ZAP Scanning Report

Site: https://jmtm-kms.kintekindo.net

Generated on Tue, 30 Jan 2024 15:48:20

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	4
Informational	5

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	6
Missing Anti-clickjacking Header	Medium	3
Cookie without SameSite Attribute	Low	1
Cross-Domain JavaScript Source File Inclusion	Low	3
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	15
Strict-Transport-Security Header Not Set	Low	1
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	3
Session Management Response Identified	Informational	3
User Agent Fuzzer	Informational	12

Alert Detail

Medium	Absence of Anti-CSRF Tokens
	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:

Description	* 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://jmtm-kms.kintekindo.net/auth
Method	GET
Attack	
Evidence	<form action="https://jmtm-kms.kintekindo.net/auth" method="POST">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "password" "username"].
URL	https://jmtm-kms.kintekindo.net/auth
Method	POST
Attack	
Evidence	<form action="https://jmtm-kms.kintekindo.net/auth" method="POST">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "password" "username"].
Instances	2
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change.

	Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/auth
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/slide%20navbar%20style.css
Method	GET
Attack	
Evidence	

Other Info	
URL	https://jmtm-kms.kintekindo.net/auth
Method	POST
Attack	
Evidence	
Other Info	
Instances	6
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 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	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/auth
Method	GET
Attack	
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/auth
Method	POST
Attack	
Evidence	
Other Info	
Instances	3
	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

Solution	If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

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://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	set-cookie: ci_session
Other Info	
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/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://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	<script src="https://unpkg.com/aos@next/dist/aos.js"></script>
Other Info	
URL	https://jmtm-kms.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://jmtm-kms.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	3
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](829)
WASC Id	15
Plugin Id	[10017](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://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/dist/script.js
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/dist/style.css
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/akhlak.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/alatberat.jpg
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/amp.jpg
Method	GET

Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/bumn.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/coldmix.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/jmtmcopy.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/JMTMLOGOKU.png
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/auth
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/robots.txt
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/sitemap.xml
Method	GET
Attack	

Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/slide%20navbar%20style.css
Method	GET
Attack	
Evidence	x-powered-by: Niagahoster
Other Info	
URL	https://jmtm-kms.kintekindo.net/auth
Method	POST
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	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/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://jmtm-kms.kintekindo.net/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

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://jmtm-kms.kintekindo.net/auth
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue= passwordParam=password referer=https://jmtm-kms.kintekindo.net/auth
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 - 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://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	From
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "<!-- <div class="faq"> <div class="container"> <div class="row"> <div class="col"> <h2 c", 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	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://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	<a class="navbar-brand fw-bold fs-4" href="#"><img src="https://jmtm-kms.kintekindo.net/assets/landing/assets/img/JMTMLOGOKU.png" alt="" width="200px"></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://jmtm-kms.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	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://jmtm-kms.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	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	3
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://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	0584b9927de0b8581581509d9b7cb70eba101807
Other Info	cookie:ci_session
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	1bc6c071d88362555dd0648a6419cc8ecfca73eb
Other Info	cookie:ci_session
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	0584b9927de0b8581581509d9b7cb70eba101807
Other Info	cookie:ci_session
Instances	3
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

CWE Id	
WASC Id	
Plugin Id	10112

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	

URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	12
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104