intruder

Vulnerability report

eramba

17 April 2026

1 target scanned

Threat Level

Low

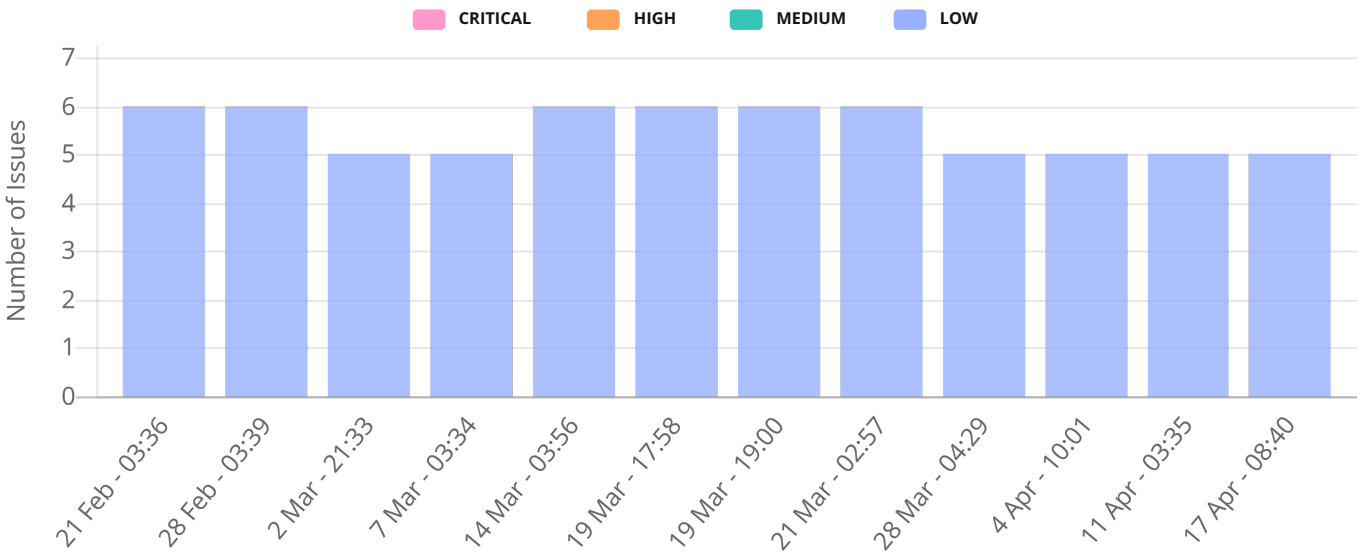
Target	Issues
1	5

Critical	High
0	0

Medium	Low
0	5

Low severity issues can not directly be exploited by an attacker, but may increase the ease of exploiting more severe issues in future. Fixing these issues may help protect against weaknesses that are not publicly known, or be used as one component in a highly targeted attack by the most sophisticated and well resourced attackers.

Exposure over time



Total checks

45,020

The types of areas we cover when reviewing your targets and their accessible web pages:

Vulnerable software & hardware

- Web servers, e.g. Apache, Nginx
- Mail servers, e.g. Exim
- Development software, e.g. PHP
- Network monitoring software, e.g. Zabbix, Nagios
- Networking systems, e.g. Cisco ASA
- Content management systems, e.g. Drupal, Wordpress
- Other well-known weaknesses, e.g. 'Log4Shell' and 'Shellshock'

Attack Surface Reduction

Our service is designed to help you reduce your attack surface and identify systems and software which do not need to be exposed to the Internet, such as:

- Publicly exposed databases
- Administrative interfaces
- Sensitive services, e.g. SMB
- Network monitoring software

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Web Application Vulnerabilities

- Checks for multiple OWASP Top Ten issues
- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- Local/remote file inclusion
- Web server misconfigurations
- Directory/path traversal, directory listing & unintentionally exposed content

Information Leakage

Checks for information which your systems are reporting to end-users which should remain private. This information includes data which could be used to assist in the mounting of further attacks, such as:

- Local directory path information
- Internal IP Addresses

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

Cloud Security

These checks assess your cloud environment for misconfiguration and accidental exposure including:

- Checks for misconfigured cloud settings
- Missing security controls and mitigations
- Insecure user roles and permissions
- Exposed services and overpermissive access controls

Open issues by severity and exploit likelihood

	N/A	Rare	Unlikely	Likely	V. Likely	Known	Total
Critical	–	–	–	–	–	–	0
High	–	–	–	–	–	–	0
Medium	–	–	–	–	–	–	0
Low	5	–	–	–	–	–	5

Issues detected

Cookie Missing HttpOnly Attribute

Low 3 occurrences

Cookie Missing SameSite Attribute

Low 5 occurrences

Missing Content-Security-Policy Header

Low 40 occurrences

Missing HSTS Header

Low 2 occurrences

Missing X-Content-Type-Options Header

Low 40 occurrences

Cookie Missing HttpOnly Attribute

Low 3 occurrences

Description

A cookie was set by the web application without the "HttpOnly" attribute, meaning it can be accessed from JavaScript run on the web page. This allows the cookie to be stolen by an attacker targeting users with issues which allow them to inject malicious JavaScript into the application, such as cross-site scripting. If the cookie contains sensitive information, for example a session identifier, then the absence of the HttpOnly attribute makes exploiting such issues easier.
For more information on the HttpOnly attribute, please see **this article**.

Remediation Advice

Add the HttpOnly attribute to all cookies set the by web application. Please consult the relevant webserver, framework or programming language documentation for more information.
It may not be possible to set this attribute on all cookies, since the web application may require access to them through JavaScript in the browser. In this case, the cookies should be reviewed to determine whether they contains sensitive content, and a risk assessment should be performed to determine whether the risk posed by this issue is acceptable.

Occurrences	Cookie Name	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	translation	01 Nov 2025 07:53:50
vulnerability.cloud.eramba.org : 443 (tcp)	translation	03 Sep 2025 11:03:52
vulnerability.cloud.eramba.org : 443 (tcp)	translation	03 Sep 2025 11:37:19

Cookie Missing SameSite Attribute

Low 5 occurrences

Description

A cookie was set by the web application without the "SameSite" attribute. This attribute can be used to prevent cookies from being sent in cross-site requests, making it harder or impossible to exploit client-side vulnerabilities such as cross-site request forgery (CSRF) and clickjacking.

More information on the SameSite attribute can be found in **this article**.

Remediation Advice

Set cookies with the "SameSite" property set to "Strict" if possible, or "Lax" if "Strict" is too restrictive. This will prevent session cookies from being sent in requests originating from third parties, so ensure that this change is fully understood and tested before it is deployed.

Occurrences	Cookie Name	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	translation	01 Nov 2025 07:53:50
vulnerability.cloud.eramba.org : 443 (tcp)	translation	03 Sep 2025 11:03:52
vulnerability.cloud.eramba.org : 443 (tcp)	csrfToken	03 Sep 2025 11:03:52
vulnerability.cloud.eramba.org : 443 (tcp)	translation	03 Sep 2025 11:37:19
vulnerability.cloud.eramba.org : 443 (tcp)	csrfToken	03 Sep 2025 11:37:19

Missing Content-Security-Policy Header

Low 40 occurrences

Description

The website does not set the "Content-Security-Policy" header in its responses. This header can be used to specify a policy to help protect against client-side attacks, such as cross-site scripting and clickjacking.

A Content Security Policy (CSP) limits the browser's behaviour to ensure that resources, such as scripts, stylesheets and images, are only loaded from trusted sources. A strong CSP will also:

Prevent or validate inline scripts to mitigate the impact of cross-site scripting attacks.

Prevent the use of unsafe JavaScript functions to block some types of DOM-based cross-site scripting.

Stop the application from being loaded in iFrame elements on untrusted websites to defend against clickjacking.

Limit the outgoing connections made by the website to guard against data exfiltration attacks.

Remediation Advice

Implement a CSP for the web application. The policy should be specified in the "Content-Security-Policy" response header for all pages. The policy should be as restrictive as possible, while still allowing the web application to function.

A strong CSP should not be considered as the primary mitigation for client-side injection attacks, such as cross-site scripting, but is an important part of a "defence in depth" approach.

For more information about implementing a CSP, please see the **OWASP CSP cheat sheet** and the **MDN article on CSP**.

Google's CSP evaluator is a useful tool for evaluating the strength of a CSP, and identifying potential weaknesses or improvements.

Occurrences	Path	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	/sitemap.xml	01 Nov 2025 07:53:48
vulnerability.cloud.eramba.org : 443 (tcp)	/robots.txt	01 Nov 2025 07:53:48
vulnerability.cloud.eramba.org : 443 (tcp)	/login	01 Nov 2025 07:53:48
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/ui/fullcalendar/'+a.htmlEscape(o.url)+'	17 Apr 2026 07:41:11
vulnerability.cloud.eramba.org : 443 (tcp)	/pages/license	17 Apr 2026 07:41:11
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/D3.js	11 Apr 2026 03:35:46
vulnerability.cloud.eramba.org : 443 (tcp)	/password-reset	17 Apr 2026 07:41:11
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/C3.js	11 Apr 2026 03:35:46
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/datepaginator.js	11 Apr 2026 03:35:47
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/listbox.js	11 Apr 2026 03:35:47
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/tagsinput.js	11 Apr 2026 03:35:47
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/tokenfield.js	11 Apr 2026 03:35:47
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/bootstrap_select.js	11 Apr 2026 03:35:47
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/selectbox.js	11 Apr 2026 03:35:47
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/multiselect.js	11 Apr 2026 03:35:47
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/select2.js	11 Apr 2026 03:35:47

Occurrences	Path	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/github.com/necolas/normalize.css	11 Apr 2026 03:35:46
vulnerability.cloud.eramba.org : 443 (tcp)	/YoonityJS-1.0.0.js	01 Nov 2025 07:53:48
vulnerability.cloud.eramba.org : 443 (tcp)	/vue_assets/application/vnd.openxmlformats-officedocument.wordprocessingml.do	17 Dec 2025 11:37:33
vulnerability.cloud.eramba.org : 443 (tcp)	/vue_assets/vue_assets/TableCellCondition-gBePsy8x.js	17 Apr 2026 07:41:11
vulnerability.cloud.eramba.org : 443 (tcp)	/sitemap.xml	03 Sep 2025 11:03:45
vulnerability.cloud.eramba.org : 443 (tcp)	/robots.txt	03 Sep 2025 11:03:45
vulnerability.cloud.eramba.org : 443 (tcp)	/login	03 Sep 2025 11:03:46
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/ui/fullcalendar/'+a.htmlEscape(o.url)+'	17 Apr 2026 07:55:53
vulnerability.cloud.eramba.org : 443 (tcp)	/pages/license	21 Mar 2026 02:26:37
vulnerability.cloud.eramba.org : 443 (tcp)	/password-reset	21 Mar 2026 02:26:37
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/D3.js	04 Apr 2026 04:01:22
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/C3.js	04 Apr 2026 04:01:22
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/datepaginator.js	04 Apr 2026 04:01:22
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/listbox.js	04 Apr 2026 04:01:22
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/tagsinput.js	04 Apr 2026 04:01:22
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/tokenfield.js	04 Apr 2026 04:01:23
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/bootstrap_select.js	04 Apr 2026 04:01:23
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/selectbox.js	04 Apr 2026 04:01:23
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/multiselect.js	04 Apr 2026 04:01:23
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/select2.js	04 Apr 2026 04:01:23
vulnerability.cloud.eramba.org : 443 (tcp)	/limitless_theme/css/github.com/necolas/normalize.css	04 Apr 2026 04:01:23
vulnerability.cloud.eramba.org : 443 (tcp)	/YoonityJS-1.0.0.js	03 Sep 2025 11:03:46
vulnerability.cloud.eramba.org : 443 (tcp)	/vue_assets/application/vnd.openxmlformats-officedocument.wordprocessingml.do	17 Dec 2025 11:43:18
vulnerability.cloud.eramba.org : 443 (tcp)	/login	03 Sep 2025 11:37:18

Missing HSTS Header

Low 2 occurrences

Description

The web server does not reply with an HTTP Strict Transport Security (HSTS) response header. The HSTS header tells web browsers to enforce HTTPS connections for future site visits, ensuring that traffic is encrypted and the server is authenticated.

HSTS provides an additional layer of security against machine-in-the-middle attacks, where in some scenarios a well-placed attacker could impersonate your web server to view or tamper with sensitive traffic. Such attacks are typically difficult to achieve, and HSTS helps eliminate this opportunity by ensuring browsers only initiate secure, encrypted connections.

Remediation Advice

Configure the server to use HSTS response headers. A 1-year enforcement period (i.e. 31536000 seconds) is generally recommended, as is including subdomains where relevant:

Strict-Transport-Security: max-age=31536000; includeSubDomains

More information on header configurations can be found **here**.

For Apache, you can update your HTTPS VirtualHost block as follows:

<VirtualHost *:443>

Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains;"

</VirtualHost>

For Nginx, you can update your server block as follows:

server {

listen 443 ssl;

add_header Strict-Transport-Security "max-age=31536000; includeSubDomains;" always;

}

Occurrences	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	01 Nov 2025 07:53:48
vulnerability.cloud.eramba.org : 443 (tcp)	03 Sep 2025 11:03:48

Missing X-Content-Type-Options Header

Low 40 occurrences

Description

The remote website does not include the header "X-Content-Type-Options: nosniff" in its responses. This header instructs browsers not to guess, or "sniff", the MIME type of a page and instead use the value provided in the "Content-Type" header.

This can be helpful in preventing attacks where content is injected into website pages to cause browsers to treat them as valid scripts or stylesheets, which can then be loaded by other domains in the "script" or "style" HTML tags and partially read. This can lead to sensitive information on these pages being disclosed if an authenticated user clicks a link sent to them by an attacker.

Remediation Advice

Add the header "X-Content-Type-Options: nosniff" to responses for all web pages.

Occurrences	Path	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	/css/font/Roboto-font/Roboto-Regular.ttf	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/favicon.png	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/js/YoonityJS/YoonityJS-2.0.2-eramba.js	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/css/eramba.css	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/css/report-blocks-grid.css	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/colors.css	01 Nov 2025 07:53:50
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/summernote/summernote.css	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/icons/icomoon/styles.css	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/css/bootstrap-colorpicker.css	01 Nov 2025 07:53:49
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/css/eramba.css	01 Nov 2025 07:53:50
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/bootstrap.css	17 Apr 2026 07:41:12
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/components.css	17 Apr 2026 07:41:12
vulnerability.cloud.eramba.org : 443 (tcp)	/vue_assets/index-CfD_x575.css	17 Apr 2026 07:41:12
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/jquery-upgrade/DataTables/ColReorder-1.5.2/js/dataTables.colReorder.min.js	01 Nov 2025 07:53:50
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/jquery-upgrade/DataTables/Buttons-1.6.1/js/dataTables.buttons.min.js	01 Nov 2025 07:53:50
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/jquery-upgrade/jquery-ui.min.js	17 Apr 2026 07:41:12

Occurrences	Path	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/loaders/pace.min.js	03 Jan 2026 04:28:05
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/core/libraries/bootstrap.min.js	04 Apr 2026 04:06:29
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/loaders/blockui.min.js	24 Jan 2026 03:56:21
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/forms/selects/select2.min.js	17 Apr 2026 07:41:13
vulnerability.cloud.eramba.org : 443 (tcp)	/favicon.png	03 Sep 2025 11:03:49
vulnerability.cloud.eramba.org : 443 (tcp)	/css/report-blocks-grid.css	03 Sep 2025 11:03:49
vulnerability.cloud.eramba.org : 443 (tcp)	/js/YoonityJS/YoonityJS-2.0.2-eramba.js	03 Sep 2025 11:03:49
vulnerability.cloud.eramba.org : 443 (tcp)	/css/eramba.css	03 Sep 2025 11:03:50
vulnerability.cloud.eramba.org : 443 (tcp)	/css/font/Roboto-font/Roboto-Regular.ttf	03 Sep 2025 11:03:50
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/css/report-blocks-grid.css	03 Sep 2025 11:03:49
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/summernote/summernote.css	03 Sep 2025 11:03:49
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/css/bootstrap-colorpicker.css	03 Sep 2025 11:03:50
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/css/policy-document.css	03 Sep 2025 11:03:49
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/colors.css	03 Sep 2025 11:03:51
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/css/eramba.css	03 Sep 2025 11:03:51
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/jquery-upgrade/DataTables/ColReorder-1.5.2/js/dataTables.colReorder.min.js	03 Sep 2025 11:03:50
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/bootstrap.css	11 Oct 2025 01:31:58
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/css/core.css	14 Mar 2026 03:56:48
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/loaders/pace.min.js	07 Feb 2026 01:28:00
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/loaders/blockui.min.js	06 Dec 2025 02:52:18
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/jquery-upgrade/DataTables/Buttons-1.6.1/js/dataTables.buttons.min.js	11 Oct 2025 01:31:57
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/plugins/forms/styling/uniform.min.js	11 Apr 2026 03:29:18
vulnerability.cloud.eramba.org : 443 (tcp)	/vue_assets/index-CfD_x575.css	17 Apr 2026 07:55:55
vulnerability.cloud.eramba.org : 443 (tcp)	/eramba-assets/limitless_theme/js/core/libraries/bootstrap.min.js	11 Apr 2026 03:29:18