Acunetix by Invicti

Comprehensive Report

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

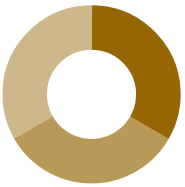
Scan Detail

Target	https://tmp-test-e.cloud.eramba.org
Scan Type	Full Scan
Start Time	Jan 15, 2024, 1:59:54 PM GMT
Scan Duration	1 hour, 9 minutes
Requests	103350
Average Response Time	63ms
Maximum Response Time	5787ms
Application Build	vnull
Authentication Profile	-

0	0	0	3	9
Critical	High	Medium	Low	Informational

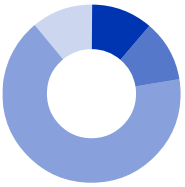
Severity	Vulnerabilities	Instances
Critical	0	0
High	0	0
Medium	0	0
Low	3	3
Informational	4	9
Total	7	12

Low Severity



	Instances
Cookies Not Marked as HttpOnly	1
Cookies with missing, inconsistent or contr...	1
Version Disclosure (PHP)	1

Informational



	Instances
Content Security Policy (CSP) Not Implem...	1
HTTP Strict Transport Security (HSTS) Erro...	1
Outdated JavaScript libraries	6
Others	1

Impacts

SEVERITY	IMPACT	
Low	1	Cookies Not Marked as HttpOnly
Low	1	Cookies with missing, inconsistent or contradictory properties
Low	1	Version Disclosure (PHP)
Informational	1	Content Security Policy (CSP) Not Implemented
Informational	1	HTTP Strict Transport Security (HSTS) Errors and Warnings
Informational	6	Outdated JavaScript libraries
Informational	1	Permissions-Policy header not implemented

Cookies Not Marked as HttpOnly

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

https://tmp-test-e.cloud.eramba.org/ Verified

Cookies without HttpOnly flag set:

- https://tmp-test-e.cloud.eramba.org/app-notification/app-notifications/check/0

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:35 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/app-notification/app-notifications/check/0

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:39 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/login

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:39 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/login

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 13:59:56 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/login

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:07 GMT; Max-
Age=31622396; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/settings/get-logo/black

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:02 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/dashboard

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:12 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/settings/get-logo/white

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:27 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/dashboard

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:01:00 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/login

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:21:58 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/dashboard

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:01:02 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:24:14 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/login

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:23:32 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:24:56 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:24:21 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/pages/license

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:27:39 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:28:35 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/users/change-language/1

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:29:51 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/settings/get-logo/

```
Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:29:58 GMT; Max-
Age=31622399; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/users/change-language/2

```
Set-Cookie: translation=2; expires=Wed, 15 Jan 2025 14:30:51 GMT; Max-
Age=31622400; path=/; secure
```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

```
Set-Cookie: translation=2; expires=Wed, 15 Jan 2025 14:30:58 GMT; Max-
Age=31622400; path=/; secure
```

Request

```
GET /app-notification/app-notifications/check/0 HTTP/1.1
Host: tmp-test-e.cloud.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: application/json, text/javascript, */*; q=0.01
accept-language: en-US
cookie: translation=1;
csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDViNzI%3D;
PHPSESSID=kvso975b56v9l95rq0rf2f62ps
x-requested-with: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://tmp-test-e.cloud.eramba.org/dashboard
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

https://tmp-test-e.cloud.eramba.org/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://tmp-test-e.cloud.eramba.org/app-notification/app-notifications/check/0

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:35 GMT; Max-Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/app-notification/app-notifications/check/0

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:39 GMT; Max-Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:39 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=b50110nesbk5osujtgd6122uaf; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 13:59:56 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie:
  csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDV
  iNzI%3D; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=deleted; expires=Thu, 01 Jan 1970 00:00:01 GMT; Max-Age=0;
  path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=kvso975b56v9l95rq0rf2f62ps; path=/; secure; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:07 GMT; Max-
  Age=31622396; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/settings/get-logo/black

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:02 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/dashboard

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:12 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://tmp-test-e.cloud.eramba.org/settings/get-logo/white

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:00:27 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/dashboard

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:01:00 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:21:58 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://tmp-test-e.cloud.eramba.org/dashboard

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:01:02 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:24:14 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:23:32 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:24:56 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:24:21 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://tmp-test-e.cloud.eramba.org/pages/license

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:27:39 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  ```

```
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://tmp-test-e.cloud.eramba.org/users/reset-password

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 15 Jan 2025 14:28:35 GMT; Max-
  Age=31622400; path=/; secure
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

Request

```
GET /app-notification/app-notifications/check/0 HTTP/1.1
Host: tmp-test-e.cloud.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: application/json, text/javascript, */*; q=0.01
accept-language: en-US
cookie: translation=1;
csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDViNzI%3D;
PHPSESSID=kvso975b56v9l95rq0rf2f62ps
x-requested-with: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://tmp-test-e.cloud.eramba.org/dashboard
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism
https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05

SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

https://tmp-test-e.cloud.eramba.org/

Version detected: **PHP/8.2.11**.

Recommendation

Configure your web server to prevent information leakage from its HTTP response.

References

PHP Documentation: header_remove()
https://www.php.net/manual/en/function.header-remove.php

PHP Documentation: php.ini directive expose_php
https://www.php.net/manual/en/ini.core.php#ini.expose-php

Content Security Policy (CSP) Not Implemented

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.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

https://tmp-test-e.cloud.eramba.org/

Paths without CSP header:

- https://tmp-test-e.cloud.eramba.org/login
- https://tmp-test-e.cloud.eramba.org/dashboard
- https://tmp-test-e.cloud.eramba.org/users/reset-password
- https://tmp-test-e.cloud.eramba.org/docs/
- https://tmp-test-e.cloud.eramba.org/img/
- https://tmp-test-e.cloud.eramba.org/media/
- https://tmp-test-e.cloud.eramba.org/pages/license
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/img/backgrounds/
- https://tmp-test-e.cloud.eramba.org/account-reviews/

- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/
- https://tmp-test-e.cloud.eramba.org/app-notification/
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/img/
- https://tmp-test-e.cloud.eramba.org/css/
- https://tmp-test-e.cloud.eramba.org/css/font/Roboto-font/
- https://tmp-test-e.cloud.eramba.org/css/font/
- https://tmp-test-e.cloud.eramba.org/users/change-language/
- https://tmp-test-e.cloud.eramba.org/awareness-programs/
- https://tmp-test-e.cloud.eramba.org/vendor-assessments/
- https://tmp-test-e.cloud.eramba.org/limitless_theme/
- https://tmp-test-e.cloud.eramba.org/limitless_theme/img/
- https://tmp-test-e.cloud.eramba.org/limitless_theme/img/backgrounds/

Request

```
GET /login?redirect=/ HTTP/1.1
Host: tmp-test-e.cloud.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
accept-language: en-US
upgrade-insecure-requests: 1
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

HTTP Strict Transport Security (HSTS) Errors and Warnings

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

https://tmp-test-e.cloud.eramba.org/

URLs where HSTS configuration is not according to best practices:

- https://tmp-test-e.cloud.eramba.org/login - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/dashboard - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/users/reset-password - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/docs/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/img/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/media/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/pages/license - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/img/backgrounds/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/account-reviews/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/app-notification/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/img/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/css/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/css/font/Roboto-font/ - No includeSubDomains directive

- https://tmp-test-e.cloud.eramba.org/css/font/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/users/change-language/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/awareness-programs/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/vendor-assessments/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/limitless_theme/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/limitless_theme/img/ - No includeSubDomains directive
- https://tmp-test-e.cloud.eramba.org/limitless_theme/img/backgrounds/ - No includeSubDomains directive

Request

```
GET /login?redirect=/ HTTP/1.1
Host: tmp-test-e.cloud.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
accept-language: en-US
upgrade-insecure-requests: 1
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
```

Recommendation

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.

References

hstspreload.org
https://hstspreload.org/

MDN: Strict-Transport-Security
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

https://tmp-test-e.cloud.eramba.org/ Confidence: 95%

- Select2 4.0.3
  - URL: https://tmp-test-e.cloud.eramba.org/limitless_theme/js/plugins/forms/selects/select2.min.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/select2/select2/tags

Request

```
GET /limitless_theme/js/plugins/forms/selects/select2.min.js HTTP/1.1
Cookie: translation=1;
csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDViNzI%3D;
PHPSESSID=kvso975b56v9l95rq0rf2f62ps
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
Host: tmp-test-e.cloud.eramba.org
Connection: Keep-alive
```

https://tmp-test-e.cloud.eramba.org/ Confidence: 95%

- bootstrap.js 3.4.1
  - URL: https://tmp-test-e.cloud.eramba.org/login
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request

```
GET /login?redirect=/ HTTP/1.1
Host: tmp-test-e.cloud.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
```

```
lication/signed-exchange;v=b3;q=0.7
accept-language: en-US
upgrade-insecure-requests: 1
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
```

https://tmp-test-e.cloud.eramba.org/ Confidence: 95%

- DataTables 1.10.20
  - URL: https://tmp-test-e.cloud.eramba.org/dashboard
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/DataTables/DataTables/tags

Request

```
GET /dashboard HTTP/1.1
Host: tmp-test-e.cloud.eramba.org
Pragma: no-cache
Cache-Control: no-cache
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
accept-language: en-US
upgrade-insecure-requests: 1
Referer: https://tmp-test-e.cloud.eramba.org/login?redirect=%2F
Accept-Encoding: gzip,deflate,br
Cookie: translation=1;
csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDViNzI%3D;
PHPSESSID=kvso975b56v9l95rq0rf2f62ps
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
```

https://tmp-test-e.cloud.eramba.org/ Confidence: 95%

- DataTables 1.6.1

- URL: https://tmp-test-e.cloud.eramba.org/js/jquery-upgrade/DataTables/Buttons-1.6.1/js/dataTables.buttons.min.js
- Detection method: The library's name and version were determined based on the file's contents.
- References:
  - https://github.com/DataTables/DataTables/tags

Request

```
GET /js/jquery-upgrade/DataTables/Buttons-1.6.1/js/dataTables.buttons.min.js HTTP/1.1
Cookie: translation=1;
csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDViNzI%3D;
PHPSESSID=b50110nesbk5osujtgd6122uaf; sidebarExpanded=true
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
Host: tmp-test-e.cloud.eramba.org
Connection: Keep-alive
```

https://tmp-test-e.cloud.eramba.org/ Confidence: 95%

- **DataTables 1.10.8**
  - URL: https://tmp-test-e.cloud.eramba.org/js/jquery-upgrade/DataTables/ColReorder-1.5.2/js/dataTables.colReorder.min.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/DataTables/DataTables/tags

Request

```
GET /js/jquery-upgrade/DataTables/ColReorder-1.5.2/js/dataTables.colReorder.min.js HTTP/1.1
Cookie: translation=1;
csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDViNzI%3D;
PHPSESSID=b50110nesbk5osujtgd6122uaf; sidebarExpanded=true
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
Host: tmp-test-e.cloud.eramba.org
Connection: Keep-alive
```

https://tmp-test-e.cloud.eramba.org/ Confidence: 95%

- **DataTables 1.3.1**
  - URL: https://tmp-test-e.cloud.eramba.org/js/jquery-upgrade/DataTables/datatables.min.js

- Detection method: The library's name and version were determined based on the file's contents.
- References:
  - https://github.com/DataTables/DataTables/tags

Request

```
GET /js/jquery-upgrade/DataTables/datatables.min.js HTTP/1.1
Cookie: translation=1;
csrfToken=0xtsz0RQXquYQ1ACbM4vZDYzYmNkYTM0MjYyZjA5OGI5MGRkNWE4MzBiOWVlNGEyZmQ1NDViNzI%3D;
PHPSESSID=b50110nesbk5osujtgd6122uaf; sidebarExpanded=true
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
Host: tmp-test-e.cloud.eramba.org
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

https://tmp-test-e.cloud.eramba.org/

Locations without Permissions-Policy header:

- https://tmp-test-e.cloud.eramba.org/login
- https://tmp-test-e.cloud.eramba.org/dashboard
- https://tmp-test-e.cloud.eramba.org/users/reset-password
- https://tmp-test-e.cloud.eramba.org/docs/
- https://tmp-test-e.cloud.eramba.org/img/
- https://tmp-test-e.cloud.eramba.org/media/
- https://tmp-test-e.cloud.eramba.org/pages/license
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/img/backgrounds/
- https://tmp-test-e.cloud.eramba.org/account-reviews/
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/
- https://tmp-test-e.cloud.eramba.org/app-notification/
- https://tmp-test-e.cloud.eramba.org/LimitlessTheme/img/

- https://tmp-test-e.cloud.eramba.org/css/
- https://tmp-test-e.cloud.eramba.org/css/font/Roboto-font/
- https://tmp-test-e.cloud.eramba.org/css/font/
- https://tmp-test-e.cloud.eramba.org/users/change-language/
- https://tmp-test-e.cloud.eramba.org/awareness-programs/
- https://tmp-test-e.cloud.eramba.org/vendor-assessments/
- https://tmp-test-e.cloud.eramba.org/limitless_theme/
- https://tmp-test-e.cloud.eramba.org/limitless_theme/img/
- https://tmp-test-e.cloud.eramba.org/limitless_theme/img/backgrounds/

Request

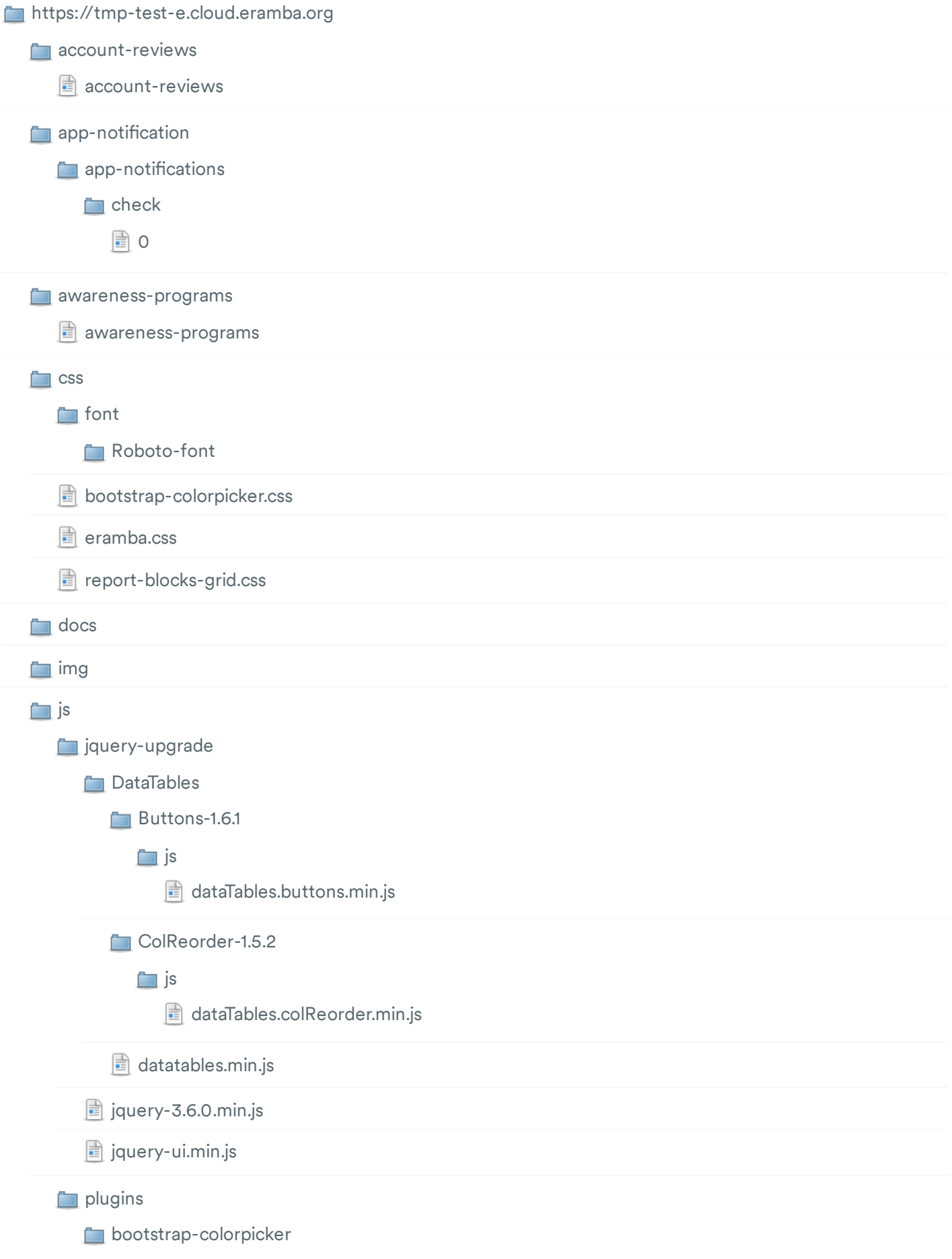
```
GET /login?redirect=/ HTTP/1.1
Host: tmp-test-e.cloud.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.7
accept-language: en-US
upgrade-insecure-requests: 1
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
```

References

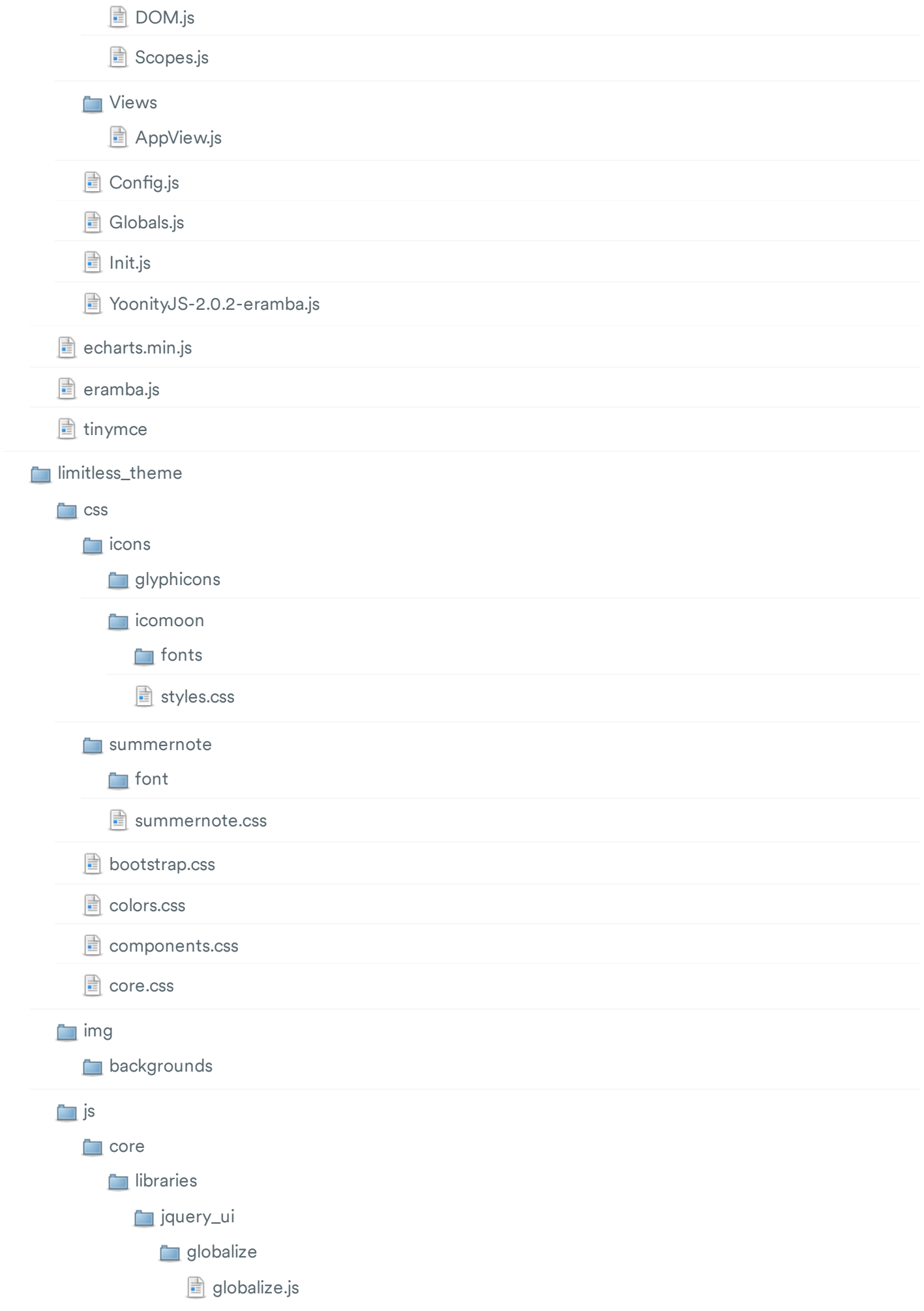
Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

Coverage


https://tmp-test-e.cloud.eramba.org
account-reviews
account-reviews
app-notification
app-notifications
check
0
awareness-programs
awareness-programs
css
font
Roboto-font
bootstrap-colorpicker.css
eramba.css
report-blocks-grid.css
docs
img
js
jquery-upgrade
DataTables
Buttons-1.6.1
js
dataTables.buttons.min.js
ColReorder-1.5.2
js
dataTables.colReorder.min.js
datatables.min.js
jquery-3.6.0.min.js
jquery-ui.min.js
plugins
bootstrap-colorpicker

- bootstrap-colorpicker.js
- nprogress
  - nprogress.js
- YoonityJS
  - Controllers
    - AppController.js
    - AppNotificationController.js
    - CrudController.js
    - ErambaController.js
  - Errors
    - ExceptionRenderer.js
    - Exceptions.js
  - Libs
    - Controller.js
    - Model.js
    - Object.js
    - View.js
  - Models
    - AppModel.js
  - Registry
    - Forms.js
    - Loaders.js
    - Modals.js
    - Notifications.js
    - Registry.js
    - Request.js
    - Response.js
    - Server.js
    - ServerRequest.js
    - ServerResponse.js
    - Templates.js
  - Resources
    - Class.js


DOM.js
Scopes.js
Views
AppView.js
Config.js
Globals.js
Init.js
YoonityJS-2.0.2-eramba.js
echarts.min.js
eramba.js
tinymce
limitless_theme
css
icons
glyphicons
icomoon
fonts
styles.css
summernote
font
summernote.css
bootstrap.css
colors.css
components.css
core.css
img
backgrounds
js
core
libraries
jquery_ui
globalize
globalize.js

- bootstrap.min.js
- app.js
- pages
  - components_popups.js
  - datatables_basic.js
- plugins
  - buttons
    - ladda.min.js
    - spin.min.js
  - editors
    - summernote
      - summernote.min.js
  - extensions
    - mousewheel.min.js
  - forms
    - selects
      - select2.min.js
    - styling
      - switch.min.js
      - switchery.min.js
      - uniform.min.js
    - wizards
      - steps.min.js
  - loaders
    - blockui.min.js
    - pace.min.js
  - notifications
    - pnotify.min.js
    - sweet_alert.min.js
  - pickers
    - color
      - spectrum.js
  - uploaders

- dropzone.min.js
- velocity
  - velocity.min.js
  - velocity.ui.min.js
- LimitlessTheme
  - img
    - backgrounds
- media
- pages
  - license
- settings
  - get-logo
    - black
    - white
- users
  - change-language
    - 1
    - 2
    - 3
    - 4
    - 5
  - reset-password
    - Inputs
      - POST _Token[fields], _Token[unlocked], _csrfToken, email
      - POST redirect
      - POST _csrfToken, email, _Token[fields], _Token[unlocked]
      - GET redirect
- vendor-assessments
  - vendor-assessments
- about
- assets
- business-continuities
- business-continuity-plans

- business-units
- compliance-analysis-findings
- compliance-exceptions
- compliance-managements
- compliance-package-regulators
- dashboard
  - Inputs
    - GET _, reload, resetCache
- data-asset-instances
- goals
- legals
- login
  - Inputs
    - POST _csrfToken, login, password, _Token[fields], _Token[unlocked]
    - POST _Token[fields], _Token[unlocked], _csrfToken, login, password
    - POST redirect
    - GET expireCsrfCookie, redirect
- logout
- policy-exceptions
- program-issues
- program-scopes
- projects
- risk-exceptions
- risks
- security-incidents
- security-policies
- security-services
- service-contracts
- settings
- team-roles
- third-parties