ZAP Scanning Report - PDSI Kominfo

Sites: https://172.30.103.119 http://172.30.103.119

Generated on Wed, 19 Oct 2022 20:27:18

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	5
Informational	6

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	5
Anti-CSRF Tokens Check	Medium	5
Content Security Policy (CSP) Header Not Set	Medium	8
HTTP Only Site	Medium	1
Sub Resource Integrity Attribute Missing	Medium	6
Vulnerable JS Library	Medium	3
Cookie No HttpOnly Flag	Low	5
Cookie Slack Detector	Low	54
Dangerous JS Functions	Low	1
Permissions Policy Header Not Set	Low	19
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	45
Base64 Disclosure	Informational	26
GET for POST	Informational	2
Information Disclosure - Suspicious Comments	Informational	22
Modern Web Application	Informational	8
Non-Storable Content	Informational	8
Storable and Cacheable Content	Informational	37

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	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: * 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	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
Instances	5
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	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**Anti-CSRF Tokens Check**
Description	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: * 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	http://172.30.103.119

Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="blog.html">
Instances	5
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	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	[352](352)
WASC Id	9
Plugin Id	[20012](20012)

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	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/visi-misi

Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/blog.html
Method	POST
Parameter	
Attack	
Evidence	
Instances	8
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
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	HTTP Only Site
Description	The site is only served under HTTP and not HTTPS.
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	
Attack	
Evidence	

Instances	1
Solution	Configure your web or application server to use SSL (https).
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html https://letsencrypt.org/
CWE Id	311
WASC Id	4
Plugin Id	10106

Medium	Sub Resource Integrity Attribute Missing
Description	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL	http://172.30.103.119/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Nunito&display=swap" rel="stylesheet">
URL	http://172.30.103.119/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<link rel="preconnect" href="https://fonts.gstatic.com">
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Nunito&display=swap" rel="stylesheet">
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	
Attack	
Evidence	<link rel="preconnect" href="https://fonts.gstatic.com">
URL	http://172.30.103.119/profil/blog.html
Method	POST
Parameter	
Attack	
Evidence	<link href="https://fonts.googleapis.com/css2?family=Nunito&display=swap" rel="stylesheet">
URL	http://172.30.103.119/profil/blog.html
Method	POST
Paramete	

r	
Attack	
Evidence	<link rel="preconnect" href="https://fonts.gstatic.com">
Instances	6
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en/docs/Web/Security/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 1.12.4 is vulnerable.
URL	http://172.30.103.119/frontend/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	* Bootstrap v4.1.1
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	/*! jQuery UI - v1.12.1
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	/*! jQuery v1.12.4
Instances	3
Solution	Please upgrade to the latest version of jquery.
Reference	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
WASC Id	
Plugin Id	10003

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	http://172.30.103.119
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
URL	http://172.30.103.119/
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	XSRF-TOKEN
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Instances	5
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie Slack Detector**
Description	Repeated GET requests: drop a different cookie each time, followed by normal request with all cookies to stabilize session, compare responses against original baseline GET. This can reveal areas where cookie based authentication/attributes are not actually enforced.
URL	http://172.30.103.119
Method	GET

Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/animate.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/bootstrap.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/custom-animate.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/custom.css
Method	GET
Parameter	
Attack	

Evidence	
URL	http://172.30.103.119/frontend/css/flaticon.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/font-awesome.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/jquery-ui.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/jquery.fancybox.min.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/jquery.mCustomScrollbar.min.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/owl.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/responsive.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/style.css
Method	GET

Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/fonts
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/fonts/flaticon.woff
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/fonts/fontawesome-webfont.woff2?v=4.6.1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/appear.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	

Evidence	
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.mCustomScrollbar.concat.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/main.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/map-script.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/owl.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/popper.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/wow.js

Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-2.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-3.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-4.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-5.jpg
Method	GET
Parameter	

Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-6.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/icons
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/icons/flag-icon.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/main-slider
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/main-slider/2.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/logo.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/struktur-organisasi

Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/uploads
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/uploads/20221005090839_logo.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/uploads/ckeditor
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/uploads/ckeditor/StrukturOrganisasi.drawio_1664961006.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	

Attack	
Evidence	
URL	http://172.30.103.119/profil/blog.html
Method	POST
Parameter	
Attack	
Evidence	
Instances	54
Solution	
Reference	http://projects.webappsec.org/Fingerprinting
CWE Id	[200](200)
WASC Id	45
Plugin Id	[90027](90027)

Low	**Dangerous JS Functions**
Description	A dangerous JS function seems to be in use that would leave the site vulnerable.
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	eval
Instances	1
Solution	See the references for security advice on the use of these functions.
Reference	https://angular.io/guide/security
CWE Id	[749](749)
WASC Id	
Plugin Id	[10110](10110)

Low	**Permissions Policy Header Not Set**
Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/
Method	GET
Paramete	

r	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/appear.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.mCustomScrollbar.concat.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/main.js
Method	GET
Parameter	
Attack	
Evidence	

URL	http://172.30.103.119/frontend/js/map-script.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/owl.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/popper.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/wow.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/sitemap.xml
Method	GET

Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/profil/blog.html
Method	POST
Parameter	
Attack	
Evidence	
Instances	19
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://developers.google.com/web/updates/2018/06/feature-policy https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/animate.css
Method	GET
Parameter	

Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/bootstrap.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/custom-animate.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/custom.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/flaticon.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/font-awesome.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/jquery-ui.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/jquery.fancybox.min.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)

URL	http://172.30.103.119/frontend/css/jquery.mCustomScrollbar.min.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/owl.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/responsive.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/css/style.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/fonts/flaticon.woff
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/fonts/fontawesome-webfont.woff2?v=4.6.1
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/appear.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/bootstrap.min.js
Method	GET
Paramete	

r	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/jquery.mCustomScrollbar.concat.min.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/main.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/map-script.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/owl.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)

URL	http://172.30.103.119/frontend/js/popper.min.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/frontend/js/wow.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-1.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-2.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-3.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-4.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-5.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-6.jpg
Method	GET

Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/icons/flag-icon.png
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/images/main-slider/2.png
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/logo.png
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/robots.txt
Method	GET
Parameter	
Attack	

Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/uploads/20221005090839_logo.png
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/uploads/ckeditor/StrukturOrganisasi.drawio_1664961006.png
Method	GET
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
URL	http://172.30.103.119/profil/blog.html
Method	POST
Parameter	
Attack	
Evidence	nginx/1.18.0 (Ubuntu)
Instances	45
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 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	10036

Informational	**Base64 Disclosure**
Description	Base64 encoded data was disclosed by the application/web server. Note: in the interests of performance not all base64 strings in the response were analyzed individually, the entire response should be looked at by the analyst/security team/developer(s).

URL	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6ImNQN3duSmh2Rkg1NmpjUmJxTlRBMEE9PSIsInZhbHVlIjoiSkExQWZVOXFpWndtU3QxRVNCdlZlV1pDREN5VjVvSXNXeC9JYnlmZzVWMnJISFF5dWdFR0k0S25RRk9VV1dEcTFGNzhqU2ZDUWRJa2xNRlgzQjNyRlhlMFlmVUhrby9jL2NQbTlRMXNEaHllR3F0OWRUbkZEMU9nRFoxdW5rZUEiLCJtYWMiOiIyNWYzZGQwYTI2ZDA4MzhiNWMyY2YyOTM0YzI5MDk3ODczMjI1ODdjMTBjNGY5NTA2OWQ3YmMxZTRhOTAwNTcxIiwidGFnIjoiIn0
URL	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IlUza3o0c3NSV0pEOThRbTFaR0VONHc9PSIsInZhbHVlIjoiOVpWYXMwZFluSmtqdHF6cTQ2K1Q3Zmg3MGV0M2E4VXhaR0NraUI1ZmJsZTVROElBYytjOG9oS3U1cFVpYy94UTdTZkRBdjl4b1hYeUdaT01NOEs3MEUvMGROZE5pM3FFZWNLSnJEUDVkWTk0MmRlcW9ETXhSTUNYNWpHakp4dnYiLCJtYWMiOiI0Mzg5YzA5Nzc1NDA4NmU1MjhlZjU1MDM3MGI5M2I4MWQ5MDEzOGVlZTA0MTg4MWU3MGQwZDVkOTlhZjJmZDYzIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IjI0TS9FZ2podGdlREJ0TnlEY0ZVZ3c9PSIsInZhbHVlIjoiL2F5Z2tnQ2tENG52TG1lbDVOT1VsZHVCUGRzQ3hjZ0dMKyswNGVuUy9vL1YxQUl5WnVJWEh3Rkl5RTEyYm5sWXpSUjZ5YWVvTVRSY1B2QTl4SnFvTGdjdkhuTkszZ3djVi9lSjlyQkZlV2VhTFBmZ1l2bkRPNGFVcEJDMm9iMG0iLCJtYWMiOiIwZGRlNzBhZDk3NzNkMTU3MTg5YWNjODI5ZTJkYzQ0MWYyZjFkNWQ3NzYyOTQ0ZGVjMTBmNzI4YzJiNGI2OGI5IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IjJrNVJEUWNtcDR3VXgwYmx4cGNtK0E9PSIsInZhbHVlIjoiK0dJRE1TN2s2dTNtVVMvSC9OaWo4MVM1OWNjdnh5czhPQld6WEpka045M0JNYm5lejhsYUtMOWpyRTBPRWNRUG1lVVpadUNCanRvaUFuQmhBVFRnK1JDRTAydmxwN1hnOENqK2lsR2krYk85TGVKVE02VjBHYzBkWUFxdjlzNWEiLCJtYWMiOiIyYWUwYjYyMWE0ODc4NDY3ZTlmMTQwMjVmMmI1ZTgzZDhmOTE5ZGM0MjdhZmI4ZmI5NDg4NzcxMThkMTRmZGQwIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IjVGWHovcnEwdHFjei9zUlZBZXJwdEE9PSIsInZhbHVlIjoiN0FnWHhlTFlyMCtHQk9lMVBZUDN4Y0pFUC8yaktheUloUUo1NnAraDdlYklLclBqeWVWMVF0eEl2QklwN2o5SkM5cHl0N3plZ3BqZExsWnhMVCtBRDVYWFJld1l3TU5KN24zN3RsOGF2Y3R4Q3BVWnVzMVBYMzl2N1pSSWtzM0siLCJtYWMiOiJkYzY3ODc1NmMwODUxMzUxYWNkNjQzY2NkNDY0MDhjZjRjYWUyZGZlYmMzZWE0MjkzYmFhMTQ4Yzc1MWRlZGViIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET

Parameter	
Attack	
Evidence	eyJpdiI6IjZ4Vkt0TW5pOHAvaU9ES2E3UFIvNHc9PSIsInZhbHVlIjoiU2dmUUs0ajJLdEoydTZ0NHJNdTdQTUhxREJNcGNTYit2cXNzcnFVemVUajNoYkZLQ2w4dlZBTWI2bVFsTXIyU1dtRjlXYkN3dElpdDg4Mmk1NFpKM0t5Y3VDblhPTDN6MlptVlhCaGlOSVY1L2lCUXRTQWpKYm1vOGMrNmRsTDUiLCJtYWMiOiI3NTRkNTk0NDlmY2U5NDk1YzQ4OWU3NTcwMjhjNjJlY2Q5MzM1MzUwOGY4YjA3MTA0YTY5ZjM3YmJjZmJjNDMzIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6ImJOMWtlaERidDA5SU5acEJlY2EzQVE9PSIsInZhbHVlIjoiV3RQaTVUY3cxL25DZUUvcndGdnUrdmRrSTE3VVZNYlp4dzdPT2JNb0dlZEdQcE1IdThlLzFtT2doemdtTzVzaWNVZHc2Q1V3d1ZkUHhmczNJQTR1bmNEYU1ydWtWTnN2UGFQaEZCVWtWN045NUxyWm1ScUJJc0R4dHhOdW9uWXciLCJtYWMiOiI2NmJiMTRkNjk5NWQxOGY1ODU1ZjIxMDkzNWVhZjNhZTNkZjZhMTAyNGRmYWRlYWE5NTE4NTkzNzAwNmMzMzRjIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6ImM3eTByZWowN0FPaWFiT0xlVW9OZGc9PSIsInZhbHVlIjoiU3Vsby9ISExIcGd2MW5iU1EzN1kxVEhHQ01MZ3lpa3ZKUTRWOGZiR1o3SW5hdjBwN2pDaFZsdkM2bzRHMmpneFRoVkRXK3JiQ2cxVnNkUDhDSi9UWnQxRHhGR3pwN0xRNEl5emxQbW1tV3plN0JlckduNTBoZElBc1FESTF2S3kiLCJtYWMiOiIzYzRkODQ2YzExYWE1NjgyMTcxMDU4ZWU0MTVjM2Q4Nzk4Nzk4ZjEzMDczZjY1ZDZiOWY2NjY4ZTRkZWVkZjA2IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6ImNvVlZVQ2VkMU9CL2M3ZWErcHo5aXc9PSIsInZhbHVlIjoiK1BmZzUyNzVsamZLTi9CdmY2OHhBallicjEwYXB2RmJOeFNxOU84SlE4cWRSS1l6STQ0VVpweGxJSFBLMzkrNnk3bXpZbnRjZGs0UElWR2JNM2IxT2d1U3ZZelp5WFZ2SXhUOEFJMEFyTTBkR0daSTBKVWMzUnVjVlRSbVNFRlMiLCJtYWMiOiIzNTMzMWY0OGQ0ZGU3MzE0OGY3YmIyY2M2ZjU4NGM4NGI1ZTRlNzBhOGNiYzUwNTRkNzdlOTZlMzQyMjUwODFiIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6Ikg3NTFNOVgrdzI5RGFINVdkRllGZ1E9PSIsInZhbHVlIjoiWEhUVHpNRERpV3RGcHd2eGlqY0x3ckpUL3JkbEhjSHJaaXlOeHU2TVRQK21JMWREbENkTURsWG9COWQ0bHBkeWlIM1M4KytOYjNDNXlQT3hvb1RTckp1R3N3UkhYbEc0Q3BvbUpiaERrUnpiRGs4SzZZeTFhNTcwZVI4VC9PN3giLCJtYWMiOiIzNTc5NTY0NmNiZmYyMWYwY2RmNzkyOTA5MmVjYzY4NmY0Nzk1NmU5NGQ2NzFkMTA0OWQ5YzJjNDNlZmRiNWU3IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	

Evidence	eyJpdiI6Ik9Lb0lHNkx6VkRQdDFpN01iWFZLWXc9PSIsInZhbHVlIjoidFpSbnR0QWkrS2ttSlo1MXRzSi83TTdMVzRJWXp3a0RNZ2pLRFBoMmViUUN2MFcwYm03b1c3bmZSMm81L043UEpEZ0ZrZm5HSWUvdXJFRzRuMTcrdHg4bXhMTEV3OWZzbzlPZHE0cWRHVU9qcXdULzVnT3ZjVDMvK0tCN1JsVm8iLCJtYWMiOiI2ZDJlODZkNmMwODllYmM2MDUyMDA2Y2U2MzRkNTMxZjI5NzczYjdlNzBmNWU1Y2QzMTY0M2Y5ZjVhNjRmMjdkIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6Ik9PTzA5VlNnVzBrWmM3REVLaHJ5Wmc9PSIsInZhbHVlIjoiUjdrWTJ3L2V1SUFJMElTdWJwd2xMRUxUNjh3Z2dWdmhNTjlkcytta3VyTUhqVy9KZEFTTHFqMHRoVTRRZUxZbHNaTDVKZGhMOXhHamwxb3YzMCsyeEZJQU9SY1crL2ZjdkZFNkFtc0Q4d1Q0RzhKRGZqNHN4MFFobytBQkM1QXYiLCJtYWMiOiJlMWRlNmRhOGViYzI2YmZmNzA1MWFkOTgwOTAyMzY4NmY4MjdlZmZhMWQ4ZjRjMzVmMzE2ZmM1ZWQ4NDFlNjBmIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6Ik9WVW0xZkhubnVMc3BqYmdqTkt5b1E9PSIsInZhbHVlIjoiVWJsTlJ5U0lISWdtTDVrZE5jVTNBZ3RCZlM3c2p4VWxQcnc5U21Pa0NuSWxCanZiT2VsaVF4T2hrLzVQZ1dPZ2Y4Q0FMSnRFWjhySTdZQXhRZ0tjL28xUFY1VFpha3FpN2FwSG91Zi84a1l6NXplMTVWOU5OWUFKT2ZYR3g4YXIiLCJtYWMiOiIxOTRkYmE1NDhhMzI1MDNkOTgxM2JlYThmNDhjZGY3ZDIxODYyOTAxYTQxNDQwOTkwZDJmYmNjY2E4MGI3ZWZkIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IlRrbFBPMWwzOGFiNnhieVpld2xsR2c9PSIsInZhbHVlIjoibUVEbjdLNElnK3V4OC9Fb1VlVjcwbE9PQ29LUUt4N3JFYVNZNGEzbXc5cGVKbm0xMFR2cGxvNmpVWmU5bXpkWXZLREFCT0pCL2tDTWRYOUk4QnVTVDkzWGRqRmNBUEpTOE1PQWVEcnN2RS9LeGRTYThWNTQ4YVJsWHFTc1QyYnAiLCJtYWMiOiI4ZWRjYzUzODQwOWE4YjYwNjIwMmI3NzI3NzJlNjE5M2IxZWY0ODYzM2M0ODhmMGViNzcyOWYxMjg1Y2NmOTVhIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IlRaUWFLUjR3d1BreTFsNzh3WG9XUHc9PSIsInZhbHVlIjoieStJaXdEWDRsNktKSWpZT2tkdlltSGNBRVAramVCeW1Yd3pueEkzSXROUjN6djMvRnV6b1NGVFowSWZVbjhsSG91WGRtMmFEVnQxUlBtalFjMFJwUkFPMlA4aHh0TlE5aHRQdERnTVQxQzNSSlI0ZjA5WmNoZkc4b2gweHFPdU4iLCJtYWMiOiI2MzBkZjJhYTA1NTMxNDJhMTllODUwNGQ0OGEyOWRmZDExNTNmZDFhZDNhNDMxZDc0NTRkZTVjZTIzMWI2ZDliIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IlYwbTNjdy8vcjdMazZmUWZwTjFXYkE9PSIsInZhbHVlIjoiNXM4UnNpWkh6N0xPMUs0YlZFbkRYSWxMZ1dyMzFlUzFjWWdPckpWZ01vVzBHTlYwWEpsVmhYWWVkTzhvNEx0OVByZnR3TU5BbkJGaHAyT2srWHcybGg5K0ZrZkc5aUgvNmxiVGVNWkx1cGEvbGVzeFBJSkl0

	UnN4dDUvUnprQk0iLCJtYWMiOiI1NmRiMDAxOTkxMjQ2MzdhMzZiMGJkMmRiNjNmZWJiOWRjNWU3N2M5NGMxMGQ3MWZhNGNiM2Q3MWRhZTYzNGM5IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6Ild1NHllY0VNcXRHckZxRUN3QkYzVVE9PSIsInZhbHVlIjoiSWRwamtBeUxDclFjcElSam9iS2MvejI5MEJxY0FWQkF2UFNGL1RMYi92MXdkUzhkc2M1a0xib1U5MkRjRzVXeUwvNVppc0dZMk9jQWU0aG5FdU1SNU9ieU5iZEY2ai9WRHVkS0ZmRmQ4YjdtNFZuUXdnZGZtQXNOc2lJbkFGTm8iLCJtYWMiOiJiMWI5NWQ4MzE4NDE4ZWFmZDczZDdhYjYyMDQ0N2QwNWI1ZGYzODVlMzI5ZGE2MDgxZDQxMGQxMjA3YjFiOGExIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IlhRT1hQS3hMUERnM2Z4WDRPZ0Q5Wmc9PSIsInZhbHVlIjoiUytNdGo2dHZibXMvZU5laHZJZWNQZ2tDeXdzZkJBSFlweGdwREtKbEl6My9NazkvajVYTzJub0xYQU5USE53ei9uMVZQTmlaM3owOHhaY0xEdlNFcHZHU0w3Z1NwRFJpL1FjczBJMzJuMlovMmh2a3BBZGNmMUkwRGVYZTVLbUwiLCJtYWMiOiIzMmFmMTcwODUxZDkxOTk0NTdkZmM2MGQyMTlhM2I3ZDgyYzg2Yjg4M2Y0M2I2NzdkZTUzYTA0Njg4ODQ3NTA0IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6InludVBlQUVtMjBnMlM2M0RWMWJoSGc9PSIsInZhbHVlIjoiay9SMWRZM2s0VVh4VzlmMGg3T3RZMndHSkRDOHJkeXp5a2RXZlh1UVh0MGV3bE9OekhPSjh1d2Q0WXliREFZczZYdTEyeXRqenlBbFhieVljM2pOM0F1citiTHZzYUJRSVhWc0dscmRaZnl4SGFnSVBJdlB6SXg2M1dTRE54OVUiLCJtYWMiOiJjODNhOGIxYmRlODkxNjc0NTcyMWU5YmY0Yjk0YzhlNWU1M2I5OWU3YmFmNDg2MTYxZDY0MjhhNGEyOTdiNGFhIiwidGFnIjoiIn0
URL	http://172.30.103.119/frontend/css/jquery-ui.css
Method	GET
Parameter	
Attack	
Evidence	R0lGODlhAQABAIAAAAAAAP///yH5BAEAAAAALAAAAAABAAEAAAIBRAA7
URL	http://172.30.103.119/frontend/css/jquery.mCustomScrollbar.min.css
Method	GET
Parameter	
Attack	
Evidence	iVBORw0KGgoAAAANSUhEUgAAAAgAAAAICAYAAADED76LAAAANElEQVQYV2NkIAAYiVbw//9/Y6DiM1ANJoyMjGdBbLgJQAX/kU0DKgDLkaQAvxW4HEvQFwCRcxIJK1XznAAAAABJRU5ErkJggg==
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	

Attack	
Evidence	D27CDB6E-AE6D-11cf-96B8-444553540000
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6Ik0rR0x2Z2grVWhVNmpCYkUyU2dnUVE9PSIsInZhbHVlIjoiTzBsZzRVQUhIYzBGQWl2alJFbFh3QTVyWTA1cVJNRTFValhuZ2tJZjlGWC9FUUlSTG1NT2E5L0c5bkJmaVFCa3M4SXVHWllIN1hvL0M5b0RJNlJRSG0ydjNPejAwLzUrcGlGczBkKy9lc2o5aHd6SmN0YkNZZFZiYmZCcitnWWUiLCJtYWMiOiJkODA5YTJkNDQzYmI3ODZlYjMwY2MxOTBmMzVjMjk0OTdjMjg5YmFiMWVjYzcwZjRiMmIyYTQ3NTdmM2FjMjY1IiwidGFnIjoiIn0
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6InZCYnR3VXBub1dra21tNmdob2swbmc9PSIsInZhbHVlIjoidFVuRW1BVnBUV1d6dzJ2dTEzWHcyVm1CM2p3YU1vU25TbTYxa1FURnZ1LyswUlBucnl3SXFLeUVEbzhxUzJBc0YwU2tOWTFrVUx0aGNyUTFvcmZ0Q1NYMk9YanRscjI5RUwxRGhQblNaVEJ0ak9leWpTUWZ5Nm1wbmxnaFRaOFkiLCJtYWMiOiI5YjIzMjhlNTA1ODdhNmQ3MWRhYTc1NDczNDhkYWFjNGIzMTc3Y2QxYTU3ODFiOGUwZDkyYmJkZjU5ZWFkMDk5IiwidGFnIjoiIn0
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IjAzNGxkbUNGSTdKY04yLytZU1kwSmc9PSIsInZhbHVlIjoiYmxabmlPZ2JkL0pkcUx1eDBCczdBQ2JKbjlKVkpwdW9jOTlCRFNjaHBrWG13b1Z2SU4vaDFIMmd4U0x2b29LWnRicGtkVTVxeHBZdVlkb1UxMHhtbjZleEV5a0ZWcHFvSDkvRjdXemZJOElMNzNMSDRlMloxTU1sQ3J2UUxkT0wiLCJtYWMiOiJiMjJhMTczM2MzNGY1NmU2NzVjZDc2YzMyZmNhNjE1MmJlMTZlNzg4NWQyMmU4YTk0ZTIyZjVlNWE4NTlhNmQzIiwidGFnIjoiIn0
URL	http://172.30.103.119/uploads/ckeditor/StrukturOrganisasi.drawio_1664961006.png
Method	GET
Parameter	
Attack	
Evidence	3E7Vtbc5s6EP41fjwdJHERjzjGqevWzsTpyUlfOtQoNlOCMpg09vn1FUYYkMCmLthOi1
Instances	26
Solution	Manually confirm that the Base64 data does not leak sensitive information, and that the data cannot be aggregated/used to exploit other vulnerabilities.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10094

Informational	GET for POST
Description	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.

URL	http://172.30.103.119/blog.html
Method	GET
Parameter	
Attack	
Evidence	GET http://172.30.103.119/blog.html?field-name= HTTP/1.1
URL	http://172.30.103.119/profil/blog.html
Method	GET
Parameter	
Attack	
Evidence	GET http://172.30.103.119/profil/blog.html?field-name= HTTP/1.1
Instances	2
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

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	http://172.30.103.119/frontend/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	from
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	bug
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	bugs
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	

Evidence	from
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	later
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	Select
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	TODO
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	user
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
Attack	
Evidence	where
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	from
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	later
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET

Parameter	
Attack	
Evidence	query
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	select
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	user
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	where
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	db
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	select
URL	http://172.30.103.119/frontend/js/jquery.mCustomScrollbar.concat.min.js
Method	GET
Parameter	
Attack	
Evidence	select
URL	http://172.30.103.119/frontend/js/main.js
Method	GET
Parameter	
Attack	

Evidence	select
URL	http://172.30.103.119/frontend/js/owl.js
Method	GET
Parameter	
Attack	
Evidence	from
URL	http://172.30.103.119/frontend/js/owl.js
Method	GET
Parameter	
Attack	
Evidence	todo
URL	http://172.30.103.119/frontend/js/owl.js
Method	GET
Parameter	
Attack	
Evidence	user
Instances	22
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	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	<a href="#">0213865607</a>
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	<a href="#">0213865607</a>
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Paramete	

r	
Attack	
Evidence	<a class='ui-datepicker-prev ui-corner-all ui-state-disabled' title='" + prevText + "'><span class='ui-icon ui-icon-circle-triangle-" + (isRTL ? "e" : "w") + "'>" + prevText + "</span></a>
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	<a download data-fancybox-download class="fancybox-button fancybox-button--download" title="{{DOWNLOAD}}">' + '<svg viewBox="0 0 40 40">' + '<path d="M20,23 L20,8 L20,23 L13,16 L20,23 L27,16 L20,23 M26,28 L13,28 L27,28 L14,28" />' + '</svg>' + '</a>
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	<a id='"+u+"'></a>
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	<a href="#">0213865607</a>
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	<a href="#">0213865607</a>
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	<a href="#">0213865607</a>
Instances	8
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Non-Storable Content**
Description	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.

URL	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	private
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	private
URL	http://172.30.103.119/profil/struktur-organisasi
Method	GET
Parameter	
Attack	
Evidence	private
URL	http://172.30.103.119/profil/tugas-fungsi
Method	GET
Parameter	
Attack	
Evidence	private
URL	http://172.30.103.119/profil/visi-misi
Method	GET
Parameter	
Attack	
Evidence	private
URL	http://172.30.103.119/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	private
URL	http://172.30.103.119/blog.html
Method	POST
Parameter	
Attack	
Evidence	private
URL	http://172.30.103.119/profil/blog.html
Method	POST

Parameter	
Attack	
Evidence	private
Instances	8
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood) The "no-store" cache directive must not appear in the request or response header fields For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives) In addition to the conditions above, at least one of the following conditions must also be satisfied by the response: It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	**Storable and Cacheable Content**
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. 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 "shared" 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	http://172.30.103.119/frontend/css/animate.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/bootstrap.css

Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/custom-animate.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/custom.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/flaticon.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/font-awesome.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/jquery-ui.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/jquery.fancybox.min.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/jquery.mCustomScrollbar.min.css
Method	GET
Parameter	

Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/owl.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/responsive.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/css/style.css
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/fonts/flaticon.woff
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/fonts/fontawesome-webfont.woff2?v=4.6.1
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/appear.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery-ui.js

Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.fancybox.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/jquery.mCustomScrollbar.concat.min.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/main.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/map-script.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/owl.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/popper.min.js
Method	GET
Parameter	

Attack	
Evidence	
URL	http://172.30.103.119/frontend/js/wow.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-1.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-2.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-3.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-4.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-5.jpg
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/gallery/footer-gallery-thumb-6.jpg
Method	GET
Parameter	
Attack	
Evidence	

URL	http://172.30.103.119/images/icons/flag-icon.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/images/main-slider/2.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/logo.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/uploads/20221005090839_logo.png
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/uploads/ckeditor/StrukturOrganisasi.drawio_1664961006.png
Method	GET
Parameter	
Attack	
Evidence	
Instances	37
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 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	524
WASC Id	13
Plugin Id	10049