Acunetix by Invicti

Comprehensive Report

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

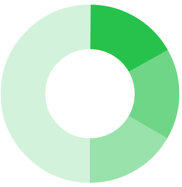
Scan Detail

Target	homeocureusa.ssbmultiservices.com
Scan Type	Full Scan
Start Time	Jan 7, 2024, 12:29:33 PM GMT+8
Scan Duration	7 minutes
Requests	3604
Average Response Time	45ms
Maximum Response Time	9454ms
Application Build	v23.7.230728157

0	3	5	6
High	Medium	Low	Informational

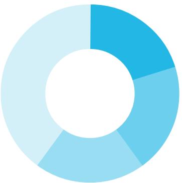
Severity	Vulnerabilities	Instances
High	0	0
Medium	3	3
Low	5	5
Informational	6	6
Total	14	14

Informational



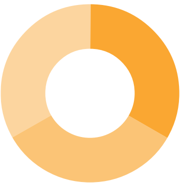
		Instances
🟩	Content Security Policy (CSP) not implement…	1
🟩	Email addresses	1
🟩	Outdated JavaScript libraries	1
🟩	Others	3

Low Severity



		Instances
🟦	Clickjacking: X-Frame-Options header	1
🟦	Cookies without HttpOnly flag set	1
🟦	Cookies without Secure flag set	1
🟦	Others	2

Medium Severity



		Instances
🟧	Laravel debug mode enabled	1
🟧	Laravel log file publicly accessible	1
🟧	Vulnerable JavaScript libraries	1

Impacts

SEVERITY	IMPACT	
Medium	1	Laravel debug mode enabled
Medium	1	Laravel log file publicly accessible
Medium	1	Vulnerable JavaScript libraries
Low	1	Clickjacking: X-Frame-Options header
Low	1	Cookies without HttpOnly flag set
Low	1	Cookies without Secure flag set
Low	1	HTTP Strict Transport Security (HSTS) not implemented
Low	1	Insecure Inline Frame (iframe)
Informational	1	Content Security Policy (CSP) not implemented
Informational	1	Email addresses
Informational	1	Outdated JavaScript libraries
Informational	1	Permissions-Policy header not implemented
Informational	1	Reverse proxy detected
Informational	1	Subresource Integrity (SRI) not implemented

Laravel debug mode enabled

The web application uses Laravel framework. Laravel Debug mode is enabled. Debug mode should be turned off in production environment, as it leads to disclosure of sensitive information about the web application.

Impact

The web application in debug mode discloses sensitive information. This information can be used to launch further attacks.

https://homeocureusa.ssbmultiservices.com/

Request

```
PUT /index.php HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6IkFkcGgzVTlmd1A4bFpHOGs1SElXenc9PSIsInZhbHVlIjoiODVPRXFXQ0Zab3gyMjgyRDZGQWZuREdTUTNNaH
hnS3cxWDFnWWJSSlBSUzIvMGZodkFWMFM4L2hvR3dDYzRjN3BmZ2RVWlpOcEV4alUxM3RwWFdTWUpLSXpGQVY4MmxmY1hvL2d1OH
Jaa1Bsb05ZdmdGeFJ4MDJpaFAyUzNpemQiLCJtYWMiOiJjNjRlOGYyYjZjNWUwZjQxZWQyN2MyOGU4Y2IyZmEwZTMyNzdjYjZiNj
UxMzY3NWQ5YzViZTNhN2FkMDY4ZjdjIn0%3D;
sk_sharma_session=eyJpdiI6InFyM2s2dnFwUS9UTTdRMDZlTWNqdUE9PSIsInZhbHVlIjoianlUUHhJak1hSko2RkpyMVd5dE
JsSHRtdjZ0ODA4VG92TGJhaXlxV1ZMYXVxb1kvTWtUNyt5aHBZZE5LRW1wOFJkQVdpMHhiUDEzenJzeDNiUUhGQ0JvVnZlajdFa2
xJQnQ0TTQ1eEkyV3dESUlrN0hKclg4UHhwQ05GdTIvS1YiLCJtYWMiOiJhZTRjNzk0MjVhYTgzNWNjOWQzOWIzOGIzYzg4YzU2Ym
U0YTUwZTg1MTdiOWQ5MjMyY2QzZWFkMzgxOGIyODgwIn0%3D
Content-Length: 0
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Disable the debug mode by setting APP_DEBUG to false

References

Error Handling

https://laravel.com/docs/7.x/errors#configuration

Laravel log file publicly accessible

Laravel is a popular PHP web application framework. A publicly accessble Laravel log file (**/storage/logs/laravel.log**) was found in this directory.

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

Impact

The Laravel log file may disclose sensitive information. This information can be used to launch further attacks.

https://homeocureusa.ssbmultiservices.com/

Request

```
GET /storage/logs/laravel.log HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6IkFkcGgzVTlmd1A4bFpHOGs1SElXenc9PSIsInZhbHVlIjoiODVPRXFXQ0Zab3gyMjgyRDZGQWZuREdTUTNNaH
hnS3cxWDFnWWJSSlBSUzIvMGZodkFWMFM4L2hvR3dDYzRjN3BmZ2RVWlpOcEV4alUxM3RwWFdTWUpLSXpGQVY4MmxmY1hvL2d1OH
Jaa1Bsb05ZdmdGeFJ4MDJpaFAyUzNpemQiLCJtYWMiOiJjNjRlOGYyYjZjNWUwZjQxZWQyN2MyOGU4Y2IyZmEwZTMyNzdjYjZiNj
UxMzY3NWQ5YzViZTNhN2FkMDY4ZjdjIn0%3D;
sk_sharma_session=eyJpdiI6InFyM2s2dnFwUS9UTTdRMDZlTWNqdUE9PSIsInZhbHVlIjoianlUUHhJak1hSko2RkpyMVd5dE
JsSHRtdjZ0ODA4VG92TGJhaXlxV1ZMYXVxb1kvTWtUNyt5aHBZZE5LRW1wOFJkQVdpMHhiUDEzenJzeDNiUUhGQ0JvVnZlajdFa2
xJQnQ0TTQ1eEkyV3dESUlrN0hKclg4UHhwQ05GdTIvS1YiLCJtYWMiOiJhZTRjNzk0MjVhYTgzNWNjOWQzOWIzOGIzYzg4YzU2Ym
U0YTUwZTg1MTdiOWQ5MjMyY2QzZWFkMzgxOGIyODgwIn0%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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Remove or restrict access from the internet to this type of files.

References

Laravel Logging
https://laravel.com/docs/5.6/logging

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

https://homeocureusa.ssbmultiservices.com/ Confidence: 95%

- **jQuery 3.4.1**
  - URL: https://homeocureusa.ssbmultiservices.com/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

https://homeocureusa.ssbmultiservices.com/

Paths without secure XFO header:

- https://homeocureusa.ssbmultiservices.com/

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Clickjacking
https://en.wikipedia.org/wiki/Clickjacking

OWASP Clickjacking
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Frame Buster Buster
https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed

Cookies without HttpOnly flag set

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://homeocureusa.ssbmultiservices.com/ Verified

Cookies without HttpOnly flag set:

- https://homeocureusa.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkFkcGgzVTlmd1A4bFpHOGs1SElXenc9PSIsInZhbHVlIjoiODVPRXFXQ0Zab3gyMjg
yRDZGQWZuREdTUTNNaHhnS3cxWDFnWWJSSlBSUzIvMGZodkFWMFM4L2hvR3dDYzRjN3BmZ2RVWlpOcEV4
alUxM3RwWFdTWUpLSXpGQVY4MmxmY1hvL2d1OHJaa1Bsb05ZdmdGeFJ4MDJpaFAyUzNpemQiLCJtYWMiO
iJjNjRlOGYyYjZjNWUwZjQxZWQyN2MyOGU4Y2IyZmEwZTMyNzdjYjZiNjUxMzY3NWQ5YzViZTNhN2FkMD
Y4ZjdjIn0%3D; expires=Sun, 07-Jan-2024 06:30:04 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://homeocureusa.ssbmultiservices.com/contact-mail

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IktxckN0VUNkZCtHSTJIVEhzUHRWS1E9PSIsInZhbHVlIjoiM2pRbWFXZHl5Tk5SdEl
ZZC8vay8raXNsVHVsUGluNFFNcHptZVNyNk14SzQyRjdicmpNa2JwdDhuSENia0I5L2wrT2NDdlpoU1hX
VWdGd1lTcmpKd2lBdVpmMy94R3FCd0QzeEt2UWw5RnJaVXFFWGdLenF1TUFoanNUVjNQK00iLCJtYWMiO
iJhOTcxY2M0Y2YzZmVlYzBhYjU3NTUxMjkxNTQ3YjQ5N2MwYWE3M2E1YWE4NGU2YjczYjVjZjAzODA5ZT
llMzA3In0%3D; expires=Sun, 07-Jan-2024 06:31:20 GMT; Max-Age=7200; path=/;
samesite=lax
```

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

https://homeocureusa.ssbmultiservices.com/ Verified

Cookies without Secure flag set:

- https://homeocureusa.ssbmultiservices.com/

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkFkcGgzVTlmd1A4bFpHOGs1SElXenc9PSIsInZhbHVlIjoiODVPRXFXQ0Zab3gyMjg
yRDZGQWZuREdTUTNNaHhnS3cxWDFnWWJSSlBSUzIvMGZodkFWMFM4L2hvR3dDYzRjN3BmZ2RVWlpOcEV4
alUxM3RwWFdTWUpLSXpGQVY4MmxmY1hvL2d1OHJaa1Bsb05ZdmdGeFJ4MDJpaFAyUzNpemQiLCJtYWMiO
iJjNjRlOGYyYjZjNWUwZjQxZWQyN2MyOGU4Y2IyZmEwZTMyNzdjYjZiNjUxMzY3NWQ5YzViZTNhN2FkMD
Y4ZjdjIn0%3D; expires=Sun, 07-Jan-2024 06:30:04 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://homeocureusa.ssbmultiservices.com/

```
Set-Cookie:
sk_sharma_session=eyJpdiI6InFyM2s2dnFwUS9UTTdRMDZlTWNqdUE9PSIsInZhbHVlIjoianlUUHh
Jak1hSko2RkpyMVd5dEJsSHRtdjZ0ODA4VG92TGJhaXlxV1ZMYXVxb1kvTWtUNyt5aHBZZE5LRW1wOFJk
QVdpMHhiUDEzenJzeDNiUUhGQ0JvVnZlajdFa2xJQnQ0TTQ1eEkyV3dESUlrN0hKclg4UHhwQ05GdTIvS
1YiLCJtYWMiOiJhZTRjNzk0MjVhYTgzNWNjOWQzOWIzOGIzYzg4YzU2YmU0YTUwZTg1MTdiOWQ5MjMyY2
QzZWFkMzgxOGIyODgwIn0%3D; expires=Sun, 07-Jan-2024 06:30:04 GMT; Max-Age=7200;
path=/; httponly; samesite=lax
```

- https://homeocureusa.ssbmultiservices.com/contact-mail

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IktxckN0VUNkZCtHSTJIVEhzUHRWS1E9PSIsInZhbHVlIjoiM2pRbWFXZHl5Tk5SdEl
ZZC8vay8raXNsVHVsUGluNFFNcHptZVNyNk14SzQyRjdicmpNa2JwdDhuSENia0I5L2wrT2NDdlpoU1hX
VWdGd1lTcmpKd2lBdVpmMy94R3FCd0QzeEt2UWw5RnJaVXFFWGdLenF1TUFoanNUVjNQK00iLCJtYWMiO
iJhOTcxY2M0Y2YzZmVlYzBhYjU3NTUxMjkxNTQ3YjQ5N2MwYWE3M2E1YWE4NGU2YjczYjVjZjAzODA5ZT
llMzA3In0%3D; expires=Sun, 07-Jan-2024 06:31:20 GMT; Max-Age=7200; path=/;
samesite=lax
```

- https://homeocureusa.ssbmultiservices.com/contact-mail

```
Set-Cookie:
sk_sharma_session=eyJpdiI6ImZyZUlTNC8zb05jVVdWbmd3RFNEMGc9PSIsInZhbHVlIjoiWFhjUFR
ML0ZCTy81b1Zac01OdkZuUWNhMTJNdFFyd1hINW0yRkZzN1JBTDF5a0ZzNnVJS0pySDVkMldYMUYxMDZR
bkhINU5JdFdaR3pGck05QzVlaG1WamZodE9Wc3dOY0dya01jeE9reFljWUtFa0xndVBhRUFFUGhNZEZwV
HciLCJtYWMiOiJhOTBiM2MyYzE3M2E2NjM5MjE1YTgwNDJiMDZkZDU0M2QwNjg4NmU5MmE4ODE2MjEwZG
M0ZmUxMjY1NmZjZDQ4In0%3D; expires=Sun, 07-Jan-2024 06:31:20 GMT; Max-Age=7200;
path=/; httponly; samesite=lax
```

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

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

HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

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

https://homeocureusa.ssbmultiservices.com/

URLs where HSTS is not enabled:

- https://homeocureusa.ssbmultiservices.com/

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org
https://hstspreload.org/

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

Insecure Inline Frame (iframe)

The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as exceptions to these restrictions.

Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

https://homeocureusa.ssbmultiservices.com/ Verified

An iframe tag references an external resource, and no sandbox attribute is set.

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.

References

MDN | iframe: The Inline Frame Element
https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe

HTML Standard: iframe
https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element

HTML 5.2: 4.7. Embedded content
https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox

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://homeocureusa.ssbmultiservices.com/

Paths without CSP header:

- https://homeocureusa.ssbmultiservices.com/

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

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/

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

https://homeocureusa.ssbmultiservices.com/

Emails found:

- https://homeocureusa.ssbmultiservices.com/
  helalforuddin@gmail.com

Request

```
GET / HTTP/1.1
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques
https://en.wikipedia.org/wiki/Anti-spam_techniques

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://homeocureusa.ssbmultiservices.com/ Confidence: 95%

- **bootstrap.js 4.4.1**
  - URL: https://homeocureusa.ssbmultiservices.com/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
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://homeocureusa.ssbmultiservices.com/

Locations without Permissions-Policy header:

- https://homeocureusa.ssbmultiservices.com/

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

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/

Reverse proxy detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

https://homeocureusa.ssbmultiservices.com/

Detected reverse proxy: Apache httpd

Request

```
GET / HTTP/1.1
Max-Forwards: 0
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

None

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

https://homeocureusa.ssbmultiservices.com/

Pages where SRI is not implemented:

- https://homeocureusa.ssbmultiservices.com/
  Script SRC: **https://unpkg.com/sweetalert/dist/sweetalert.min.js**

- https://homeocureusa.ssbmultiservices.com/
  Script SRC: **https://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit**

Request

```
GET / HTTP/1.1
Referer: https://homeocureusa.ssbmultiservices.com/
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/114.0.0.0 Safari/537.36
Host: homeocureusa.ssbmultiservices.com
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

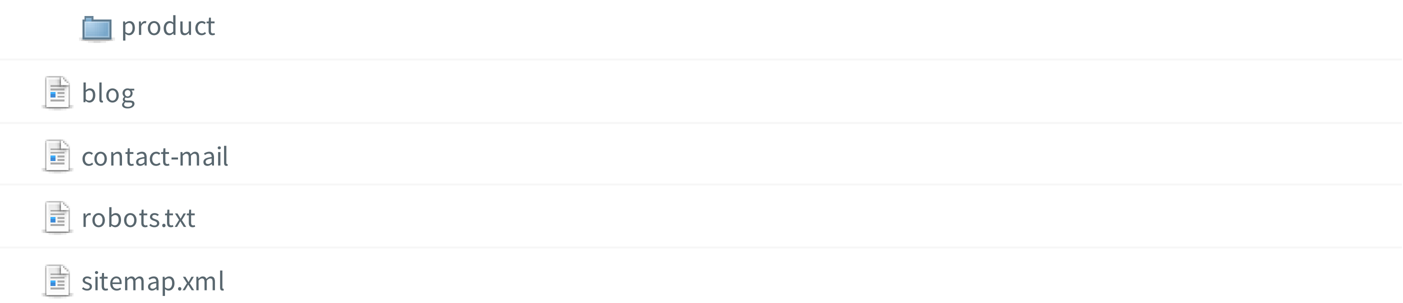
References

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
https://www.srihash.org/

Coverage

- https://homeocureusa.ssbmultiservices.com
  - #fragments
    - googtrans(bn)
    - googtrans(en)
  - _ignition
    - health-check
  - front
    - assets
      - css
        - all.min.css
        - bootstrap.min.css
        - font.css
        - style.css
        - swiper.min.css
      - images
      - js
        - bootstrap.min.js
        - custom.js
        - jquery.min.js
        - magnic-zoom.js
        - SmoothScroll.min.js
        - sticky-sidebar.js
        - swiper.min.js
      - webfonts
  - toastr
    - css
      - toastr.min.css
    - js
      - toastr.min.js
  - uploads
    - home-slider



- product
- blog
- contact-mail
- robots.txt
- sitemap.xml