ZAP by Checkmarx Scanning Report

Site: http://tmuapp.tmu.edu.tw:8080

Generated on , 10 4 2026 15:49:59

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	2
Informational	6

	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	1
Vulnerable JS Library	Medium	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	Systemic
X-Content-Type-Options Header Missing	Low	Systemic
Information Disclosure - Suspicious Comments	Informational	12
Modern Web Application	Informational	1
Tech Detected - Bootstrap	Informational	1
Tech Detected - Kestrel	Informational	1
Tech Detected - Microsoft ASP.NET	Informational	1
Tech Detected - jQuery	Informational	1

Alert Detail

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	http://tmuapp.tmu.edu.tw:8080/
Node Name	http://tmuapp.tmu.edu.tw:8080/
	GET
Evidence	
Other Info	
Instances	1
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	**Vulnerable JS Library**
Description	The identified library appears to be vulnerable.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	* jQuery JavaScript Library v3.3.1
Other Info	The identified library jquery, version 3.3.1 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2019-11358 https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	1395
WASC Id	
Plugin Id	10003

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://tmuapp.tmu.edu.tw:8080/
Node Name	http://tmuapp.tmu.edu.tw:8080/
	GET
Evidence	X-Powered-By: ASP.NET
Other Info	
URL	http://tmuapp.tmu.edu.tw:8080/css/home_icon.css
Node Name	http://tmuapp.tmu.edu.tw:8080/css/home_icon.css
	GET
Evidence	X-Powered-By: ASP.NET
Other Info	
URL	http://tmuapp.tmu.edu.tw:8080/css/site.css
Node Name	http://tmuapp.tmu.edu.tw:8080/css/site.css
	GET
Evidence	X-Powered-By: ASP.NET
Other Info	
URL	http://tmuapp.tmu.edu.tw:8080/robots.txt
Node Name	http://tmuapp.tmu.edu.tw:8080/robots.txt
	GET
Evidence	X-Powered-By: ASP.NET
Other Info	
URL	http://tmuapp.tmu.edu.tw:8080/sitemap.xml
Node Name	http://tmuapp.tmu.edu.tw:8080/sitemap.xml
	GET
Evidence	X-Powered-By: ASP.NET
Other Info	
Instances	Systemic

Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10037

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://tmuapp.tmu.edu.tw:8080/
Node Name	http://tmuapp.tmu.edu.tw:8080/
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://tmuapp.tmu.edu.tw:8080/css/home_icon.css
Node Name	http://tmuapp.tmu.edu.tw:8080/css/home_icon.css
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://tmuapp.tmu.edu.tw:8080/css/site.css
Node Name	http://tmuapp.tmu.edu.tw:8080/css/site.css
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://tmuapp.tmu.edu.tw:8080/fontawsome/css/solid.css
Node	

Name	http://tmuapp.tmu.edu.tw:8080/fontawsome/css/solid.css
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://tmuapp.tmu.edu.tw:8080/js/site.js?v=4q1jwFhaPaZgr8WAUSrux6hAuh0XDg9kPS3xIVq36I0
Node Name	http://tmuapp.tmu.edu.tw:8080/js/site.js (v)
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	Systemic
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://tmuapp.tmu.edu.tw:8080/lib/bootstrap/dist/js/bootstrap.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/bootstrap/dist/js/bootstrap.js
	GET
Evidence	stop cycling until user tapped out of it;
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "// would stop cycling until user tapped out of it;", see evidence field for the suspicious comment /snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/bootstrap/dist/js/bootstrap.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/bootstrap/dist/js/bootstrap.js
	GET

Evidence	// TODO: Remove in v5
Other Info	The following pattern was used: \bTODO\b and was detected 3 times, the first in likely comment: "// TODO: Remove in v5", see evidence field for the suspicious comment/snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	dataType: null, username: null, password:
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "/* timeout: 0, data: null, dataType: null, username: null, password: null, cache: null, throws: false, t", see evidence field for the suspicious comment/snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	be adjusted by the user
Other Info	The following pattern was used: \bUSER\b and was detected 9 times, the first in likely comment: "// Can be adjusted by the user", see evidence field for the suspicious comment /snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	// See https://bugs.jquery.com/ticket/1
Other Info	The following pattern was used: \bBUGS\b and was detected 7 times, the first in likely comment: "// See https://bugs.jquery.com/ticket/13378", see evidence field for the suspicious comment/snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	// TODO: identify versions

Other Info	The following pattern was used: \bTODO\b and was detected 4 times, the first in likely comment: "// TODO: identify versions", see evidence field for the suspicious comment /snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	// want to query the value if it is
Other Info	The following pattern was used: \bQUERY\b and was detected 2 times, the first in likely comment: "// want to query the value if it is a CSS custom property", see evidence field for the suspicious comment/snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	S-like environments where a proper `window`
Other Info	The following pattern was used: \bWHERE\b and was detected 9 times, the first in likely comment: "// For CommonJS and CommonJS-like environments where a proper `window`", see evidence field for the suspicious comment/snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	or POS matching in `select`
Other Info	The following pattern was used: \bSELECT\b and was detected 3 times, the first in likely comment: "// We use this for POS matching in `select`", see evidence field for the suspicious comment/snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	re and will not see later tests
Other Info	The following pattern was used: \bLATER\b and was detected 8 times, the first in likely comment: "// IE8 throws error here and will not see later tests", see evidence field for the suspicious comment/snippet.
URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	ust the one element from the set
Other Info	The following pattern was used: \bFROM\b and was detected 47 times, the first in likely comment: "// Return just the one element from the set", see evidence field for the suspicious comment/snippet.

URL	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
Node Name	http://tmuapp.tmu.edu.tw:8080/lib/jquery/dist/jquery.js
	GET
Evidence	w this because of a bug in IE8/9 that throw
Other Info	The following pattern was used: \bBUG\b and was detected 7 times, the first in likely comment: "// We allow this because of a bug in IE8/9 that throws an error", see evidence field for the suspicious comment/snippet.
Instances	12
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	http://tmuapp.tmu.edu.tw:8080/
Node Name	http://tmuapp.tmu.edu.tw:8080/
	GET
Evidence	<script src="/lib/jquery/dist/jquery.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Tech Detected - Bootstrap**
Description	The following "UI frameworks" technology was identified: Bootstrap. Described as: Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components.
URL	http://tmuapp.tmu.edu.tw:8080/
Node Name	http://tmuapp.tmu.edu.tw:8080/
	GET
Evidence	<link href="/lib/bootstrap/dist/css/bootstrap.css

Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Kestrel**
Description	The following "Web servers" technology was identified: Kestrel.
URL	http://tmuapp.tmu.edu.tw:8080/sitemap.xml
Node Name	http://tmuapp.tmu.edu.tw:8080/sitemap.xml
	GET
Evidence	Kestrel
Other Info	
Instances	1
Solution	
Reference	https://docs.microsoft.com/en-us/aspnet/core/fundamentals/servers/kestrel
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Microsoft ASP.NET**
Description	The following "Web frameworks" technology was identified: Microsoft ASP.NET. Described as: ASP.NET is an open-source, server-side web-application framework designed for web development to produce dynamic web pages.
URL	http://tmuapp.tmu.edu.tw:8080/sitemap.xml
Node Name	http://tmuapp.tmu.edu.tw:8080/sitemap.xml
	GET
Evidence	ASP.NET
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:microsoft:asp.net:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://www.asp.net
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - jQuery
Description	The following "JavaScript libraries" technology was identified: jQuery. Described as: jQuery is a JavaScript library which is a free, open-source software designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax.
URL	http://tmuapp.tmu.edu.tw:8080/
Node Name	http://tmuapp.tmu.edu.tw:8080/
	GET
Evidence	jquery
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://jquery.com
CWE Id	
WASC Id	13
Plugin Id	10004