DRTPROC JMTO

Site: https://drtproc.jmto.co.id

Generated on Tue, 29 Aug 2023 14:35:35

ZAP Version: 2.13.0

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	25
Cross-Domain Misconfiguration	Medium	11
Hidden File Found	Medium	1
Missing Anti-clickjacking Header	Medium	2
Cookie Without Secure Flag	Low	1
Cross-Domain JavaScript Source File Inclusion	Low	32
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	36
Strict-Transport-Security Header Not Set	Low	36
X-Content-Type-Options Header Missing	Low	11
Modern Web Application	Informational	2
Session Management Response Identified	Informational	3
User Agent Fuzzer	Informational	31

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://drtproc.jmto.co.id
Method	GET
Attack	

Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/about-us.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/blog-detail.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/blog.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/coming-soon.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/contact-us.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/course-detail.html
Method	GET
Attack	
Evidence	

Other Info	
URL	https://drtproc.jmto.co.id/course.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/error-page.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/event-detail.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/events-grid.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/events-list.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/faq.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/gallery.html
Method	GET
Attack	
Evidence	
Other Info	

URL	https://drtproc.jmto.co.id/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/pricing.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/privacy-policy.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/sign-in.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/sign-up.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/teachers-single.html
Method	GET

Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/teachers.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/terms-and-conditions.html
Method	GET
Attack	
Evidence	
Other Info	
Instances	25
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

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://drtproc.jmto.co.id/assets/img/gardu.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/gerbang.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/jalan.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/jmto_logo.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/logo3.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/monitoring.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/proc.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

Other Info	implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/ruastol.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/support.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/volume_logo.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://drtproc.jmto.co.id/assets/img/wa_logo.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	11
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	Hidden File Found
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	https://drtproc.jmto.co.id/composer.lock
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	composer
Instances	1
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

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://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
Solution	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. 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 Secure Flag
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	Set-Cookie: ci_session
Other Info	
Instances	1
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/dataTables.bootstrap4.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	

Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/bootstrap/bootstrap.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/counter/jquery.countTo.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/custom.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax-video.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jquery-3.4.1.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jquery.appear.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id

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://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/owl-carousel/owl.carousel.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/popper/popper.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/shuffle/shuffle.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiper/swiper.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiperanimation/SwiperAnimation.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
Other Info	

URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/dataTables.bootstrap4.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://cdn.datatables.net/1.13.4/js/jquery.dataTables.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/bootstrap/bootstrap.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/counter/jquery.countTo.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/custom.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax-video.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jarallax/jarallax.min.js"></script>

Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jquery-3.4.1.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/jquery.appear.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
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://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/owl-carousel/owl.carousel.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/popper/popper.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/shuffle/shuffle.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	

Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiper/swiper.min.js"></script>
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	<script src="https://themes.potenzaglobalsolutions.com/html/academic/js/swiperanimation/SwiperAnimation.min.js"></script>
Other Info	
Instances	32
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://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/about-us.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/gardu.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod

Other Info	
URL	https://drtproc.jmto.co.id/assets/img/gerbang.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/jalan.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/jmto_logo.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/logo3.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/monitoring.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/proc.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/ruastol.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	

URL	https://drtproc.jmto.co.id/assets/img/support.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/volume_logo.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/wa_logo.png
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/blog-detail.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/blog.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/coming-soon.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/contact-us.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/course-detail.html
Method	GET

Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/course.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/error-page.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/event-detail.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/events-grid.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/events-list.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/faq.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/gallery.html
Method	GET
Attack	

Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/index.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/pricing.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/privacy-policy.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/robots.txt
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/sign-in.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/sign-up.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other	

Info	
URL	https://drtproc.jmto.co.id/teachers-single.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/teachers.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
URL	https://drtproc.jmto.co.id/terms-and-conditions.html
Method	GET
Attack	
Evidence	X-Powered-By: centminmod
Other Info	
Instances	36
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

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://drtproc.jmto.co.id
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	
Other Info	

URL	https://drtproc.jmto.co.id/about-us.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/gardu.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/gerbang.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/jalan.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/jmto_logo.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/logo3.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/monitoring.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/proc.png
Method	GET

Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/ruastol.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/support.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/volume_logo.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img/wa_logo.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/blog-detail.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/blog.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/coming-soon.html
Method	GET
Attack	

Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/contact-us.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/course-detail.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/course.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/error-page.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/event-detail.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/events-grid.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/events-list.html
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://drtproc.jmto.co.id/faq.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/gallery.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/index.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/pricing.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/privacy-policy.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/sign-in.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/sign-up.html

Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/teachers-single.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/teachers.html
Method	GET
Attack	
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/terms-and-conditions.html
Method	GET
Attack	
Evidence	
Other Info	
Instances	36
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 http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

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	https://drtproc.jmto.co.id/assets/img/gardu.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/gerbang.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/jalan.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/jmto_logo.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/logo3.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/monitoring.png
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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	https://drtproc.jmto.co.id/assets/img/proc.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/ruastol.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/support.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/volume_logo.png
Method	GET
Attack	
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	https://drtproc.jmto.co.id/assets/img/wa_logo.png
Method	GET
Attack	
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	11
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	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

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://drtproc.jmto.co.id
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://drtproc.jmto.co.id/
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://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	erc8ae2h225vpkcupeihlm0enk799b4d
Other Info	cookie:ci_session
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	td217kvj78vmnhom4dcio6pakg4ufv92

Other Info	cookie:ci_session
URL	https://drtproc.jmto.co.id/
Method	GET
Attack	
Evidence	erc8ae2h225vpkcupeihlm0enk799b4d
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](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://drtproc.jmto.co.id/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets
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://drtproc.jmto.co.id/assets
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://drtproc.jmto.co.id/assets
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://drtproc.jmto.co.id/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets
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://drtproc.jmto.co.id/assets
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://drtproc.jmto.co.id/assets
Method	GET

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img
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://drtproc.jmto.co.id/assets/img
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://drtproc.jmto.co.id/assets/img
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://drtproc.jmto.co.id/assets/img
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/assets/img
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://drtproc.jmto.co.id/assets/img
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://drtproc.jmto.co.id/assets/img
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/robots.txt
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/robots.txt
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://drtproc.jmto.co.id/robots.txt
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/robots.txt
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://drtproc.jmto.co.id/robots.txt
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://drtproc.jmto.co.id/robots.txt
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://drtproc.jmto.co.id/robots.txt
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	31
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	[10104](10104)