ZAP by Checkmarx Scanning Report

Site: https://nouapp.nou.edu.tw

Generated on , 8 5 2026 14:15:05

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	4
Low	8
Informational	15

	Risk Level	Number of Instances
Cross Site Scripting (Reflected)	High	7
Path Traversal	High	1
Absence of Anti-CSRF Tokens	Medium	Systemic
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Sub Resource Integrity Attribute Missing	Medium	Systemic
Vulnerable JS Library	Medium	4
Application Error Disclosure	Low	1
Cookie No HttpOnly Flag	Low	3
Cookie Without Secure Flag	Low	3
Cookie without SameSite Attribute	Low	Systemic
Cross-Domain JavaScript Source File Inclusion	Low	Systemic
Information Disclosure - Debug Error Messages	Low	1
Private IP Disclosure	Low	1
Timestamp Disclosure - Unix	Low	Systemic
Authentication Request Identified	Informational	1
Information Disclosure - Sensitive Information in URL	Informational	2
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	Systemic
Re-examine Cache-control Directives	Informational	Systemic

Session Management Response Identified	Informational	53
Tech Detected - Apache HTTP Server	Informational	1
Tech Detected - Bootstrap	Informational	1
Tech Detected - Font Awesome	Informational	1
Tech Detected - Google Maps	Informational	1
Tech Detected - HSTS	Informational	1
Tech Detected - TinyMCE	Informational	1
Tech Detected - jQuery	Informational	1
Tech Detected - jQuery UI	Informational	1
User Controllable HTML Element Attribute (Potential XSS)	Informational	48

Alert Detail

High	Cross Site Scripting (Reflected)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML /JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	https://nouapp.nou.edu.tw/depkind/courses?_b=%5B%5D&discipline=06&discipline_name=%3C%2Fdiv%3E%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E%3Cdiv%3E&faculty=90&faculty_name=%E5%85%B1%E5%90%8C%E8%AA%B2%E7%A8%8B&type=1
Node Name	https://nouapp.nou.edu.tw/depkind/courses (_b,discipline,discipline_name,faculty, faculty_name,type)
	GET

	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
Other Info	
URL	https://nouapp.nou.edu.tw/depkind/courses?_b=%5B%5D&discipline=06&discipline_name=%E5%85%B6%E4%BB%96%E9%A19E&faculty=90&faculty_name=%3C%2Fdiv%3E%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E%3Cdiv%3E&type=1
Node Name	https://nouapp.nou.edu.tw/depkind/courses (_b,discipline,discipline_name,faculty,faculty_name,type)
	GET
	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
Other Info	
URL	https://nouapp.nou.edu.tw/depys/courses?_b=%5B%5D&ayear=075&ayear_name=%3C%2Fdiv%3E%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E%3Cdiv%3E&sms=1
Node Name	https://nouapp.nou.edu.tw/depys/courses (_b,ayear,ayear_name,sms)
	GET
	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
Other Info	
URL	https://nouapp.nou.edu.tw/qrybulletin/list?_b=%5B%5D&code=02&code_name=%3C%2Fp%3E%3Cimg+src%3Dx+onerror%3Dprompt%28%29%3E%3Cp%3E
Node Name	https://nouapp.nou.edu.tw/qrybulletin/list (_b,code,code_name)
	GET
	<img src=x onerror=prompt()>
Evidence	<img src=x onerror=prompt()>
Other Info	
URL	https://nouapp.nou.edu.tw/qrybulletin/view?_b=%5B%7B%22t%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22lt%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D&code=02&code_name=%22+onMouseOver%3D%22alert%281%29%3B&page=1&seq=00011382
Node Name	https://nouapp.nou.edu.tw/qrybulletin/view (_b,code,code_name,page,seq)
	GET
	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
Other Info	
URL	https://nouapp.nou.edu.tw/qrybulletin/view?_b=%5B%7B%22t%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22lt%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%

	5D&code=02&code_name=%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&page=%22+onMouseOver%3D%22alert%281%29%3B&seq=00011382
Node Name	https://nouapp.nou.edu.tw/qrybulletin/view (_b,code,code_name,page,seq)
	GET
	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
Other Info	
URL	https://nouapp.nou.edu.tw/qrynews/view?_b=%5B%5D&page=%22+onMouseOver%3D%22alert%281%29%3B&seq=00011353
Node Name	https://nouapp.nou.edu.tw/qrynews/view (_b,page,seq)
	GET
	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
Other Info	
Instances	7
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. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Phase: Implementation

	For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40012

High	**Path Traversal**
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences. The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2e%2e%2f"), and double URL encoding ("..%255c") of the backslash character. Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-supplied input. This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an executable

	script. These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NULL characters in order to bypass rudimentary file extension checks.
URL	https://nouapp.nou.edu.tw/admin/credits?section=credits
Node Name	https://nouapp.nou.edu.tw/admin/credits (section)
	GET
	credits
Evidence	
Other Info	
Instances	1
Solution	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent allow lists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses, and exclude directory separators such as "/". Use an allow list of allowable file extensions. Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters such as '.' and ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker injects a '.' inside a filename (e.g. "sensi.tiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed to be safe, then the file may be compromised. Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not decode the same input twice. Such errors could be used to bypass allow list schemes by introducing dangerous inputs after they have been checked. Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences and symbolic links. Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are only used for a single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applications rarely need to run as the database administrator, especially in day-to-day operations. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations.

	This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.
Reference	https://owasp.org/www-community/attacks/Path_Traversal https://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Plugin Id	6

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. 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://nouapp.nou.edu.tw/admin/modules
Node Name	https://nouapp.nou.edu.tw/admin/modules
	GET
Evidence	<form method="post" id="adminForm" class="overview">
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: "about[disabled]" "about[secure]" "admin[disabled]" "admin[secure]" "adminSubmit" "athletics[disabled]" "athletics[secure]" "banner[disabled]" "banner[secure]" "calendar[disabled]" "calendar[secure]" "dashboard[disabled]" "dashboard[secure]" "dining[disabled]" "dining[secure]" "emergency[disabled]" "emergency[secure]" "fullweb[disabled]" "fullweb[secure]" "home[disabled]" "home[secure]" "info[disabled]" "info[secure]" "links[disabled]" "links[secure]" "login[disabled]" "login[secure]" "map[disabled]" "map[secure]" "news[disabled]" "news[secure]" "people[disabled]" "people[secure]" "photos[disabled]" "photos[secure]" "rtcontent[disabled]" "rtcontent[secure]" "schoolsystem[disabled]" "schoolsystem[secure]" "social[disabled]" "social[secure]" "stats[disabled]" "stats[secure]" "video[disabled]" "video[secure]" "weather[disabled]" "weather[secure]"].
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET

Evidence	<form method="post" id="adminForm" enctype="multipart/form-data">
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: "adminSubmit" "section" "subsection" "type"].
URL	https://nouapp.nou.edu.tw/admin/site?section=setup
Node Name	https://nouapp.nou.edu.tw/admin/site (section)
	GET
Evidence	<form method="post" id="adminForm" enctype="multipart/form-data">
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: "adminSubmit" "section" "subsection" "type"].
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)
	POST
Evidence	<form method="post" id="adminForm" enctype="multipart/form-data">
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: "adminSubmit" "section" "subsection" "type"].
URL	https://nouapp.nou.edu.tw/admin/site?section=security
Node Name	https://nouapp.nou.edu.tw/admin/site (section)(section,submit,subsection,type)
	POST
Evidence	<form method="post" id="adminForm" enctype="multipart/form-data">
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: "adminSubmit" "section" "subsection" "type"].
Instances	Systemic
	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.

Solution	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://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET
Evidence	
Other Info	
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET

Evidence	
Other Info	
URL	https://nouapp.nou.edu.tw/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	https://nouapp.nou.edu.tw/kurogo/error (code,id,page)
	GET
Evidence	
Other Info	
URL	https://nouapp.nou.edu.tw/login/login?authority=nou
Node Name	https://nouapp.nou.edu.tw/login/login (authority)
	GET
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	**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://nouapp.nou.edu.tw/admin/credits
Node Name	https://nouapp.nou.edu.tw/admin/credits
	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/modules
Node Name	https://nouapp.nou.edu.tw/admin/modules

	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site?section=setup
Node Name	https://nouapp.nou.edu.tw/admin/site (section)
	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)
	POST
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
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

Medium	**Vulnerable JS Library**
Description	The identified library appears to be vulnerable.
URL	https://nouapp.nou.edu.tw/min/?config=admin&g=file-/common/javascript/lib/jquery-1.5.1.js
Node Name	https://nouapp.nou.edu.tw/min/ (config,g)
	GET
Evidence	* jQuery JavaScript Library v1.5.1
	The identified library jquery, version 1.5.1 is vulnerable.

Other Info	CVE-2011-4969 CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 https://bugs.jquery.com/ticket/9521 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2011-4969
URL	https://nouapp.nou.edu.tw/min/?config=admin&g=file-/common/javascript/lib/jquery-ui-1.8.11.js
Node Name	https://nouapp.nou.edu.tw/min/ (config,g)
	GET
Evidence	/* * jQuery UI 1.8.11
	The identified library jquery-ui, version 1.8.11 is vulnerable. CVE-2021-41184 CVE-2021-41183 CVE-2021-41182 CVE-2022-31160

Other Info	https://github.com/advisories/GHSA-h6gj-6jjq-h8g9 https://bugs.jqueryui.com/ticket/15284 https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9 https://nvd.nist.gov/vuln/detail/CVE-2022-31160 https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327 https://nvd.nist.gov/vuln/detail/CVE-2021-41184 https://nvd.nist.gov/vuln/detail/CVE-2021-41183 https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc https://nvd.nist.gov/vuln/detail/CVE-2021-41182 https://github.com/jquery/jquery-ui/issues/2101
URL	https://nouapp.nou.edu.tw/min/?config=admin&g=file-/common/javascript/lib/jquery-ui-1.8.24.js
Node Name	https://nouapp.nou.edu.tw/min/ (config,g)
	GET
Evidence	/* jQuery UI - v1.8.24
Other Info	The identified library jquery-ui, version 1.8.24 is vulnerable. CVE-2021-41184 CVE-2021-41183 CVE-2021-41182 CVE-2022-31160 https://github.com/advisories/GHSA-h6gj-6jjq-h8g9 https://bugs.jqueryui.com/ticket/15284 https://github.com/jquery/jquery-ui/commit/8cc5bae1caa1fcf96bf5862c5646c787020ba3f9 https://nvd.nist.gov/vuln/detail/CVE-2022-31160 https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327 https://nvd.nist.gov/vuln/detail/CVE-2021-41184 https://nvd.nist.gov/vuln/detail/CVE-2021-41183 https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc https://nvd.nist.gov/vuln/detail/CVE-2021-41182 https://github.com/jquery/jquery-ui/issues/2101
URL	https://nouapp.nou.edu.tw/min/?config=home&g=file-/common/javascript/lib/jquery-1.8.3.min.js
Node Name	https://nouapp.nou.edu.tw/min/ (config,g)
	GET

Evidence	/* jQuery v1.8.3
Other Info	The identified library jquery, version 1.8.3 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-7656 CVE-2012-6708 https://nvd.nist.gov/vuln/detail/CVE-2012-6708 https://github.com/jquery/jquery/issues/2432 http://research.insecurelabs.org/jquery/test/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://bugs.jquery.com/ticket/11974 https://github.com/jquery/jquery.com/issues/162 https://nvd.nist.gov/vuln/detail/CVE-2020-7656 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://bugs.jquery.com/ticket/11290 https://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/advisories/GHSA-q4m3-2j7h-f7xw https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Instances	4
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	**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	https://nouapp.nou.edu.tw/kurogo/error?code=internal&id=stats&page=index
Node Name	https://nouapp.nou.edu.tw/kurogo/error (code,id,page)

	GET
Evidence	HTTP/1.1 500 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	https://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	https://nouapp.nou.edu.tw/rest/
Node Name	https://nouapp.nou.edu.tw/rest/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
Instances	3
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://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	https://nouapp.nou.edu.tw/rest/
Node Name	https://nouapp.nou.edu.tw/rest/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
Instances	3
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	https://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/

	GET
Evidence	Set-Cookie: deviceClassification
Other Info	
URL	https://nouapp.nou.edu.tw/rest/
Node Name	https://nouapp.nou.edu.tw/rest/
	GET
Evidence	Set-Cookie: apiDeviceClassification
Other Info	
URL	https://nouapp.nou.edu.tw/rest/
Node Name	https://nouapp.nou.edu.tw/rest/
	GET
Evidence	Set-Cookie: e6f53a77f1692ed32baa4220d6c522e5
Other Info	
URL	https://nouapp.nou.edu.tw/robots.txt
Node Name	https://nouapp.nou.edu.tw/robots.txt
	GET
Evidence	Set-Cookie: deviceClassification
Other Info	
URL	https://nouapp.nou.edu.tw/sitemap.xml
Node Name	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/admin/credits
Node Name	https://nouapp.nou.edu.tw/admin/credits
	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/modules
Node Name	https://nouapp.nou.edu.tw/admin/modules
	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site?section=setup
Node Name	https://nouapp.nou.edu.tw/admin/site (section)
	GET
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></script>
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)
	POST
Evidence	<script src="https://html5shiv.googlecode.com/svn/trunk/html5.js"></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

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	https://nouapp.nou.edu.tw/kurogo/error?code=internal&id=stats&page=index
Node Name	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/min/?g=file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Node Name	https://nouapp.nou.edu.tw/min/ (g)
	GET
Evidence	10.1.9.34
Other Info	10.1.9.34 10.8.1.1 10.8.1.1
Instances	1
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	https://nouapp.nou.edu.tw/

Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	1729731292
Other Info	1729731292, which evaluates to: 2024-10-24 08:54:52.
URL	https://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	1778219175
Other Info	1778219175, which evaluates to: 2026-05-08 13:46:15.
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET
Evidence	1729731292
Other Info	1729731292, which evaluates to: 2024-10-24 08:54:52.
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET
Evidence	1778219175
Other Info	1778219175, which evaluates to: 2026-05-08 13:46:15.
URL	https://nouapp.nou.edu.tw/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	https://nouapp.nou.edu.tw/kurogo/error (code,id,page)
	GET
Evidence	1729731292
Other Info	1729731292, which evaluates to: 2024-10-24 08:54:52.
Instances	Systemic
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	https://nouapp.nou.edu.tw/login/login
Node Name	https://nouapp.nou.edu.tw/login/login ()(agreeTerm,anticsrf,authority,loginPassword, loginUser,startOver)
	POST
Evidence	loginPassword
Other Info	userParam=loginPassword userValue=ZAP passwordParam=loginPassword referer=https://nouapp.nou.edu.tw/login/login?authority=nou csrfToken=anticsrf
Instances	1
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	https://nouapp.nou.edu.tw/min/?g=file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Node Name	https://nouapp.nou.edu.tw/min/ (g)
	GET
Evidence	file-/common/javascript/bootstrap@5.3.3.bundle.min.js
Other Info	The URL contains email address(es).
URL	https://nouapp.nou.edu.tw/min/?g=file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Node Name	https://nouapp.nou.edu.tw/min/ (g)
	GET
Evidence	file-/common/javascript/fontawesome-free@6.6.0.all.min.js
Other Info	The URL contains email address(es).
Instances	2

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://nouapp.nou.edu.tw/min/?config=admin&g=file-/common/javascript/lib/jquery.form.js
Node Name	https://nouapp.nou.edu.tw/min/ (config,g)
	GET
Evidence	ires jQuery v1.5 or later * Copyright (c) 20
Other Info	The following pattern was used: \bLATER\b and was detected in likely comment: "/* * jQuery Form Plugin * version: 3.51.0-2014.06.20 * Requires jQuery v1.5 or later * Copyright (c) 2014 M. Alsup * Exampl", see evidence field for the suspicious comment/snippet.
Instances	1
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://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/
	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://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/login/login?authority=nou
Node Name	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/people/
Node Name	https://nouapp.nou.edu.tw/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.
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://nouapp.nou.edu.tw/

Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	max-age=0
Other Info	
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET
Evidence	max-age=0
Other Info	
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET
Evidence	max-age=0
Other Info	
URL	https://nouapp.nou.edu.tw/login/login?authority=nou
Node Name	https://nouapp.nou.edu.tw/login/login (authority)
	GET
Evidence	max-age=0
Other Info	
URL	https://nouapp.nou.edu.tw/robots.txt
Node Name	https://nouapp.nou.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://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	https://nouapp.nou.edu.tw/
Node Name	https://nouapp.nou.edu.tw/
	GET
Evidence	e6f53a77f1692ed32baa4220d6c522e5
Other Info	cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:visitID
URL	https://nouapp.nou.edu.tw/about/about
Node Name	https://nouapp.nou.edu.tw/about/about
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/credits
Node Name	https://nouapp.nou.edu.tw/admin/credits
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/credits?section=credits
Node Name	https://nouapp.nou.edu.tw/admin/credits (section)
	GET

Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/modules
Node Name	https://nouapp.nou.edu.tw/admin/modules
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/modules?module=about
Node Name	https://nouapp.nou.edu.tw/admin/modules (module)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/modules?section=overview
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/site?section=setup
Node Name	https://nouapp.nou.edu.tw/admin/site (section)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/depkind/courses?_b=%5B%5D&discipline=02&discipline_name=Other&faculty=00&faculty_name=%E6%A0%A1%E5%

	B1%AC%E8%AA%B2%E7%A8%8B&type=2
Node Name	https://nouapp.nou.edu.tw/depkind/courses (_b,discipline,discipline_name,faculty, faculty_name,type)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/depkind/index
Node Name	https://nouapp.nou.edu.tw/depkind/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/depys/courses?_b=%5B%5D&ayear=114&ayear_name=114%E5%AD%B8%E5%B9%B4%E6%9A%91%E6%9C%9F&sms=3
Node Name	https://nouapp.nou.edu.tw/depys/courses (_b,ayear,ayear_name,sms)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/depys/index
Node Name	https://nouapp.nou.edu.tw/depys/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET
Evidence	e6f53a77f1692ed32baa4220d6c522e5
Other Info	cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:visitID
URL	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET

Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/kurogo/error?args%5Bv%5D=1778219175&code=notfound&id=modules&page=home%2Fjavascript%2Findex-common.js
Node Name	https://nouapp.nou.edu.tw/kurogo/error (args[v],code,id,page)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/kurogo/error?code=notfound&id=sitemap.xml&page=index
Node Name	https://nouapp.nou.edu.tw/kurogo/error (code,id,page)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/login/login?authority=nou
Node Name	https://nouapp.nou.edu.tw/login/login (authority)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/people/
Node Name	https://nouapp.nou.edu.tw/people/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/people/group (_b,group)
	GET
Evidence	visitID

Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/preferences/
Node Name	https://nouapp.nou.edu.tw/preferences/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrybulletin/
Node Name	https://nouapp.nou.edu.tw/qrybulletin/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrybulletin/index
Node Name	https://nouapp.nou.edu.tw/qrybulletin/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrybulletin/list?_b=%5B%5D&code=02&code_name=%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
Node Name	https://nouapp.nou.edu.tw/qrybulletin/list (_b,code,code_name)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrybulletin/view?_b=%5B%7B%22t%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22lt%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D&code=02&code_name=%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&page=1&seq=00011382
Node Name	https://nouapp.nou.edu.tw/qrybulletin/view (_b,code,code_name,page,seq)
	GET
Evidence	visitID
Other	

Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrycalendar/
Node Name	https://nouapp.nou.edu.tw/qrycalendar/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrycontact/
Node Name	https://nouapp.nou.edu.tw/qrycontact/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrycourse/index
Node Name	https://nouapp.nou.edu.tw/qrycourse/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrycourse/index?filter=ZAP
Node Name	https://nouapp.nou.edu.tw/qrycourse/index (filter)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrynews/
Node Name	https://nouapp.nou.edu.tw/qrynews/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrynews/index?page=1
Node Name	https://nouapp.nou.edu.tw/qrynews/index (page)
	GET

Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qrynews/view?_b=%5B%5D&page=1&seq=00011353
Node Name	https://nouapp.nou.edu.tw/qrynews/view (_b,page,seq)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qryrecruit/
Node Name	https://nouapp.nou.edu.tw/qryrecruit/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qryroadmap/
Node Name	https://nouapp.nou.edu.tw/qryroadmap/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qryroadmap/index
Node Name	https://nouapp.nou.edu.tw/qryroadmap/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qryroadmap/view?_b=%5B%5D&code=000
Node Name	https://nouapp.nou.edu.tw/qryroadmap/view (_b,code)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qryschoolmap/

Node Name	https://nouapp.nou.edu.tw/qryschoolmap/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qryschoolmap/index
Node Name	https://nouapp.nou.edu.tw/qryschoolmap/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/qryschoolmap/view?_b=%5B%5D&code=000
Node Name	https://nouapp.nou.edu.tw/qryschoolmap/view (_b,code)
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/rest/
Node Name	https://nouapp.nou.edu.tw/rest/
	GET
Evidence	e6f53a77f1692ed32baa4220d6c522e5
Other Info	cookie:e6f53a77f1692ed32baa4220d6c522e5 cookie:apiDeviceClassification
URL	https://nouapp.nou.edu.tw/rest/login/session
Node Name	https://nouapp.nou.edu.tw/rest/login/session
	GET
Evidence	visitID
Other Info	cookie:visitID json:response.token cookie:apiDeviceClassification
URL	https://nouapp.nou.edu.tw/robots.txt
Node Name	https://nouapp.nou.edu.tw/robots.txt
	GET

Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	https://nouapp.nou.edu.tw/schoolsystem/
Node Name	https://nouapp.nou.edu.tw/schoolsystem/
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/schoolsystem/index
Node Name	https://nouapp.nou.edu.tw/schoolsystem/index
	GET
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/sitemap.xml
Node Name	https://nouapp.nou.edu.tw/sitemap.xml
	GET
Evidence	deviceClassification
Other Info	cookie:deviceClassification
URL	https://nouapp.nou.edu.tw/admin/modules
Node Name	https://nouapp.nou.edu.tw/admin/modules ()(about[disabled],about[secure],admin[disabled],admin[secure],athletics[disabled],athletics[secure],banner[disabled],banner[secure],calendar[disabled],calendar[secure],dashboard[disabled],dashboard[secure],dining[disabled],dining[secure],emergency[disabled],emergency[secure],fullweb[disabled],fullweb[secure],home[disabled],home[secure],info[disabled],info[secure],links[disabled],links[secure],login[disabled],login[secure],map[disabled],map[secure],news[disabled],news[secure],people[disabled],people[secure],photos[disabled],photos[secure],rtcontent[disabled],rtcontent[secure],schoolsystem[disabled],schoolsystem[secure],social[disabled],social[secure],stats[disabled],stats[secure],video[disabled],video[secure],weather[disabled],weather[secure])
	POST
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/modules?module=dining
Node Name	https://nouapp.nou.edu.tw/admin/modules (module)
	POST

Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar,dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent,schoolsystem,social,stats,video,weather)
	POST
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/modules?section=overview
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about[disabled],about[secure],admin[disabled],admin[secure],athletics[disabled],athletics[secure],banner[disabled],banner[secure],calendar[disabled],calendar[secure],dashboard[disabled],dashboard[secure],dining[disabled],dining[secure],emergency[disabled],emergency[secure],fullweb[disabled],fullweb[secure],home[disabled],home[secure],info[disabled],info[secure],links[disabled],links[secure],login[disabled],login[secure],map[disabled],map[secure],news[disabled],news[secure],people[disabled],people[secure],photos[disabled],photos[secure],rtcontent[disabled],rtcontent[secure],schoolsystem[disabled],schoolsystem[secure],social[disabled],social[secure],stats[disabled],stats[secure],video[disabled],video[secure],weather[disabled],weather[secure])
	POST
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)
	POST
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/admin/site?section=security
Node Name	https://nouapp.nou.edu.tw/admin/site (section)(section,submit,subsection,type)
	POST
Evidence	visitID
Other Info	cookie:visitID
URL	https://nouapp.nou.edu.tw/login/login
Node Name	https://nouapp.nou.edu.tw/login/login ()(agreeTerm,anticsrf,authority,loginPassword,loginUser,startOver)
	POST

Evidence	visitID
Other Info	cookie:visitID
Instances	53
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	https://nouapp.nou.edu.tw/sitemap.xml
Node Name	https://nouapp.nou.edu.tw/sitemap.xml
	GET
Evidence	Apache
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*
Instances	1
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	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/home/
	GET
Evidence	<link href="/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	1
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	https://nouapp.nou.edu.tw/home/
Node Name	https://nouapp.nou.edu.tw/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	1
Solution	
Reference	https://fontawesome.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	https://nouapp.nou.edu.tw/qryschoolmap/view?_b=%5B%5D&code=011
Node Name	https://nouapp.nou.edu.tw/qryschoolmap/view (_b,code)
	GET
Evidence	//maps.googleapis.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	https://nouapp.nou.edu.tw/sitemap.xml
Node Name	https://nouapp.nou.edu.tw/sitemap.xml
	GET
Evidence	Strict-Transport-Security
Other Info	
Instances	1
Solution	
Reference	https://www.rfc-editor.org/rfc/rfc6797#section-6.1
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - TinyMCE
Description	The following "Rich text editors" technology was identified: TinyMCE. Described as: TinyMCE is an online rich-text editor released as open-source software. TinyMCE is designed to integrate with JavaScript libraries, Vue.js, and AngularJS as well as content management systems such as Joomla!, and WordPress.
URL	https://nouapp.nou.edu.tw/admin/credits
Node Name	https://nouapp.nou.edu.tw/admin/credits
	GET
Evidence	/tinymce.min.js
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:tiny:tinymce:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://www.tiny.cloud/tinymce/
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - jQuery
	The following "JavaScript libraries" technology was identified: jQuery.

Description	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	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET
Evidence	/jquery-1.5.1.
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: 1.5.1
Instances	1
Solution	
Reference	https://jquery.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - jQuery UI**
Description	The following "JavaScript libraries" technology was identified: jQuery UI. Described as: jQuery UI is a collection of GUI widgets, animated visual effects, and themes implemented with jQuery, Cascading Style Sheets, and HTML.
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site
	GET
Evidence	jquery-ui-1.8.11.js
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:jquery:jquery_ui:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 1.8.11
Instances	1
Solution	
Reference	https://jqueryui.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	https://nouapp.nou.edu.tw/admin/credits?section=credits

Node Name	https://nouapp.nou.edu.tw/admin/credits (section)
	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: https://nouapp.nou.edu.tw/admin/credits?section=credits appears to include user input in: a(n) [a] tag [section] attribute The user input found was: section=credits The user-controlled value was: credits
URL	https://nouapp.nou.edu.tw/admin/modules?module=about
Node Name	https://nouapp.nou.edu.tw/admin/modules (module)
	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: https://nouapp.nou.edu.tw/admin/modules?module=about appears to include user input in: a(n) [a] tag [section] attribute The user input found was: module=about The user-controlled value was: about
URL	https://nouapp.nou.edu.tw/admin/modules?section=overview
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)
	GET
Evidence	
Other	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://nouapp.nou.edu.tw/admin/modules?section=overview appears to include user input in: a(n) [a] tag [section] attribute

Info	The user input found was: section=overview The user-controlled value was: overview
URL	https://nouapp.nou.edu.tw/admin/site?section=setup
Node Name	https://nouapp.nou.edu.tw/admin/site (section)
	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: https://nouapp.nou.edu.tw/admin/site?section=setup appears to include user input in: a(n) [a] tag [section] attribute The user input found was: section=setup The user-controlled value was: setup
URL	https://nouapp.nou.edu.tw/depkind/courses?_b=%5B%5D&discipline=1&discipline_name=%E6%A0%A1%E5%B1%AC%E9%A1%9E&faculty=00&faculty_name=%E6%A0%A1%E5%B1%AC%E8%AA%B2%E7%A8%8B&type=1
Node Name	https://nouapp.nou.edu.tw/depkind/courses (_b,discipline,discipline_name,faculty, faculty_name,type)
	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: https://nouapp.nou.edu.tw/depkind/courses?_b=%5B%5D&discipline=1&discipline_name=%E6%A0%A1%E5%B1%AC%E9%A1%9E&faculty=00&faculty_name=%E6%A0%A1%E5%B1%AC%E8%AA%B2%E7%A8%8B&type=1 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: discipline=1 The user-controlled value was: ie=edge,chrome=1
URL	https://nouapp.nou.edu.tw/depkind/courses?_b=%5B%5D&discipline=03&discipline_name=%E5%AE%97%E6%95%99%E8%88%87%E5%93%B2%E5%AD%B8%E9%A1%9E&faculty=10&faculty_name=%E4%BA%BA%E6%96%87%E5%AD%B8%E7%B3%BB&type=1

Node Name	https://nouapp.nou.edu.tw/depkind/courses (_b,discipline,discipline_name,faculty, faculty_name,type)
	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: https://nouapp.nou.edu.tw/depkind/courses?_b=%5B%5D&discipline=03&discipline_name=%E5%AE%97%E6%95%99%E8%88%87%E5%93%B2%E5%AD%B8%E9%A1%9E&faculty=10&faculty_name=%E4%BA%BA%E6%96%87%E5%AD%B8%E7%B3%BB&type=1 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: type=1 The user-controlled value was: ie=edge,chrome=1
URL	https://nouapp.nou.edu.tw/depys/courses?_b=%5B%5D&ayear=114&ayear_name=114%E5%AD%B8%E5%B9%B4%E4%B8%8A%E5%AD%B8%E6%9C%9F&sms=1
Node Name	https://nouapp.nou.edu.tw/depys/courses (_b,ayear,ayear_name,sms)
	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: https://nouapp.nou.edu.tw/depys/courses?_b=%5B%5D&ayear=114&ayear_name=114%E5%AD%B8%E5%B9%B4%E4%B8%8A%E5%AD%B8%E6%9C%9F&sms=1 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: sms=1 The user-controlled value was: ie=edge,chrome=1
URL	https://nouapp.nou.edu.tw/login/login?authority=nou
Node Name	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/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	https://nouapp.nou.edu.tw/qrybulletin/view?_b=%5B%7B%22t%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22lt%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D&code=02&code_name=%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&page=1&seq=00011382
Node Name	https://nouapp.nou.edu.tw/qrybulletin/view (_b,code,code_name,page,seq)
	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: https://nouapp.nou.edu.tw/qrybulletin/view?_b=%5B%7B%22t%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22lt%22%3A%22%5Cu516c%5Cu4f48%5Cu6b04%22%2C%22p%22%3A%22index%22%2C%22a%22%3A%22%22%7D%5D&code=02&code_name=%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&page=1&seq=00011382 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: page=1 The user-controlled value was: ie=edge,chrome=1
URL	https://nouapp.nou.edu.tw/qrycourse/index?filter=ZAP
Node Name	https://nouapp.nou.edu.tw/qrycourse/index (filter)
	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: https://nouapp.nou.edu.tw/qrycourse/index?filter=ZAP appears to include user input in: a(n) [input] tag [value] attribute

	The user input found was: filter=ZAP The user-controlled value was: zap
URL	https://nouapp.nou.edu.tw/qrynews/index?page=1
Node Name	https://nouapp.nou.edu.tw/qrynews/index (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: https://nouapp.nou.edu.tw/qrynews/index?page=1 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: page=1 The user-controlled value was: ie=edge,chrome=1
URL	https://nouapp.nou.edu.tw/qrynews/view?_b=%5B%5D&page=1&seq=00011353
Node Name	https://nouapp.nou.edu.tw/qrynews/view (_b,page,seq)
	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: https://nouapp.nou.edu.tw/qrynews/view?_b=%5B%5D&page=1&seq=00011353 appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: page=1 The user-controlled value was: ie=edge,chrome=1
URL	https://nouapp.nou.edu.tw/qryschoolmap/view?_b=%5B%5D&code=all
Node Name	https://nouapp.nou.edu.tw/qryschoolmap/view (_b,code)
	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: https://nouapp.nou.edu.tw/qryschoolmap/view?_b=%5B%5D&code=all appears to include user input in: a(n) [link] tag [media] attribute The user input found was: code=all The user-controlled value was: all
URL	https://nouapp.nou.edu.tw/admin/modules?module=dining
Node Name	https://nouapp.nou.edu.tw/admin/modules (module)
	POST
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://nouapp.nou.edu.tw/admin/modules?module=dining appears to include user input in: a(n) [a] tag [section] attribute The user input found was: module=dining The user-controlled value was: dining
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: about= The user-controlled value was:

URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: admin= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: athletics= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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	https://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: banner= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: calendar= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: dashboard= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen

Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: dining= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: emergency=Emergency Info The user-controlled value was: emergency info
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen

Other Info	appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: fullweb= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: info= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: links= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar,

Name	dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: login= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: map= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in:

Other Info	a(n) [img] tag [alt] attribute The user input found was: news= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: people= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: photos= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)

	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: rtcontent= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: schoolsystem= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [a] tag [section] attribute

	The user input found was: section=homescreen The user-controlled value was: homescreen
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: social= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: stats= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST

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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: video= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=homescreen
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about,admin,athletics,banner,calendar, dashboard,dining,emergency,fullweb,info,links,login,map,news,people,photos,rtcontent, schoolsystem,social,stats,video,weather)
	POST
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://nouapp.nou.edu.tw/admin/modules?section=homescreen appears to include user input in: a(n) [img] tag [alt] attribute The user input found was: weather= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/modules?section=overview
Node Name	https://nouapp.nou.edu.tw/admin/modules (section)(about[disabled],about[secure],admin [disabled],admin[secure],athletics[disabled],athletics[secure],banner[disabled],banner [secure],calendar[disabled],calendar[secure],dashboard[disabled],dashboard[secure],dining [disabled],dining[secure],emergency[disabled],emergency[secure],fullweb[disabled],fullweb [secure],home[disabled],home[secure],info[disabled],info[secure],links[disabled],links [secure],login[disabled],login[secure],map[disabled],map[secure],news[disabled],news [secure],people[disabled],people[secure],photos[disabled],photos[secure],rtcontent [disabled],rtcontent[secure],schoolsystem[disabled],schoolsystem[secure],social[disabled], social[secure],stats[disabled],stats[secure],video[disabled],video[secure],weather[disabled], weather[secure])
	POST
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://nouapp.nou.edu.tw/admin/modules?section=overview

Other Info	appears to include user input in: a(n) [a] tag [section] attribute The user input found was: section=overview The user-controlled value was: overview
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)
	POST
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://nouapp.nou.edu.tw/admin/site appears to include user input in: a(n) [a] tag [section] attribute The user input found was: section=setup The user-controlled value was: setup
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)
	POST
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://nouapp.nou.edu.tw/admin/site appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)

	POST
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://nouapp.nou.edu.tw/admin/site appears to include user input in: a(n) [input] tag [value] attribute The user input found was: subsection= / The user-controlled value was: /
URL	https://nouapp.nou.edu.tw/admin/site
Node Name	https://nouapp.nou.edu.tw/admin/site ()(section,submit,subsection,type)
	POST
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://nouapp.nou.edu.tw/admin/site appears to include user input in: a(n) [span] tag [id] attribute The user input found was: type=site The user-controlled value was: sitename
URL	https://nouapp.nou.edu.tw/admin/site?section=security
Node Name	https://nouapp.nou.edu.tw/admin/site (section)(section,submit,subsection,type)
	POST
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://nouapp.nou.edu.tw/admin/site?section=security appears to include user input in: a(n) [a] tag [section] attribute The user input found was:

	section=security The user-controlled value was: security
URL	https://nouapp.nou.edu.tw/admin/site?section=security
Node Name	https://nouapp.nou.edu.tw/admin/site (section)(section,submit,subsection,type)
	POST
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://nouapp.nou.edu.tw/admin/site?section=security appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit= The user-controlled value was:
URL	https://nouapp.nou.edu.tw/admin/site?section=security
Node Name	https://nouapp.nou.edu.tw/admin/site (section)(section,submit,subsection,type)
	POST
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://nouapp.nou.edu.tw/admin/site?section=security appears to include user input in: a(n) [input] tag [value] attribute The user input found was: subsection= / The user-controlled value was: /
URL	https://nouapp.nou.edu.tw/admin/site?section=security
Node Name	https://nouapp.nou.edu.tw/admin/site (section)(section,submit,subsection,type)
	POST
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://nouapp.nou.edu.tw/admin/site?section=security appears to include user input in: a(n) [span] tag [id] attribute The user input found was: type=site The user-controlled value was: sitename
URL	https://nouapp.nou.edu.tw/login/login
Node Name	https://nouapp.nou.edu.tw/login/login ()(agreeTerm,anticsrf,authority,loginPassword, loginUser,startOver)
	POST
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://nouapp.nou.edu.tw/login/login 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	https://nouapp.nou.edu.tw/login/login
Node Name	https://nouapp.nou.edu.tw/login/login ()(agreeTerm,anticsrf,authority,loginPassword, loginUser,startOver)
	POST
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://nouapp.nou.edu.tw/login/login 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

Instances	48
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