ZAP Scanning Report

Site: https://loonar.cloud

Generated on Sat, 15 Nov 2025 01:57:37

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	6
Informational	7
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	5
Content Security Policy (CSP) Header Not Set	Medium	12
Missing Anti-clickjacking Header	Medium	13
Sub Resource Integrity Attribute Missing	Medium	13
Cross-Domain JavaScript Source File Inclusion	Low	6
Insufficient Site Isolation Against Spectre Vulnerability	Low	18
Permissions Policy Header Not Set	Low	12
Strict-Transport-Security Header Not Set	Low	12
Timestamp Disclosure - Unix	Low	14
X-Content-Type-Options Header Missing	Low	15
Charset Mismatch	Informational	4
Information Disclosure - Suspicious Comments	Informational	12
Modern Web Application	Informational	12
Re-examine Cache-control Directives	Informational	12
Storable and Cacheable Content	Informational	11
Storable but Non-Cacheable Content	Informational	1
User Controllable HTML Element Attribute (Potential XSS)	Informational	9

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	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	<form class="elementor-form" method="post" id="form_loonar" name="lp-cloud">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-aceite_lgpd" "form-field-cargo" "form-field-email" "form-field-empresa" "form-field-mensagem" "form-field-nome" "form-field-telefone" "form_id" "post_id" "queried_id" "referer_title"].
URL	https://loonar.cloud/2021/06/29/hello-world/
Method	GET
Parameter	
Attack	
Evidence	<form action="https://loonar.cloud/wp-comments-post.php" method="post" id="commentform" class="comment-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	<form class="elementor-form" method="post" name="Novo formulário">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-cargo" "form-field-email" "form-field-empresa" "form-field-mensagem" "form-field-nome" "form-field-Produto" "form-field-site" "form-field-telefone" "form_id" "post_id" "queried_id" "referer_title"].
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/embed/
Method	GET
Parameter	
Attack	
Evidence	<form class="elementor-form" method="post" name="Novo formulário">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-cargo" "form-field-email" "form-field-empresa" "form-field-mensagem" "form-field-nome" "form-field-Produto" "form-field-site" "form-field-telefone" "form_id" "post_id" "queried_id" "referer_title"].
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	<form class="elementor-form" method="post" name="Novo formulário">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "form-field-cargo" "form-field-email" "form-field-empresa" "form-field-mensagem" "form-field-nome" "form-field-Produto" "form-field-site" "form-field-telefone" "form_id" "post_id" "queried_id" "referer_title"].
Instances	5
	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.

Solution	Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/2021/06/29/hello-world/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/2021/06/29/hello-world/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author/marcel-rodrigues/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author/zelir/

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/obrigado/embed/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-comments-post.php
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
Instances	12
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/

Reference	https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://loonar.cloud
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/2021/06/29/hello-world/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/2021/06/29/hello-world/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author/marcel-rodrigues/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author/zelir/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/category/uncategorized/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/embed/
Method	GET

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/obrigado/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/politica-de-privacidade/embed/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	13
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/Reference/Headers/X-Frame-Options
CWE Id	[1021]()
WASC Id	15
Plugin Id	[10020]()

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	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	<link data-optimized="2" rel="stylesheet" href="https://loonar.com.br/wp-content/litespeed/css/c1d2e7a4f0a572bbbb42ba1b46be11f2.css?ver=b297c" />
Other Info	

URL	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	<script src="https://loonar.com.br/wp-content/plugins/gtranslate/js/flags.js" data-no-optimize="1" data-no-minify="1" data-gt-orig-url="/servicos/cloud/" data-gt-orig-domain="loonar.com.br" data-gt-widget-id="67152195" defer></script>
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='google-fonts-1-css' href='https://fonts.googleapis.com/css?family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CDosis%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic&#038;display=auto&#038;ver=6.8.3' type='text/css' media='all' />
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=explicit&amp;ver=3.3.0" id="elementor-recaptcha_v3-api-js"></script>
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/embed/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='google-fonts-1-css' href='https://fonts.googleapis.com/css?family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CDosis%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic&#038;display=auto&#038;ver=6.8.3' type='text/css' media='all' />
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/embed/
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=explicit&amp;ver=3.3.0" id="elementor-recaptcha_v3-api-js"></script>
Other Info	
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='google-fonts-1-css' href='https://fonts.googleapis.com/css?family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CDosis%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic&#038;display=auto&#038;ver=6.8.3' type='text/css' media='all' />
Other Info	
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	

Attack	
Evidence	<script type="text/javascript" async src="https://d335luupugsy2.cloudfront.net/js/loader-scripts/af28ea6f-0e76-485a-a18d-723b70d16631-loader.js" ></script>
Other Info	
URL	https://loonar.cloud/obrigado/embed/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='google-fonts-1-css' href='https://fonts.googleapis.com/css?family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CDosis%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic&#038;display=auto&#038;ver=6.8.3' type='text/css' media='all' />
Other Info	
URL	https://loonar.cloud/obrigado/embed/
Method	GET
Parameter	
Attack	
Evidence	<script type="text/javascript" async src="https://d335luupugsy2.cloudfront.net/js/loader-scripts/af28ea6f-0e76-485a-a18d-723b70d16631-loader.js" ></script>
Other Info	
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='google-fonts-1-css' href='https://fonts.googleapis.com/css?family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CDosis%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CLato%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic&#038;display=auto&#038;ver=6.8.3' type='text/css' media='all' />
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	<link rel='stylesheet' id='google-fonts-1-css' href='https://fonts.googleapis.com/css?family=Roboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic%7CDosis%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic%2C900%2C900italic&#038;display=auto&#038;ver=6.8.3' type='text/css' media='all' />
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=explicit&amp;ver=3.3.0" id="elementor-recaptcha_v3-api-js"></script>
Other Info	
Instances	13
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://loonar.cloud
Method	GET
Parameter	https://loonar.com.br/wp-content/plugins/gtranslate/js/flags.js
Attack	
Evidence	<script src="https://loonar.com.br/wp-content/plugins/gtranslate/js/flags.js" data-no-optimize="1" data-no-minify="1" data-gt-orig-url="/servicos/cloud/" data-gt-orig-domain="loonar.com.br" data-gt-widget-id="67152195" defer></script>
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=explicit&ver=3.3.0
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=explicit&amp;ver=3.3.0" id="elementor-recaptcha_v3-api-js"></script>
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/embed/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=explicit&ver=3.3.0
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=explicit&amp;ver=3.3.0" id="elementor-recaptcha_v3-api-js"></script>
Other Info	
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	https://d335luupugsy2.cloudfront.net/js/loader-scripts/af28ea6f-0e76-485a-a18d-723b70d16631-loader.js
Attack	
Evidence	<script type="text/javascript" async src="https://d335luupugsy2.cloudfront.net/js/loader-scripts/af28ea6f-0e76-485a-a18d-723b70d16631-loader.js" ></script>
Other Info	
URL	https://loonar.cloud/obrigado/embed/
Method	GET
Parameter	https://d335luupugsy2.cloudfront.net/js/loader-scripts/af28ea6f-0e76-485a-a18d-723b70d16631-loader.js
Attack	
Evidence	<script type="text/javascript" async src="https://d335luupugsy2.cloudfront.net/js/loader-scripts/af28ea6f-0e76-485a-a18d-723b70d16631-loader.js" ></script>
Other Info	
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?render=explicit&ver=3.3.0
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=explicit&amp;ver=3.3.0" id="elementor-recaptcha_v3-api-js"></script>
Other Info	
Instances	6
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	**Insufficient Site Isolation Against Spectre Vulnerability**
Description	Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.

URL	https://loonar.cloud
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author-sitemap.xml
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/category-sitemap.xml
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/e-landing-page-sitemap.xml
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/page-sitemap.xml
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/post-sitemap.xml
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/robots.txt
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/sitemap_index.xml
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/06/Artboard-5@2x-1-4.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	

Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/06/Artboard-5@3.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/06/rocket_buster.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/07/04-lua-1.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/07/fire_booster.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/07/Frame-1.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/07/Frame-17.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/07/Vector-2.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud
Method	GET
Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud
Method	GET
Parameter	Cross-Origin-Opener-Policy

Attack	
Evidence	
Other Info	
Instances	18
Solution	Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages. 'same-site' is considered as less secured and should be avoided. If resources must be shared, set the header to 'cross-origin'. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cross-Origin-Embedder-Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

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	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/2021/06/29/hello-world/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author/marcel-rodrigues/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/plugins/duracelltomi-google-tag-manager/js/gtm4wp-form-move-tracker.js?ver=1.15.2
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/plugins/elementor-pro/assets/js/webpack-pro.runtime.min.js?ver=3.3.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?ver=3.3.0
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/plugins/elementor/assets/js/webpack.runtime.min.js?ver=3.2.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=3.2.4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	12
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/Reference/Headers/Permissions-Policy https://developer.chrome.com/blog/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	**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://loonar.cloud

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/category-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/e-landing-page-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/page-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/post-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/sitemap_index.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/06/rocket_buster.png
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/07/fire_booster.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-content/uploads/2021/07/Frame-1.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-json/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	12
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	1655836437
Other Info	1655836437, which evaluates to: 2022-06-21 18:33:57.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	1662393781
Other Info	1662393781, which evaluates to: 2022-09-05 16:03:01.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	1662397874
Other Info	1662397874, which evaluates to: 2022-09-05 17:11:14.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	

Evidence	1752204712
Other Info	1752204712, which evaluates to: 2025-07-11 03:31:52.
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	1655836437
Other Info	1655836437, which evaluates to: 2022-06-21 18:33:57.
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	1656108275
Other Info	1656108275, which evaluates to: 2022-06-24 22:04:35.
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	1752204712
Other Info	1752204712, which evaluates to: 2025-07-11 03:31:52.
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	
Attack	
Evidence	1655836437
Other Info	1655836437, which evaluates to: 2022-06-21 18:33:57.
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	
Attack	
Evidence	1656067928
Other Info	1656067928, which evaluates to: 2022-06-24 10:52:08.
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	
Attack	
Evidence	1752204712
Other Info	1752204712, which evaluates to: 2025-07-11 03:31:52.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	1655836437
Other Info	1655836437, which evaluates to: 2022-06-21 18:33:57.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	1662393781
Other Info	1662393781, which evaluates to: 2022-09-05 16:03:01.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST

Parameter	
Attack	
Evidence	1662397874
Other Info	1662397874, which evaluates to: 2022-09-05 17:11:14.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	1752204712
Other Info	1752204712, which evaluates to: 2025-07-11 03:31:52.
Instances	14
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	[497](497)
WASC Id	13
Plugin Id	[10096](10096)

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://loonar.cloud
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/author-sitemap.xml
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/category-sitemap.xml
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/e-landing-page-sitemap.xml
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/page-sitemap.xml
Method	GET
Parameter	x-content-type-options

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://loonar.cloud/post-sitemap.xml
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/robots.txt
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/sitemap_index.xml
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/wp-content/uploads/2021/06/Artboard-5@2x-1-3.png
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/wp-content/uploads/2021/06/Artboard-5@3.png
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/wp-content/uploads/2021/06/rocket_buster.png
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/wp-content/uploads/2021/07/04-lua-1.png
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/wp-content/uploads/2021/07/fire_booster.png
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/wp-content/uploads/2021/07/Frame-1.png
Method	GET
Parameter	x-content-type-options
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://loonar.cloud/wp-content/uploads/2021/07/Vector-2.png
Method	GET
Parameter	x-content-type-options
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	15
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	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Charset Mismatch**
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	https://loonar.cloud/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Floonar.cloud%2F2021%2F06%2F29%2Fhello-world%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://loonar.cloud/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Floonar.cloud%2Fmorpheus-data-multicloud-management-platform%2F
Method	GET
Parameter	
Attack	
Evidence	

Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://loonar.cloud/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Floonar.cloud%2Fobrigado%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://loonar.cloud/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Floonar.cloud%2Fpolitica-de-privacidade%2F
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
Instances	4
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"WebPage","@id":"https://loonar.com.br/servicos/cloud/","url":"https://loonar.com.br/servicos/c", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/2021/06/29/hello-world/
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"Organization","@id":"https://loonar.cloud/#organization","name":"Loonar","url":"https://loonar", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/author/marcel-rodrigues/
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"Organization","@id":"https://loonar.cloud/#organization","name":"Loonar","url":"https://loonar", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"Organization","@id":"https://loonar.cloud/#organization","name":"Loonar","url":"https://loonar", see evidence field for the suspicious comment/snippet.

URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"Organization","@id":"https://loonar.cloud/#organization","name":"Loonar","url":"https://loonar", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"Organization","@id":"https://loonar.cloud/#organization","name":"Loonar","url":"https://loonar", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"Organization","@id":"https://loonar.cloud/#organization","name":"Loonar","url":"https://loonar", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/wp-content/plugins/elementor-pro/assets/js/preloaded-elements-handlers.min.js?ver=3.3.0
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.w3.org/2000/svg",viewBox:"0 0 500 150",preserveAspectRatio:"none"}).html(this.getSvgPaths(e.marker));this.elements.$dynami", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/wp-content/plugins/elementor/assets/js/frontend.min.js?ver=3.2.4
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.youtube-nocookie.com",a.origin=window.location.hostname),r.addClass("elementor-loading elementor-invisible"),this.player=n", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/wp-content/plugins/elementor/assets/lib/share-link/share-link.min.js?ver=3.2.4
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//.test(f),h=g?"":"_self";open(f,h,b)},i=function(){a.each(b.classList,function(){var a=f(this);if(a)return g(a),!1})},j=functio", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//,Bt={},_t={},zt="*/".concat("*"),Xt=C.createElement("a");function Ut(o){return function(e,t){"string"!=typeof e&&(t=e,e="*");v", see evidence field for the suspicious comment/snippet.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST

Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org","@graph":[{"@type":"Organization","@id":"https://loonar.cloud/#organization","name":"Loonar","url":"https://loonar", see evidence field for the suspicious comment/snippet.
Instances	12
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	<a href="#" class="ekit-menu-nav-link ekit-menu-dropdown-toggle">Serviços<i class="icon icon-down-arrow1 elementskit-submenu-indicator"></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://loonar.cloud/2021/06/29/hello-world/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/author/marcel-rodrigues/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/author/zelir/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/category/uncategorized/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	GET
Parameter	

Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/embed/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/obrigado/embed/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/politica-de-privacidade/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/politica-de-privacidade/embed/
Method	GET
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	
Attack	
Evidence	<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-K4RCLQC" height="0" width="0" style="display:none;visibility:hidden" aria-hidden="true"></iframe></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
Instances	12
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	

Plugin Id	10109

Informational	Re-examine Cache-control Directives
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://loonar.cloud
Method	GET
Parameter	cache-control
Attack	
Evidence	max-age=0
Other Info	
URL	https://loonar.cloud/author-sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/author/marcel-rodrigues/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/category-sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/category/uncategorized/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/e-landing-page-sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/obrigado/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/page-sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	

Other Info	
URL	https://loonar.cloud/post-sitemap.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/robots.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/sitemap_index.xml
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://loonar.cloud/wp-json/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
Instances	12
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

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	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/author-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

URL	https://loonar.cloud/category-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/e-landing-page-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/page-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/post-sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/sitemap_index.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://loonar.cloud/wp-content/uploads/2021/07/fire_booster.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

URL	https://loonar.cloud/wp-json/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
Instances	11
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://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	Storable but Non-Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, but will not be retrieved directly from the cache, without validating the request upstream, in response to similar requests from other users.
URL	https://loonar.cloud
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
Instances	1
Solution	
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	form_fields[Produto]
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: form_fields[Produto]=Morpheus Data – Multicloud Management Platform The user-controlled value was: morpheus data – multicloud management platform
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	form_id
Attack	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [div] tag [data-id] attribute The user input found was: form_id=28df5d65 The user-controlled value was: 28df5d65
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	form_id
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: form_id=28df5d65 The user-controlled value was: 28df5d65
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	post_id
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: post_id=2956 The user-controlled value was: 2956
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	post_id
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: post_id=2956 The user-controlled value was: 2956
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	queried_id
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [div] tag [data-elementor-id] attribute The user input found was: queried_id=2973 The user-controlled value was: 2973
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	queried_id
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: queried_id=2973 The user-controlled value was: 2973
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST
Parameter	referer_title
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: referer_title=Morpheus Data - Multicloud Management Platform - Loonar The user-controlled value was: morpheus data - multicloud management platform - loonar
URL	https://loonar.cloud/morpheus-data-multicloud-management-platform/
Method	POST

Parameter	referer_title
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://loonar.cloud/morpheus-data-multicloud-management-platform/ appears to include user input in: a(n) [meta] tag [content] attribute The user input found was: referer_title=Morpheus Data - Multicloud Management Platform - Loonar The user-controlled value was: morpheus data - multicloud management platform - loonar
Instances	9
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031

Sequence Details

With the associated active scan results.