JMTM-KMS ZAP VAT KINTEK TEAM-LAST_5

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

Generated on Mon, 26 Feb 2024 14:05:14

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	3
Informational	4

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	4
Cookie without SameSite Attribute	Low	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	14
Strict-Transport-Security Header Not Set	Low	1
Modern Web Application	Informational	1
Retrieved from Cache	Informational	9
Session Management Response Identified	Informational	3
User Agent Fuzzer	Informational	12

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	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	
Instances	4
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

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	**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/assets/landing_bootsrap.min.css
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	
Instances	14
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	**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	<img src="https://jmtm-kms.kintekindo.net/assets/landing/assets/img/JMTMLOGOKU.png" alt="" width="200px">
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	1

Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/dist/script.js
Method	GET
Attack	
Evidence	Age: 3773
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/dist/style.css
Method	GET
Attack	
Evidence	Age: 3453
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/akhlak.png
Method	GET
Attack	
Evidence	Age: 2821
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/alatberat.jpg
Method	GET
Attack	
Evidence	Age: 3850
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/amp.jpg
Method	GET
Attack	
Evidence	Age: 2821
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/bumn.png
Method	GET

Attack	
Evidence	Age: 3449
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/coldmix.png
Method	GET
Attack	
Evidence	Age: 3449
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/jmtmcopy.png
Method	GET
Attack	
Evidence	Age: 3449
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://jmtm-kms.kintekindo.net/assets/landing_bootsrap.min.css
Method	GET
Attack	
Evidence	Age: 1949
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
Instances	9
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

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	22414a2ee13c03a95233042b072bb83d0ef5fe95
Other Info	cookie:ci_session
URL	https://jmtm-kms.kintekindo.net/
Method	GET
Attack	
Evidence	77b5369d4a7f889830570c6d6177c27403c85305
Other Info	cookie:ci_session
URL	https://jmtm-kms.kintekindo.net/assets/landing/assets/img/coldmix.png
Method	GET
Attack	
Evidence	22414a2ee13c03a95233042b072bb83d0ef5fe95
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