img src=http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg tag=img src=http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg tag=img src=http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg tag=img src=http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg tag=img src=http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg tag=img src=http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg tag=img src=http://www.ntuaacf.ntu.edu.tw/images/icon/bullet.jpg
Instances	1
Solution	A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
CWE Id	311
WASC Id	4
Plugin Id	10040

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	https://www.alumni.ntu.edu.tw/@25.0160195,121.5397224,17z/data=!3m1!4b1!4m5!3m4!1s0x3442abe14d93c04f:0xa1bdfa397a1ff83a!8m2!3d25.0160504!4d121.5418839?authuser=0&hl=zh-TW
Node Name	https://www.alumni.ntu.edu.tw/@25.0160195,121.5397224,17z/data=!3m1!4b1!4m5!3m4!1s0x3442abe14d93c04f:0xa1bdfa397a1ff83a!8m2!3d25.0160504!4d121.5418839 (authuser,hl)
Method	GET
Attack	
Evidence	authuser
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user

	authuser
Instances	1
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	598
WASC Id	13
Plugin Id	10024

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://www.alumni.ntu.edu.tw/Home/Register
Node Name	https://www.alumni.ntu.edu.tw/Home/Register
Method	GET
Attack	
Evidence	//$('select[name$="[' + count +
Other Info	The following pattern was used: \bSELECT\b and was detected 7 times, the first in likely comment: "//$('select[name$="[' + count + '].Year"]').on('change', function(){", see evidence field for the suspicious comment/snippet.
URL	https://www.alumni.ntu.edu.tw/lib/blockUI/jquery.blockUI.js?v=nFsCIcV22WBeVv-l4EN0pFihnx9e83C2oplm7Nu4jmo
Node Name	https://www.alumni.ntu.edu.tw/lib/blockUI/jquery.blockUI.js (v)
Method	GET
Attack	
Evidence	ress tab navigation from leaving blocking co
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// be default blockUI will supress tab navigation from leaving blocking content", see evidence field for the suspicious comment/snippet.
URL	https://www.alumni.ntu.edu.tw/lib/blockUI/jquery.blockUI.js?v=nFsCIcV22WBeVv-l4EN0pFihnx9e83C2oplm7Nu4jmo
Node Name	https://www.alumni.ntu.edu.tw/lib/blockUI/jquery.blockUI.js (v)
Method	GET
Attack	
Evidence	t back into the DOM where it started
Other Info	The following pattern was used: \bWHERE\b and was detected 2 times, the first in likely comment: "// move blocking element back into the DOM where it started", see evidence field for the suspicious comment/snippet.
URL	https://www.alumni.ntu.edu.tw/lib/daterangepicker/v3.1/daterangepicker.js?v=nCVry5qhDvfmuraDoHeq7bv91trY3tpPHnq_T3_hBOw
Node Name	https://www.alumni.ntu.edu.tw/lib/daterangepicker/v3.1/daterangepicker.js (v)
Method	GET
Attack	
Evidence	custom options from user

Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in likely comment: "//custom options from user", see evidence field for the suspicious comment /snippet.
URL	https://www.alumni.ntu.edu.tw/lib/daterangepicker/v3.1/daterangepicker.js?v=nCVry5qhDvfmuraDoHeq7bv91trY3tpPHnq_T3_hBOw
Node Name	https://www.alumni.ntu.edu.tw/lib/daterangepicker/v3.1/daterangepicker.js (v)
Method	GET
Attack	
Evidence	ute/second from the select boxes to the clicke
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "// * if the time picker is enabled, apply the hour/minute/second from the select boxes to the clicked date", see evidence field for the suspicious comment/snippet.
URL	https://www.alumni.ntu.edu.tw/lib/taiwan-id-validator2/taiwan-id-validator2.min.js
Node Name	https://www.alumni.ntu.edu.tw/lib/taiwan-id-validator2/taiwan-id-validator2.min.js
Method	GET
Attack	
Evidence	ad the output file, select a different devtool
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "/* * ATTENTION: The "eval" devtool has been used (maybe by default in mode: "development"). * This devtool is neither made for", see evidence field for the suspicious comment/snippet.
URL	https://www.alumni.ntu.edu.tw/Home/Register
Node Name	https://www.alumni.ntu.edu.tw/Home/Register ()(AlumniExtendItem.Alumnus.Birthday, AlumniExtendItem.Alumnus.CurrentAddress,AlumniExtendItem.Alumnus.CurrentCityId, AlumniExtendItem.Alumnus.CurrentCountryI...,AlumniExtendItem.Alumnus.Email, AlumniExtendItem.Alumnus.EnName,AlumniExtendItem.Alumnus.Idnumber, AlumniExtendItem.Alumnus.Mobile,AlumniExtendItem.Alumnus.Name,AlumniExtendItem. Alumnus.PermanentAddres...,AlumniExtendItem.Alumnus.PermanentCityId, AlumniExtendItem.Alumnus.PermanentCountr...,AlumniExtendItem.Alumnus.Sex, AlumniExtendItem.Alumnus.Tel,Current_AddrType,Current_CountryId_Home,IDPhoto, Permanent_AddrType,Permanent_CountryId_Home,Photo,__X-XSRFVerificationToken)
Method	POST
Attack	
Evidence	//$('select[name$="[' + count +
Other Info	The following pattern was used: \bSELECT\b and was detected 7 times, the first in likely comment: "//$('select[name$="[' + count + '].Year"]').on('change', function(){", see evidence field for the suspicious comment/snippet.
Instances	7
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://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
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	https://www.alumni.ntu.edu.tw/About/About?LangCode=en
Node Name	https://www.alumni.ntu.edu.tw/About/About (LangCode)
Method	GET
Attack	
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	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000324
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000324
Method	GET
Attack	
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	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000394
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000394
Method	GET
Attack	
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	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Node Name	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Method	GET
Attack	
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	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://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	no-cache, no-store
Other Info	
URL	https://www.alumni.ntu.edu.tw/
Node Name	https://www.alumni.ntu.edu.tw/
Method	GET
Attack	
Evidence	no-cache, no-store
Other Info	
URL	https://www.alumni.ntu.edu.tw/About/About?LangCode=tw
Node Name	https://www.alumni.ntu.edu.tw/About/About (LangCode)
Method	GET
Attack	
Evidence	no-cache, no-store
Other Info	
URL	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Method	GET
Attack	
Evidence	no-cache, no-store
Other Info	
URL	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Node Name	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Method	GET
Attack	
Evidence	no-cache, no-store
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://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Antiforgery.FHLYmWbUJH8
URL	https://www.alumni.ntu.edu.tw/About/About?LangCode=en
Node Name	https://www.alumni.ntu.edu.tw/About/About (LangCode)
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/AlumniCard
Node Name	https://www.alumni.ntu.edu.tw/AlumniCard
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/AlumniInfo
Node Name	https://www.alumni.ntu.edu.tw/AlumniInfo
Method	GET
Attack	

Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/AlumniServe/FindAlumni
Node Name	https://www.alumni.ntu.edu.tw/AlumniServe/FindAlumni
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/AlumniZone/ClassDirectory
Node Name	https://www.alumni.ntu.edu.tw/AlumniZone/ClassDirectory
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/Communicate/Submission
Node Name	https://www.alumni.ntu.edu.tw/Communicate/Submission
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Node Name	https://www.alumni.ntu.edu.tw/News/NewsDetail/NN00000413
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6 cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Node Name	https://www.alumni.ntu.edu.tw/OutstandingAlumni/SelectRegulation
Method	GET
Attack	
Evidence	TS01037fe6
Other	cookie:TS01037fe6

Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://www.alumni.ntu.edu.tw/robots.txt
Node Name	https://www.alumni.ntu.edu.tw/robots.txt
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6
URL	https://www.alumni.ntu.edu.tw/sitemap.xml
Node Name	https://www.alumni.ntu.edu.tw/sitemap.xml
Method	GET
Attack	
Evidence	TS01037fe6
Other Info	cookie:TS01037fe6
URL	https://www.alumni.ntu.edu.tw
Node Name	https://www.alumni.ntu.edu.tw
Method	GET
Attack	
Evidence	.AspNetCore.Antiforgery.FHLYmWbUJH8
Other Info	cookie:.AspNetCore.Antiforgery.FHLYmWbUJH8
Instances	12
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://www.alumni.ntu.edu.tw/About/About?LangCode=en
Node Name	https://www.alumni.ntu.edu.tw/About/About (LangCode)
Method	GET
Attack	
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: https://www.alumni.ntu.edu.tw/About/About?LangCode=en

Other Info	appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: LangCode=en The user-controlled value was: en
URL	https://www.alumni.ntu.edu.tw/SiteSearch
Node Name	https://www.alumni.ntu.edu.tw/SiteSearch ()(Search.Keyword,__X-XSRFVerificationToken)
Method	POST
Attack	
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: https://www.alumni.ntu.edu.tw/SiteSearch appears to include user input in: a(n) [input] tag [value] attribute The user input found was: Search.Keyword=ZAP The user-controlled value was: zap
Instances	2
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