JMTO-EPROC ZAP VAT KINTEK TEAM

Site: https://jmto-eproc.kintekindo.net

Generated on Mon, 4 Sep 2023 09:19:28

ZAP Version: 2.13.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	2
Informational	3

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	3
Content Security Policy (CSP) Header Not Set	Medium	3
Cookie No HttpOnly Flag	Low	5
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	15
Information Disclosure - Suspicious Comments	Informational	6
Modern Web Application	Informational	2
Session Management Response Identified	Informational	8

Alert Detail

Medium	CSP: Wildcard Directive
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	default-src 'self';style-src 'self';script-src 'self' 'nonce-NjRmNTNlYTVlZjlhYQ==';img-src 'self'; frame-src 'self' https://www.google.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	default-src 'self';style-src 'self';script-src 'self' 'nonce-NjRmNTNlYTUzY2Q4Yg==';img-src 'self';frame-src 'self' https://www.google.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	default-src 'self';style-src 'self';script-src 'self' 'nonce-NjRmNTNlYTVmMjRjYQ==';img-src 'self';frame-src 'self' https://www.google.com
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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://jmto-eproc.kintekindo.net/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmto-eproc.kintekindo.net/robots.txt
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://jmto-eproc.kintekindo.net/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
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/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

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://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
URL	https://jmto-eproc.kintekindo.net/index.html
Method	GET
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
URL	https://jmto-eproc.kintekindo.net/robots.txt
Method	GET

Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
URL	https://jmto-eproc.kintekindo.net/sitemap.xml
Method	GET
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
Instances	5
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	**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	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/wa_logo.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/plugins-lte/datatables/jquery.dataTables.min.js
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	

URL	https://jmto-eproc.kintekindo.net/assets_landing/bootstrap.min.css
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets_landing/dataTables.bootstrap4.min.css
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets_landing/foto_navbar.jpeg
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets_landing/jarallax-video.min.js
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets_landing/jarallax.min.js
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets_landing/jquery.min.js
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets_landing/sticky.css
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets_landing/style.css

Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/index.html
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/robots.txt
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/sitemap.xml
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
Instances	15
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://jmto-eproc.kintekindo.net/assets/plugins-lte/datatables/jquery.dataTables.min.js
Method	GET
Attack	
Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected 7 times, the first in the element starting with: "0;for(h=d.length;n<h;n++){var p=0;for(f=c.length;p<f;p++){m[p]===q&&(m[p]=T(a,p,g,"type"));var t=d[n](m[p],a);if(!t&&n!==d.lengt", see evidence field for the suspicious comment/snippet.
URL	https://jmto-eproc.kintekindo.net/assets/plugins-lte/datatables/jquery.dataTables.min.js
Method	GET

Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "fnStateSaveParams:null,iStateDuration:7200,iDeferLoading:null,iDisplayLength:10, iDisplayStart:0,iTabIndex:0,oClasses:{},oLanguag", see evidence field for the suspicious comment/snippet.
URL	https://jmto-eproc.kintekindo.net/assets/plugins-lte/datatables/jquery.dataTables.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "200)}function Pa(a,b){a._bInitComplete=!0;(b||a.oInit.aaData)&&ta(a); F(a,null,"plugin-init",[a,b]);F(a,"aoInitComplete","init",[", see evidence field for the suspicious comment/snippet.
URL	https://jmto-eproc.kintekindo.net/assets/plugins-lte/datatables/jquery.dataTables.min.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "R(r,"aoDrawCallback",g.fnDrawCallback,"user");R(r," aoServerParams",g.fnServerParams,"user");R(r,"aoStateSaveParams",g.fnStateSav", see evidence field for the suspicious comment/snippet.
URL	https://jmto-eproc.kintekindo.net/assets_landing/jquery.min.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 2 times, the first in the element starting with: "a.removeEventListener("load",R),r.ready()}"complete"===d.readyState||" loading"!==d.readyState&&!d.documentElement.doScroll?a.set", see evidence field for the suspicious comment/snippet.
URL	https://jmto-eproc.kintekindo.net/assets_landing/jquery.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=a.document?b(a,!0):function(", see evidence field for the suspicious comment/snippet.
Instances	6
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[200](200)
WASC Id	13
Plugin Id	[10027](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://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<a class="nav-link dropdown-toggle btn btn-dark text-black d-lg-flex d-none" href="#" role="button" data-toggle="dropdown" aria-haspopup="true" aria-expanded="false"><i>LOGIN</i><i class="fa fa-chevron-down"></i> </a>
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://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<a class="nav-link dropdown-toggle btn btn-dark text-black d-lg-flex d-none" href="#" role="button" data-toggle="dropdown" aria-haspopup="true" aria-expanded="false"><i>LOGIN</i><i class="fa fa-chevron-down"></i> </a>
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	2
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	03f194d74d4959c5a3954b6ad902d42b17be4645
Other Info	cookie:ci_session cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	423c83c5336ea40b98773737e8a75f6d3bc13d85
Other Info	cookie:ci_session cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	94109406809df2e65b8cda3ab2b88f335a761973
Other Info	cookie:ci_session cookie:csrf_cookie

URL	https://jmto-eproc.kintekindo.net/index.html
Method	GET
Attack	
Evidence	5dcc33730ae20986c778bbe4c4cd24bb
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/robots.txt
Method	GET
Attack	
Evidence	5dcc33730ae20986c778bbe4c4cd24bb
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/sitemap.xml
Method	GET
Attack	
Evidence	6fbf157079b31fa84279338468e083e1
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	423c83c5336ea40b98773737e8a75f6d3bc13d85
Other Info	cookie:ci_session
URL	https://jmto-eproc.kintekindo.net/index.html
Method	GET
Attack	
Evidence	5dcc33730ae20986c778bbe4c4cd24bb
Other Info	cookie:csrf_cookie
Instances	8
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