Acunetix
by Invicti

Comprehensive Report

Acunetix Threat Level 1

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

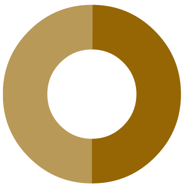
Scan Detail

Target	https://acunetix.eramba.org/
Scan Type	Full Scan
Start Time	Apr 23, 2024, 11:27:13 AM GMT
Scan Duration	3 hours, 25 minutes
Requests	74629
Average Response Time	64ms
Maximum Response Time	30000ms
Application Build	vnull
Authentication Profile	-

0	0	0	2	5
Critical	High	Medium	Low	Informational

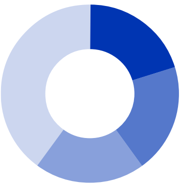
Severity	Vulnerabilities	Instances
Critical	0	0
High	0	0
Medium	0	0
Low	2	2
Informational	5	5
Total	7	7

Low Severity



	Instances
■ Cookies Not Marked as HttpOnly	1
■ Cookies with missing, inconsistent or contr...	1

Informational



	Instances
■ Access-Control-Allow-Origin header with ...	1
■ Content Security Policy (CSP) Not Implem...	1
■ HTTP Strict Transport Security (HSTS) Erro...	1
■ Others	2

Impacts

SEVERITY	IMPACT	
Low	1	Cookies Not Marked as HttpOnly
Low	1	Cookies with missing, inconsistent or contradictory properties
Informational	1	Access-Control-Allow-Origin header with wildcard (*) value
Informational	1	Content Security Policy (CSP) Not Implemented
Informational	1	HTTP Strict Transport Security (HSTS) Errors and Warnings
Informational	1	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://acunetix.eramba.org/ Verified

Cookies without HttpOnly flag set:

- https://acunetix.eramba.org/login

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:27:15 GMT; Max-Age=31536000; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document/24

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:32:53 GMT; Max-Age=31535999; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document/24

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:33:51 GMT; Max-Age=31535999; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document/24

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:33:52 GMT; Max-Age=31535999; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document-pdf/29

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:35:14 GMT; Max-Age=31535998; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document/30

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:28:14 GMT; Max-Age=31536000; path=/; secure
  ```

- https://acunetix.eramba.org/portal/policy/document/34

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:37:16 GMT; Max-Age=31535999; path=/; secure
  ```

- https://acunetix.eramba.org/portal/policy/document-pdf/25

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:39:04 GMT; Max-Age=31535998; path=/; secure
  ```

- https://acunetix.eramba.org/portal/policy/document/35

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:39:58 GMT; Max-Age=31536000; path=/; secure
  ```

- https://acunetix.eramba.org/portal/policy/document-pdf/31

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:42:37 GMT; Max-Age=31535997; path=/; secure
  ```

- https://acunetix.eramba.org/portal/policy/document/30

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:43:48 GMT; Max-Age=31536000; path=/; secure
  ```

- https://acunetix.eramba.org/login

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:43:21 GMT; Max-Age=31536000; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document-pdf/30

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:44:15 GMT; Max-Age=31535998; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document-pdf/22

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:44:30 GMT; Max-Age=31535997; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document/26

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:44:22 GMT; Max-Age=31536000; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document-pdf/26

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:45:12 GMT; Max-Age=31535998; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document/27

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:46:06 GMT; Max-Age=31535999; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/login

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:46:22 GMT; Max-Age=31536000; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document/30

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:46:30 GMT; Max-
Age=31536000; path=/; secure
```

- https://acunetix.eramba.org/settings/get-logo/login

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:27:19 GMT; Max-
Age=31536000; path=/; secure
```

- https://acunetix.eramba.org/portal/policy/document-pdf/27

```
Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:46:15 GMT; Max-
Age=31535997; path=/; secure
```

Request

```
GET /login?redirect=/ HTTP/1.1
Host: acunetix.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/121.0.0.0 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://acunetix.eramba.org/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://acunetix.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:27:15 GMT; Max-
  Age=31536000; 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://acunetix.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie:
  csrfToken=Q0COsl9LuL0iYNhBFvtedDkzMGY2NDQ4OGYyZDAzYWQ3MGZiNGM1NDE2YTgzYzI3ZTMxYmY
  xMTM%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://acunetix.eramba.org/portal/policy/document/24

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:32:53 GMT; Max-Age=31535999; 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://acunetix.eramba.org/portal/policy/document/24

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:33:51 GMT; Max-Age=31535999; 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://acunetix.eramba.org/portal/policy/document/24

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:33:52 GMT; Max-Age=31535999; 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://acunetix.eramba.org/portal/policy/document-pdf/29

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:35:14 GMT; Max-Age=31535998; 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://acunetix.eramba.org/portal/policy/document/30

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:28:14 GMT; Max-Age=31536000; 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://acunetix.eramba.org/portal/policy/document/34

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:37:16 GMT; Max-Age=31535999; 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://acunetix.eramba.org/portal/policy/document-pdf/25

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:39:04 GMT; Max-Age=31535998; 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://acunetix.eramba.org/portal/policy/document/35

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:39:58 GMT; Max-Age=31536000; 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://acunetix.eramba.org/portal/policy/document-pdf/31

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:42:37 GMT; Max-Age=31535997; 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://acunetix.eramba.org/portal/policy/document/30

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:43:48 GMT; Max-
  Age=31536000; 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://acunetix.eramba.org/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:43:21 GMT; Max-
  Age=31536000; 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://acunetix.eramba.org/portal/policy/document-pdf/30

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:44:15 GMT; Max-
  Age=31535998; 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://acunetix.eramba.org/portal/policy/document-pdf/22

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:44:30 GMT; Max-
  Age=31535997; 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://acunetix.eramba.org/portal/policy/document/26

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:44:22 GMT; Max-
  Age=31536000; 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://acunetix.eramba.org/portal/policy/document-pdf/26

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:45:12 GMT; Max-
  Age=31535998; 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://acunetix.eramba.org/portal/policy/document/27

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:46:06 GMT; Max-Age=31535999; 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://acunetix.eramba.org/portal/policy/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:46:22 GMT; Max-Age=31536000; 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://acunetix.eramba.org/portal/policy/document/30

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:46:30 GMT; Max-Age=31536000; 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://acunetix.eramba.org/settings/get-logo/login

  Cookie was set with:

  ```
  Set-Cookie: translation=1; expires=Wed, 23 Apr 2025 11:27:19 GMT; Max-
  Age=31536000; 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 /login?redirect=/ HTTP/1.1
Host: acunetix.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/121.0.0.0 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

Access-Control-Allow-Origin header with wildcard (*) value

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHTTPRequest) requests to the site and access the responses.

Impact

Any website can make XHR requests to the site and access the responses.

https://acunetix.eramba.org/

Affected paths (max. 25):

- /system-api/users/change-translation
- /system-api/login
- /system-api/users/info

Request

```
GET /system-api/users/change-translation HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: application/json
accept-language: en-US
cookie: translation=1;
csrfToken=Q0COsl9LuL0iYNhBFvtedDkzMGY2NDQ4OGYyZDAzYWQ3MGZiNGM1NDE2YTgzYzI3ZTMxYmYxMTM%3D
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
```

```
Referer: https://acunetix.eramba.org/login?redirect=%2F
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/121.0.0.0 Safari/537.36
```

Recommendation

Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.

References

Test Cross Origin Resource Sharing (OTG-CLIENT-007)
https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007)

Cross-origin resource sharing
https://en.wikipedia.org/wiki/Cross-origin_resource_sharing

Cross-Origin Resource Sharing
http://www.w3.org/TR/cors/

CrossOriginRequestSecurity
https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity

Cross-Origin Resource Sharing (CORS) and the Access-Control-Allow-Origin Header
https://www.acunetix.com/blog/web-security-zone/cross-origin-resource-sharing-cors-access-control-allow-origin-header/

PortSwigger Research on CORS misconfiguration
https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties

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://acunetix.eramba.org/

Paths without CSP header:

- https://acunetix.eramba.org/login
- https://acunetix.eramba.org/portal/policy/document/24
- https://acunetix.eramba.org/portal/policy/document/32
- https://acunetix.eramba.org/portal/policy/document/35
- https://acunetix.eramba.org/limitless_theme/css/icons/icomoon/fonts/
- https://acunetix.eramba.org/portal/policy/document/33
- https://acunetix.eramba.org/portal/policy/document/25
- https://acunetix.eramba.org/css/font/
- https://acunetix.eramba.org/portal/policy/document/34
- https://acunetix.eramba.org/limitless_theme/img/
- https://acunetix.eramba.org/portal/policy/document/31
- https://acunetix.eramba.org/portal/policy/document-pdf/29
- https://acunetix.eramba.org/portal/policy/document-pdf/24
- https://acunetix.eramba.org/vue_assets/
- https://acunetix.eramba.org/portal/policy/document/30

- https://acunetix.eramba.org/portal/policy
- https://acunetix.eramba.org/portal/policy/document-pdf/25
- https://acunetix.eramba.org/css/font/Roboto-font/
- https://acunetix.eramba.org/fonts/
- https://acunetix.eramba.org/portal/policy/document/22
- https://acunetix.eramba.org/LimitlessTheme/img/backgrounds/

Request

```
GET /login?redirect=/ HTTP/1.1
Host: acunetix.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/121.0.0.0 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://acunetix.eramba.org/

URLs where HSTS configuration is not according to best practices:

- https://acunetix.eramba.org/login - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/24 - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/32 - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/35 - No includeSubDomains directive
- https://acunetix.eramba.org/limitless_theme/css/icons/icomoon/fonts/ - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/33 - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/25 - No includeSubDomains directive
- https://acunetix.eramba.org/css/font/ - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/34 - No includeSubDomains directive
- https://acunetix.eramba.org/limitless_theme/img/ - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/31 - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document-pdf/29 - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document-pdf/24 - No includeSubDomains directive
- https://acunetix.eramba.org/vue_assets/ - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/30 - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document-pdf/25 - No includeSubDomains directive
- https://acunetix.eramba.org/css/font/Roboto-font/ - No includeSubDomains directive
- https://acunetix.eramba.org/fonts/ - No includeSubDomains directive
- https://acunetix.eramba.org/portal/policy/document/22 - No includeSubDomains directive
- https://acunetix.eramba.org/LimitlessTheme/img/backgrounds/ - No includeSubDomains directive

Request

```
GET /login?redirect=/ HTTP/1.1
Host: acunetix.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/121.0.0.0 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://acunetix.eramba.org/ Confidence: 95%

- **Bootbox 4.0.0**
  - URL: https://acunetix.eramba.org/js/plugins/bootbox/bootbox.min.js
  - Detection method: The library's name and version were determined based on the file's contents.

  - References:
    - https://github.com/makeusabrew/bootbox/tags

Request

```
GET /js/plugins/bootbox/bootbox.min.js HTTP/1.1
Cookie: translation=1;
csrfToken=Q0COsl9LuL0iYNhBFvtedDkzMGY2NDQ4OGYyZDAzYWQ3MGZiNGM1NDE2YTgzYzI3ZTMxYmYxMTM%3D
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/121.0.0.0 Safari/537.36
Host: acunetix.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://acunetix.eramba.org/

Locations without Permissions-Policy header:

- https://acunetix.eramba.org/login
- https://acunetix.eramba.org/portal/policy/document/24
- https://acunetix.eramba.org/portal/policy/document/32
- https://acunetix.eramba.org/portal/policy/document/35
- https://acunetix.eramba.org/limitless_theme/css/icons/icomoon/fonts/
- https://acunetix.eramba.org/portal/policy/document/33
- https://acunetix.eramba.org/portal/policy/document/25
- https://acunetix.eramba.org/css/font/
- https://acunetix.eramba.org/portal/policy/document/34
- https://acunetix.eramba.org/limitless_theme/img/
- https://acunetix.eramba.org/portal/policy/document/31
- https://acunetix.eramba.org/portal/policy/document-pdf/29
- https://acunetix.eramba.org/portal/policy/document-pdf/24

- https://acunetix.eramba.org/vue_assets/
- https://acunetix.eramba.org/portal/policy/document/30
- https://acunetix.eramba.org/portal/policy
- https://acunetix.eramba.org/portal/policy/document-pdf/25
- https://acunetix.eramba.org/css/font/Roboto-font/
- https://acunetix.eramba.org/fonts/
- https://acunetix.eramba.org/portal/policy/document/22
- https://acunetix.eramba.org/LimitlessTheme/img/backgrounds/

Request

```
GET /login?redirect=/ HTTP/1.1
Host: acunetix.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/121.0.0.0 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://acunetix.eramba.org
  - css
    - font
      - Montserrat-font
      - Roboto-font
    - fontawesome
      - font-awesome.min.css
    - bootstrap.min.css
    - eramba.css
    - policy-document.css
    - policy.css
    - report-blocks-grid.css
  - docs
  - fonts
  - img
  - js
    - jquery-upgrade
      - jquery-3.6.0.min.js
      - jquery-ui.min.js
    - plugins
      - bootbox
        - bootbox.min.js
      - nprogress
        - nprogress.js
      - slimscroll
        - jquery.slimscroll.min.js
    - YoonityJS
      - YoonityJS-2.0.2-eramba.js
    - bootstrap.min.js
    - eramba.js
    - policy-document.js

```
    tinymce
limitless_theme
    css
        icons
            glyphicons
            icomoon
                fonts
                styles.css
        bootstrap.css
        colors.css
        components.css
        core.css
    img
        backgrounds
    js
        plugins
            notifications
                pnotify.min.js
LimitlessTheme
    img
        backgrounds
locales
    en
        translation.json
media
pages
    license
portal
    policy
        Inputs
            GET policy_search
        document-pdf
            22
            24
```

- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35

- document
  - 22
    - Inputs
      - GET policy_search
  - 24
    - Inputs
      - GET policy_search
  - 25
    - Inputs
      - GET policy_search
  - 26
    - Inputs
      - GET policy_search
  - 27
    - Inputs
      - GET policy_search
  - 28
    - Inputs
      - GET policy_search
  - 29
    - Inputs
      - GET policy_search

                    - 30
                        - Inputs
                            - GET policy_search
                    - 31
                        - Inputs
                            - GET policy_search
                    - 32
                        - Inputs
                            - GET policy_search
                    - 33
                        - Inputs
                            - GET policy_search
                    - 34
                        - Inputs
                            - GET policy_search
                    - 35
                        - Inputs
                            - GET policy_search
                - login
                    - Inputs
                        - GET redirect
            - policy
                - Inputs
                    - GET policy_search
        - settings
            - get-logo
                - login
                - white
        - system-api
            - users
                - change-translation
                - info
            - login

    - Inputs
        - POST login, password

- vue_assets
    - FormButtonField.vue_vue_type_script_setup_true_lang-sOoOlkSu.js
    - FormTextField.vue_vue_type_script_setup_true_lang-6DQKRJo6.js
    - index-oQ4yA2-7.js
    - index-SDils33E.css
    - LanguageSelect.vue_vue_type_script_setup_true_lang-uah_O2xp.js
    - LicenseLabel.vue_vue_type_script_setup_true_lang-kuNCWeA0.js
    - LoginView-WC0A6EhE.js
    - PasswordResetView-T_5yFjGk.js
    - SetupNavbar.vue_vue_type_script_setup_true_lang-iPlsTVJj.js
- index.html
- login
    - Inputs
        - GET portal, redirect, login, password, submit
- password-reset
- set-password
- welcome