intruder

Vulnerability report

eramba

14 June 2025

1 target scanned

Executive summary

Threat Level

Low

Target	Issues
1	6

Critical	High
0	0

Medium	Low
0	6

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.

What we checked

Total checks

70,635

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'

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

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

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

What we checked

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

Common mistakes & misconfigurations

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

Issue summary

Cookie Missing HttpOnly Attribute
Low 1 occurrence

Cookie Missing SameSite Attribute
Low 1 occurrence

Error Page Information Disclosure
Low 1 occurrence

Missing Content-Security-Policy Header
Low 20 occurrences

Missing X-Content-Type-Options Header
Low 20 occurrences

Strict Transport Security HTTP Header Not Set
Low 1 occurrence

Severity Threshold

Cookie Missing HttpOnly Attribute

Low 1 occurrence

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	13 Jun 2025 12:23:37

Cookie Missing SameSite Attribute

Low 1 occurrence

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	13 Jun 2025 12:23:37

Error Page Information Disclosure

Low 1 occurrence

Description

When a user sends malformed requests, or attempts to visit pages which do not exist on the server, the server's response contains information which could be useful to an attacker in planning or executing an attack.
Certain information such as local directory paths, internal IP addresses, software versioning information and other detailed error output is valuable information to an attacker as it could assist them in the reconnaissance phase of an attack. If this type of information is made available to an attacker about a target, they are more likely to be successful in mounting a wide variety of attacks. Normal application users do not need to have access to this type of information and as such, access to it should be removed.

Remediation Advice

Where possible, the server should be configured with a custom error page which simply tells the user that an error has occurred. The page should not disclose any detailed information about the error, version information, or any information about the configuration of the server or its file system.
As an alternative, in some cases the software in use which produces this information can be configured to turn verbose error messages off. This option should also be considered.
For more information on how to create a custom error page, refer to the following documentation:
https://technet.microsoft.com/en-us/library/cc753103(v=ws.10).aspx
https://httpd.apache.org/docs/current/custom-error.html
http://nginx.org/en/docs/http/ngx_http_core_module.html#error_page

Occurrences	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	13 Jun 2025 12:23:41

Missing Content-Security-Policy Header

Low 20 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)	/assets	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/risks	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/data-asset-instances	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/security-policies	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/policy-exceptions	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/legals	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/business-units	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/risk-exceptions	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/security-services	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/robots.txt	13 Jun 2025 12:23:36
vulnerability.cloud.eramba.org : 443 (tcp)	/sitemap.xml	13 Jun 2025 12:23:36
vulnerability.cloud.eramba.org : 443 (tcp)	/login	13 Jun 2025 12:23:36
vulnerability.cloud.eramba.org : 443 (tcp)	/dashboard	13 Jun 2025 12:23:36
vulnerability.cloud.eramba.org : 443 (tcp)	/team-roles	13 Jun 2025 12:23:36
vulnerability.cloud.eramba.org : 443 (tcp)	/goals	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/program-scopes	13 Jun 2025 12:23:36
vulnerability.cloud.eramba.org : 443 (tcp)	/third-parties	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/program-issues	13 Jun 2025 12:23:37

Occurrences	Path	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	/business-continuity-plans	13 Jun 2025 12:23:37
vulnerability.cloud.eramba.org : 443 (tcp)	/service-contracts	13 Jun 2025 12:23:36

Missing X-Content-Type-Options Header

Low 20 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)	/js/jquery-upgrade/DataTables/ColReorder-1.5.2/js/dataTables.colReorder.min.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/js/jquery-upgrade/DataTables/Buttons-1.6.1/js/dataTables.buttons.min.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/js/jquery-upgrade/jquery-3.6.0.min.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/js/jquery-upgrade/jquery-ui.min.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/js/plugins/bootstrap-colorpicker/bootstrap-colorpicker.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/js/jquery-upgrade/DataTables/datatables.min.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/js/echarts.min.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/css/policy-document.css	13 Jun 2025 12:23:41
vulnerability.cloud.eramba.org : 443 (tcp)	/js/policy-document.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/css/fontawesome/font-awesome.min.css	13 Jun 2025 12:23:41
vulnerability.cloud.eramba.org : 443 (tcp)	/css/bootstrap.min.css	13 Jun 2025 12:23:41
vulnerability.cloud.eramba.org : 443 (tcp)	/js/plugins/nprogress/nprogress.js	14 Jun 2025 09:13:20
vulnerability.cloud.eramba.org : 443 (tcp)	/css/report-blocks-grid.css	13 Jun 2025 12:23:39
vulnerability.cloud.eramba.org : 443 (tcp)	/favicoı	13 Jun 2025 12:23:39
vulnerability.cloud.eramba.org : 443 (tcp)	/js/Yoo	13 Jun 2025 12:23:39
vulnerability.cloud.eramba.org : 443 (tcp)	/css/foı	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/css/erı	13 Jun 2025 12:23:39
vulnerability.cloud.eramba.org : 443 (tcp)	/vue_as	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/vue_assets/index-Xg0nX_J3.js	13 Jun 2025 12:23:40
vulnerability.cloud.eramba.org : 443 (tcp)	/css/bootstrap-colorpicker.css	13 Jun 2025 12:23:40

Strict Transport Security HTTP Header Not Set

Low 1 occurrence

Description

The server does not set a “Strict Transport Security” HTTP header in its response.

The HTTP Strict Transport Security policy defines a timeframe within which a browser must connect to the web server via HTTPS. The header adds additional protection against MitM (Man-in-the-Middle) attacks by instructing the user's web browser not to connect to the server unless it is done so over HTTPS with a valid certificate. This helps prevent an attacker in a MitM position from tricking the user into connecting to an attacker controlled server which is impersonating the targeted site.

Remediation Advice

Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]

The parameter max-age gives the time frame for requirement of HTTPS in seconds and is recommended to be set for at least several months, with 90 days being a minimum (ie. 7776000 seconds). The flag includeSubDomains defines that the policy should also apply for sub domains of the sender of the response.

For example, the following lines can be added to an Apache configuration file:

Header set Strict-Transport-Security "max-age=7776000"

Header append Strict-Transport-Security includeSubDomains

Occurrences	First seen
vulnerability.cloud.eramba.org : 443 (tcp)	13 Jun 2025 12:23:39

contact@intruder.io