ZAP Scanning JMTO KINTEK baru

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

Generated on Fri, 1 Sep 2023 14:35:17

ZAP Version: 2.13.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	3
Informational	4

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	2
CSP: script-src unsafe-inline	Medium	2
CSP: style-src unsafe-inline	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	9
Cookie No HttpOnly Flag	Low	11
Cross-Domain JavaScript Source File Inclusion	Low	36
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	23
Authentication Request Identified	Informational	2
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	2
Session Management Response Identified	Informational	20

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	img-src 'self' *
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, prefetch-src, 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	img-src 'self' *
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, prefetch-src, 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	2
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	**CSP: script-src unsafe-inline**
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	img-src 'self' *
Other Info	script-src includes unsafe-inline.
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	img-src 'self' *
Other Info	script-src includes unsafe-inline.
Instances	2
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	CSP: style-src unsafe-inline
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	img-src 'self' *
Other Info	style-src includes unsafe-inline.
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	img-src 'self' *
Other Info	style-src includes unsafe-inline.
Instances	2
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/about-us.html

Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmto-eproc.kintekindo.net/auth
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmto-eproc.kintekindo.net/course.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmto-eproc.kintekindo.net/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmto-eproc.kintekindo.net/pricing.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmto-eproc.kintekindo.net/privacy-policy.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	
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	
Other Info	
Instances	9
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/about-us.html
Method	GET
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	

URL	https://jmto-eproc.kintekindo.net/auth
Method	GET
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
URL	https://jmto-eproc.kintekindo.net/course.html
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/pricing.html
Method	GET
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
URL	https://jmto-eproc.kintekindo.net/privacy-policy.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	
URL	https://jmto-eproc.kintekindo.net/auth

Method	POST
Attack	
Evidence	set-cookie: csrf_cookie
Other Info	
Instances	11
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	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/dataTables.bootstrap4.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.1.1/jquery.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/bootstrap/bootstrap.min.js"></script>
Other Info	

URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/counter/jquery.countTo.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/custom.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax-video.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jquery.appear.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/magnific-popup/jquery.magnific-popup.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/owl-carousel/owl.

Evidence	carousel.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/popper/popper.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/shuffle/shuffle.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiper/swiper.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiperanimation/SwiperAnimation.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/dataTables.bootstrap4.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	

Evidence	<script src="https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.1.1/jquery.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/bootstrap/bootstrap.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/counter/jquery.countTo.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/custom.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax-video.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET

Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jquery.appear.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/magnific-popup/jquery.magnific-popup.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/owl-carousel/owl.carousel.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/popper/popper.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/shuffle/shuffle.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiper/swiper.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiperanimation/SwiperAnimation.min.js"></script>
Other Info	

URL	https://jmto-eproc.kintekindo.net/auth
Method	GET
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/auth
Method	GET
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=onload&hl=en" async defer></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
Other Info	
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=onload&hl=en" async defer></script>
Other Info	
Instances	36
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	**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/about-us.html
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/gardu.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/gerbang.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/jalan.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/jmto_logo.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/logo3.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/monitoring.png
Method	GET
Attack	

Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/proc.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/ruastol.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/support.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/assets/img/volume_logo.png
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/auth
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster

Other Info	
URL	https://jmto-eproc.kintekindo.net/course.html
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/pricing.html
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmto-eproc.kintekindo.net/privacy-policy.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	
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	

Instances	23
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	**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://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	password
Other Info	userParam=userName userValue=ZAP passwordParam=password referer=https://jmto-eproc.kintekindo.net/auth
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	password
Other Info	userParam=userName userValue=ZAP passwordParam=password referer=https://jmto-eproc.kintekindo.net/auth csrfToken=csrf_token
Instances	2
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 - 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.
Instances	4
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
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://jmto-eproc.kintekindo.net
Method	GET
Attack	
Evidence	LOGIN< /i>
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	LOGIN< /i>
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	24f4313dca2f3223ed8bb45c2d91f51ea1d98ef4
Other Info	cookie:ci_session cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	00fb4a89b4477bd8d84857278604eed320a90a6c
Other Info	cookie:ci_session cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	ece216d42015a7c7840ddc92d3e9d2cf401a9991
Other Info	cookie:ci_session cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/about-us.html
Method	GET
Attack	
Evidence	4683ecfd2429d796554b74dc26ee5c68
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	GET
Attack	
Evidence	4683ecfd2429d796554b74dc26ee5c68
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/course.html
Method	GET
Attack	

Evidence	4683ecfd2429d796554b74dc26ee5c68
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/index.html
Method	GET
Attack	
Evidence	4683ecfd2429d796554b74dc26ee5c68
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/pricing.html
Method	GET
Attack	
Evidence	4683ecfd2429d796554b74dc26ee5c68
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/privacy-policy.html
Method	GET
Attack	
Evidence	4683ecfd2429d796554b74dc26ee5c68
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/robots.txt
Method	GET
Attack	
Evidence	7f9107a391ecd3dfc815f248ca78888f
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/sitemap.xml
Method	GET
Attack	
Evidence	5618a48f2335d8bd84a8f1fdfe33f450
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	43ab0add1f7113ae984f4b7a4ac49461
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	b9b5fda434924160c679c4e922d37ac4
Other	

Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	d0bc7d207c747e41deef8600af92c76c
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	d802b9b7f494641b3413cca0f06e35c8
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/
Method	GET
Attack	
Evidence	ece216d42015a7c7840ddc92d3e9d2cf401a9991
Other Info	cookie:ci_session
URL	https://jmto-eproc.kintekindo.net/about-us.html
Method	GET
Attack	
Evidence	4683ecfd2429d796554b74dc26ee5c68
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	43ab0add1f7113ae984f4b7a4ac49461
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	d0bc7d207c747e41deef8600af92c76c
Other Info	cookie:csrf_cookie
URL	https://jmto-eproc.kintekindo.net/auth
Method	POST
Attack	
Evidence	d802b9b7f494641b3413cca0f06e35c8
Other Info	cookie:csrf_cookie
Instances	20

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