ZAP Scanning Report - PDSI Kominfo

Sites: //172.30.103.119 http://172.30.103.119

Generated on Tue, 25 Oct 2022 10:31:03

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Cookie No HttpOnly Flag	Low	2
Cookie Slack Detector	Low	46
Dangerous JS Functions	Low	1
Permissions Policy Header Not Set	Low	13
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	37
Base64 Disclosure	Informational	21
Information Disclosure - Suspicious Comments	Informational	32
Modern Web Application	Informational	5
Non-Storable Content	Informational	3
Storable and Cacheable Content	Informational	34

Alert Detail

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
Instances	2
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/api
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/api/home
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/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.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/js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	
URL	http://172.30.103.119/logo.png
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	
Instances	46
Solution	
Reference	http://projects.webappsec.org/Fingerprinting

CWE Id	200
WASC Id	45
Plugin Id	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/js/app.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
WASC Id	
Plugin Id	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
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.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/js/app.js
Method	GET
Parameter	
Attack	
Evidence	
Instances	13
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/api/home

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/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

Parameter	
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.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/js/app.js
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/robots.txt
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)
Instances	37
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	eyJpdiI6IjNTSmUxUm0yVHB3VlBVbzJLVC9IVmc9PSIsInZhbHVlIjoic0hpQlB4NVpoRUlhM1BNdTZoOWpqYU1mZ1lWcFJ5V3FxMXpscGpMTkUvWEphRmNxMGdqVFAycjBjODhRZFNYVnhlMlBxaENaY09TSnJDVHJsUDliVk9VTEkybkY5bm9LVGtaUHhEenB6bkJSV2pDaTlwY1o5SWtUKzZod1IvZzQiLCJtYWMiOiI1Y2JhZGExNTQwZjg5ZjBiMThjNmEzNWY3NWRkYTJhZWY4ZDcxNjY3MmRmYzYyYjVhMmY1NTUzMzI2MTVmYTI3IiwidGFnIjoiIn0
URL	http://172.30.103.119
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IndtU05MMTQ5MFNvOUY3U1BRbEZjZWc9PSIsInZhbHVlIjoiWnZFTVJzSzlxS2o2VGVlQjk4WmRpSFNkRGdqRWpQalpEYWR5aFNtUDFHcXpDQ2tlbDZzQlZxRm5uOCtmUDh6WDdGY2FSZE9FTldpVXRaa1VLdTZPbVRpMjI3empvU3o0VjJkTG5vdzg3Ry9RVkR3OG5LOU1RWGFpRStuNitvTVUiLCJtYWMiOiIwZGRmOTgzZmNjNGIyYzcwZWJmM2JkNTRjMzkzYWIzZGQ4YWU2ZTYyZmEyMjE1YjEwMmRlNjM2YWRmMzM3ODY2IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IjVkTUZmcWNYMk9HNGtmSlQ3dUhOcEE9PSIsInZhbHVlIjoicUt5dWRnZThvUGZQWTNQRFVNY1FOSWVFeVBCVFVKYS9NVUkzbHkwa0xpNTljOHpRMi8vWGRmZ3B1bVRtNkRzOTRKZGdkVkpLUUNSeXhxUnd1TVg3aVF5THM3UDFXKzJoelJMaTJGSWhGWXZmVnAydmpPa3ZmL2RtQm9ZUHgxWGQiLCJtYWMiOiJhODM3YWFkZDgzMjc5Y2IxMmM3ZmY2ODZhYzk2YmI5NTUzN2JhZTU5Zjg5NGQ4Y2FkZjI2ZTgzNDI3NGQ0ZTVmIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	

Evidence	eyJpdiI6IjZWbDZ4MXBqMGRSQXNvcDg5eGdtRlE9PSIsInZhbHVlIjoiNVNYamtkeE51OUZFdTlPVHBYYUNOV2hHZG9uMmdMQStWQmhKbnBnYmg2VGlYWHZZSnpGNnREVlVKLzNNNHE4dGxjNXdMbUwveUo3b0krUEhQRFZGVktDR0tySGVlRnNaVGhhU0l2Tk5GckVWZzRtaTlQbVhtU0l2cmcyV3hETnAiLCJtYWMiOiI0NjhjMjAzNjdmNTlhYTZiMDQ4Mzk3MjI4MzlhNGNmMWU0MDA0YTEzODIxNDhhODVjZjQ3YjdlNjdjOTU4NzU4IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6ImE1Z2ZiRkVTbDB3OTdaT2VjcGkvMGc9PSIsInZhbHVlIjoid1UxM3Jkc05oMTRiQ2tCNXltc1RvT3N1RTF3SlB6QkorbEcwazJxNEhpTGx4OVNJN3FPbU1FcGlaWDlUNkNCVkdxWlNJakI0MEN4NFZHTVNUa1NpTzJxYmFaVTBhc0NtRUdmTEN3b2VKVVRHcXFUZ1hwUmFBS3BOczBNT0c0WkkiLCJtYWMiOiJiM2E0NDdhOTkyZTI2OGIwMDY2OGFlMmE0YWI4MDA0MmRlMjE5ODZiNjhmNTdlOWI3YzkyMDllYWVhMjRmMjRlIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6ImRqclBJWFRUVUFiY29vL2JPWFlsaVE9PSIsInZhbHVlIjoiU3pJWmNKNzZuSWI1dG50ZGpoeTE2WEdhUjAwSkgxY04yZDUzZGNwSTRsa0dCN2toV01Cd0x6T3g5czdhR3lCcDJDMlVoYURNbHR3OVk1d1d4WS9RVUFoWnMxWUZQc0ptQ1ByUGgwTHBsUmpya1J0RG14aGpzU1pDcGZya1lvVzMiLCJtYWMiOiI3MTQ0OGJkZjEzYmI1NzM2MjIyZjQ1YTk4ZWY1ZjM4MDA0ZWE5YmRlZTYxNzk3YTEwMDljZmY3YWQ5NGI4YmM0IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IkV3cEdoa1RFTjBTNWk1WEp1SmRZTWc9PSIsInZhbHVlIjoiSFMvdDQ3cERiMFJEWXdEOTRPNHdGQUs4WnFvdVdQVHkyQnBQcXphaFBGSjkvdGJNMnFUWXg4NWZyNitoaWtiZVlwTGZmbkU0TEdKaGNOaU5EZGVpZjkyQ2lsZ0R4L2hEVHJjaEhwNUo2M3hBVnhqWWk5K3M4RGR5ZnpiQWYxZjQiLCJtYWMiOiI0NGQ2NzFjY2U3ODU4OWE3M2JkZDk5NzNjNTc5ZmIwMGNlMDI4ZDNlODE0Njg0YTk3NjQ0YTRkYTkwZGU4ZjUwIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IkZxOXFxTmtzMmRuQjNLR3dja1BXbUE9PSIsInZhbHVlIjoiWngxdmFKUHVkWXZzSlJJTThiV3h0Q1ZpVEVzWmQwNk4zUnNGOVZQSVd1ZVlyODNkV0dXS2ZiR0tWOEdaYjQ1K0REU3Yvdk9pUUhnSU42bnE0amVxL2dxSndSTDJTbWtXZ2huTUJCMjNlaHQrL3lmRFpGNTJwenBHK1JETnc2d0EiLCJtYWMiOiI1ZWMwZmQyYTBlYzhkMDFjODhlZTJlNWZjOWJhMjQ0NzQ5NGQ1YTdmNTc2YWUyNTk0YmNhYzYwZTgyNTQ1MzIyIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	

Evidence	eyJpdiI6IkdjNVIydnBTOVlOSHd2NUtRMzNQS2c9PSIsInZhbHVlIjoiczRWSGNKNDBjZXdwYUNUcnpka1B4VlZ1Z3JYUmxNVU9xY1drY0x0STgzL3l6VllxSis0ZGZUY1RoMGZieklRL3ZkT1N5RldFZVZGMlJOeHdqN09uREhuWjZDWW5lWTRic1JheFBqTjcrTnNocGZENVdQZzVBSXRLVTdrRkwvbmwiLCJtYWMiOiI5MDU1OGIwZDU4YTI1YmJlMDM0YTJlY2NlNzFmZjBmMTk1Nml4OWQ0MDhiMGNhMzg2NjIwZGQ5OTI3NjNjYjFhIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6ImhQc3RCVlFtQ1ZIWlhueklvR1Jocnc9PSIsInZhbHVlIjoiQlJzSSt4RVBZNE95UDJ5T08rL3hZK3VNZ05XK3FCR25HSU1kRlBuMFZ3SWJYblp0NVVTZEg5b3MwZG5xOC9YZ2NySWJhYjMwelBXekwwZ1F0R1BKVzMzbU53TTM3MVdkOWxyZm5qV3AvSGE2VURhakNwTTJ1N0FWMStNOGN3YUwiLCJtYWMiOiI0NTY4NGY5OTk1ZWNmMWMwYjY2NDA1OTU5ZTk0MWU0NjRlY2QzODQ3YWQyOWVhNDZiOTg4MzE3OGExMjk4YjMxIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IktEd0pFbVU2K1pMNUFEa3V0WjlOZVE9PSIsInZhbHVlIjoiMysrRGJqSEM2bVFoa2w1VDVNQlVURTY0VXBWWXI5UmdHVG9nVXdXUmZVQ1J5cnNVTHducXRSWm1adVhrMTBVY21ob3ZxaW9VVHVLUmpHTUlvRWR0dEtkQzhMV3VQcGNNYllvdHZZWWw0MlBZZ3ZUMzdZN0NYWkVMcThpVmJ2MSsiLCJtYWMiOiIxZWU4ODljMGJiNDg4YzYwYzQ2YmMwMjE4YTJmOTFhYWYxYmZkYjgzMDk1YTRjNzFkMWIyNGExY2RiNGY5MDlkIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6Im03R0NNVlZ1MDRIckpMenQ0YWF5eFE9PSIsInZhbHVlIjoid05iYStkeWFBTmxLWFpTTFI0bGI3TVlwYTJNRzBuUnF3R0F3Tlg2MzBoRVAyWWUybmE0ajZ5b2FwTzBESVFIbjdZWEZVcTlFRXlhMmhSUEp6RnczMktXSW8wVGNWWjRVSTVCaDY1cWc2WEJqcWw3bmhES243bFFOSVg1L0ROLysiLCJtYWMiOiI2Nzc3YTQ0NGE3Y2E4YmUzMmEyY2I0MDMzMmY2YjA4YWY0ZDM0ZGE2NjhmNTE4OWY4NzVlMzNkYjFiZGE5ZTM0IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6Ik1lQ3NXM2d6NktSS3YvWjExQzc0M2c9PSIsInZhbHVlIjoiUm8vUHk0aThESFpUaTRaNG5JZHdsWmkxL1VZc085aXZXWTBzcHFOVC8wMlZSZFhMZkFuOTlJdjJoSUV5UGtBcEovT2dScHB0MVNKQWtJMXBldzd1bDdYbCtmVGpSMzRRUjVQTUNRT2N0SzJWcGNiNkpObXJSNk1oc1hrVElycEUiLCJtYWMiOiJkMzFkYWI1ZGFkYTJkY2I2ZDU3OTk2ZTY2ZTQzMTkwNzBiMjg0NjFjYmQwNzIyNDM5OGEwZmZmNGE4YmZjYzdhIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	

Evidence	eyJpdiI6Im95TUE0Y0o4OXZZK096dEZzVE9aM0E9PSIsInZhbHVlIjoieEZFd0UrN0JMVmZHNGoxRFZuc2ZyUm9xT05ZMUJOR0VNYnpOazRONnZTdVpyQnlQV0lUSHVvMFhNVGIrS3ZCK0pPamVXeHloTWFnRnMzaDN5aTlJWkFRRnZnU2MzZ0dnMWQyenNvSGtGWjVqQ1MxYXkzcDZ0ZEluQkJvRGtHWVMiLCJtYWMiOiJlYmU4MDIwMDdmYzA0MGU5NTEyZTU2YjVjMzRjNGZmMzJmNjJlMjkxNDk3YWI1MWRkZWI1MGYxZjdkNzM0ODkyIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6InBDeC9aaDM5MldxUktPUlhUK0RSTGc9PSIsInZhbHVlIjoiYVhER0ZhU2gxdnlkV1lkd2dtK0RoMnU4TDFZTXFTYnRuRktPdTZ2S0dvNEhaZFU5a0NPT2ZBZ2ZvZ2FuT3ZJazY5NFozdkkwdVdhdU4xYjJuVHZ3eDlFSjhCeGRhdGlTaVR2TE94ZWVBaEwzWk1DdjA5eFhiRlpHRHRPVDJjbTMiLCJtYWMiOiJkMDY5NGRmYzNkYjE0NzAxNGIyY2IzMDVkYzYxOTQ2YTBhYjI4MWU5NzM3ODliZjAzNWZlNjQwMmMwNjM5YzFiIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6InRkRlRsdGhjTEd5dUdVMHgzWmpEYUE9PSIsInZhbHVlIjoiY1psVkh1VjcvZFJhTGxKVlVYeW1CVmVUTE1PSWFxQUNzcVY2c3NFSlFVcTQrOVB0ZmZybFU0OXlLRmtLWXptRS9TTzVPdE1XNFI3MTAxVitTS2xZTHRGODJNcG1zWW1xOHNPMkpLTVRhdm56SzVZTmxzMGtvbFF2M1lrRHVSZlIiLCJtYWMiOiJjNjc3NmM2NjJlYWM3YzA5MDM5ZmI0MWRjYTk3MTBmN2IxZWYyYWQzN2Y2NjBjMDM1MzQyNjE0Y2E4YjJiMDJhIiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6IlkxK0tOeDJHcERBa05qVVZiSDU3V1E9PSIsInZhbHVlIjoiM3hXT3k4WWN5ak1nUFVMRXREWUM1MlltUmt3Rm9yd2pIQ2psS3p5cCsxVVUzSFM5NVl6eUZkQWt0VkhKRis1UkVtTkdZWGhra093KzJ1R1pyYno4OXVza0xlVEVzYlA5djBNSUp4Z24xNTFPdVZRSGIyU2diZkdzZHZQc29yWGQiLCJtYWMiOiJjNDhmNTQyODI1ZDE0NTZmYTYzOTE4MGM5NmE1MzhlZWU5MTViNmFiNmE3NmQ4ZDBlOGE3NjNlNDY4ZjRmMjc4IiwidGFnIjoiIn0
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	eyJpdiI6InlnbjFlT3VLWlZLN2VZSEJleGxIa1E9PSIsInZhbHVlIjoibFZHMXV3S1RpOVpFU1ZZcjdtdmphZllXSWlKUUM2TlMyZVBhaW1uOGpTZC9tQWdqc2h0VyswY1dGbFlGbHdxZXFsRkppaVQxZnU4d3BkZ0tmRDdSUkhvTzBxYjlMRkNuOGx4clZwV2dzMm9ZVVBNanhUUnRKM0RvY3RERFFaZ3oiLCJtYWMiOiJmYzI5OWZhYzg1YTI0OTE3NzI0ZmU2NmQxNWMyNmNlNGU1MTA0NzRhZTM0MWQ0MmRkZTFkYmQ1MTdiYTIxOTQ2IiwidGFnIjoiIn0
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/js/app.js
Method	GET
Parameter	
Attack	
Evidence	_layouts_Header_vue__WEBPACK_IMPORTED_MODULE_0__
Instances	21
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	**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.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
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	Admin
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	bug
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	bugs
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	from
URL	http://172.30.103.119/js/app.js
Method	GET

Parameter	
Attack	
Evidence	later
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	query
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	select
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	TODO
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	user
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	username
URL	http://172.30.103.119/js/app.js
Method	GET
Parameter	
Attack	
Evidence	where
URL	http://172.30.103.119/js/app.js
Method	GET

Parameter	
Attack	
Evidence	xxx
Instances	32
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	<script src="/js/app.js"></script>
URL	http://172.30.103.119/
Method	GET
Parameter	
Attack	
Evidence	<script src="/js/app.js"></script>
URL	http://172.30.103.119/frontend/js/jquery-ui.js
Method	GET
Parameter	
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/js/app.js
Method	GET

Parameter	
Attack	
Evidence	<a>
Instances	5
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	[10109](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/api/home
Method	GET
Parameter	
Attack	
Evidence	private
Instances	3
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/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.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/js/app.js
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	
Instances	34
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