【WriteUp】网鼎杯2020线下半决赛两道WEB

原创

杜沐清 于 2020-11-29 01:12:12 发布 6235 收藏 19

分类专栏： 网络安全 文章标签： 网络安全 安全漏洞 cms 渗透测试 wp

本文链接：https://blog.csdn.net/weixin_42337765/article/details/110298641

网鼎杯2020线下半决赛两道WEB题WriteUp

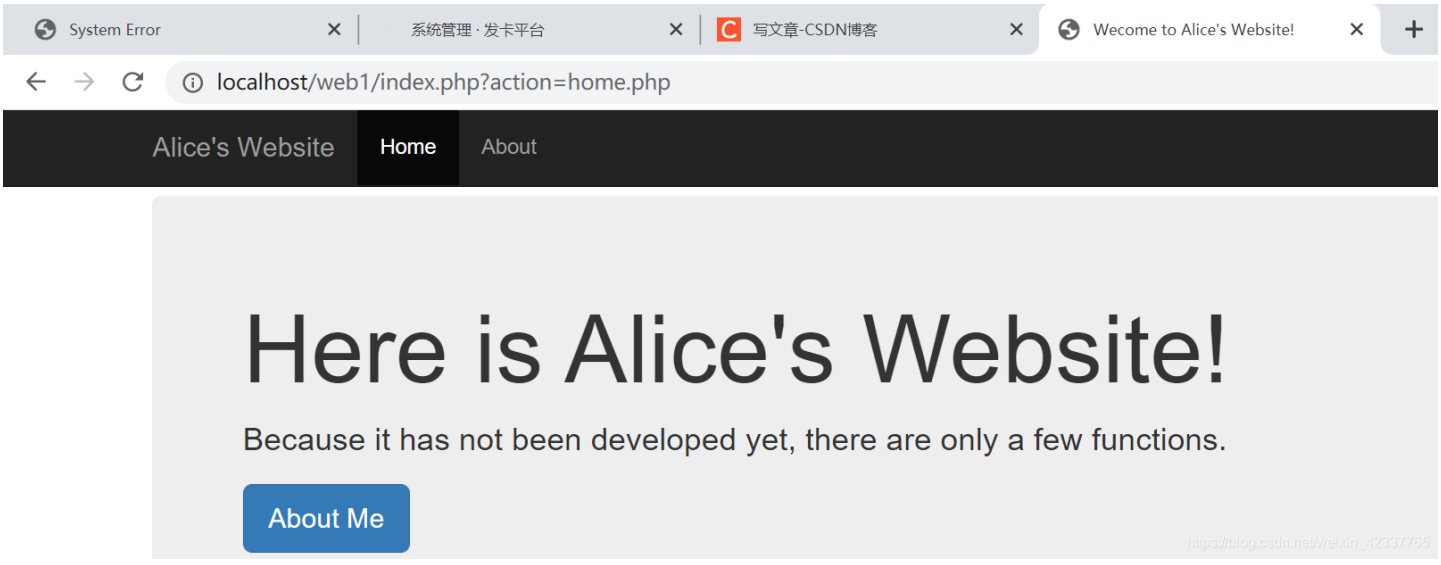
网鼎杯2020线下半决赛两道WEB题WriteUp

第一次参与网鼎杯线下赛，五道题3道PWN、两道WEB(PHP)，下午又加了一道web(nodejs)。

先说下赛制，网鼎杯赛制叫做AWD PLUS，应该是全国唯一采用这个赛制的比赛。名字叫做AWD，实际这个赛制队伍之间不需要也不允许相互打。每个队伍每个题目有一个GameBox，提供下载源代码包，攻击和修复代码漏洞就可以得分。与一般AWD不同的是，网鼎杯赛制不需要准备不死马/通防脚本等，更加偏重于代码审计、漏洞挖掘、漏洞利用和修复。（也许叫CTF PLUS或者 AWD STATIC 更合适？）

两道web题write_up

WEB1 web_AliceWebsite



打开主页，容易看到上面有个文件包含。

查看源码，看到

```php
<?php
        $action = (isset($_GET['action']) ? $_GET['action'] : 'home.php');
        if (file_exists($action)) {
            include $action;
        } else {
            echo "File not found!";
        }
?>
```

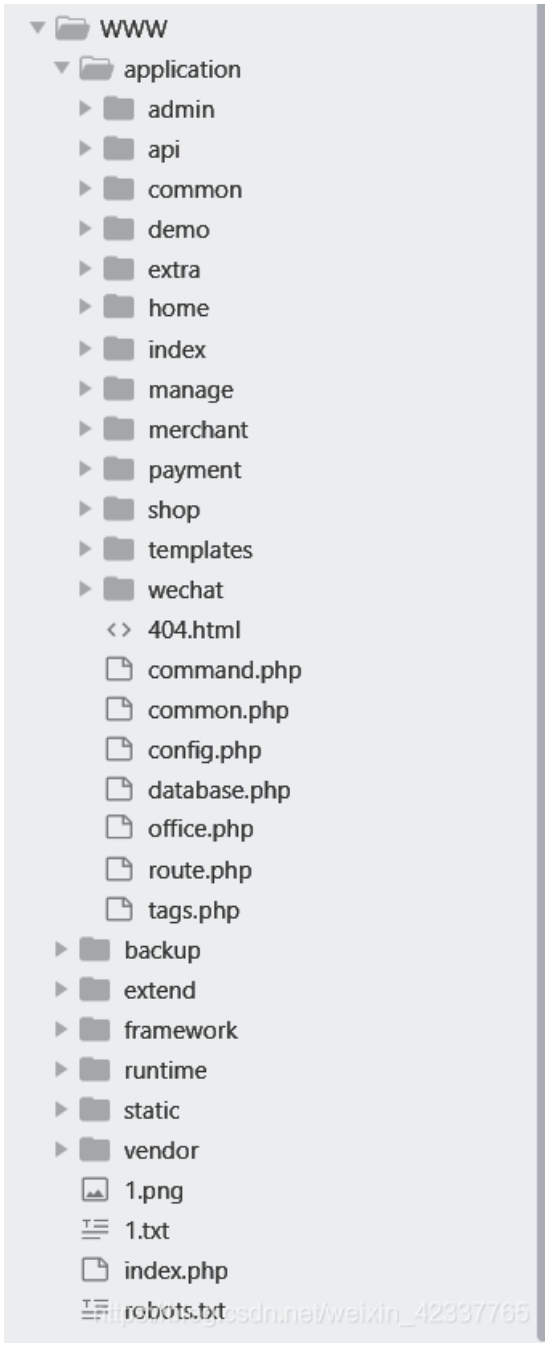
没有任何过滤, include /flag 拿到flag;

payload

?action=/flag

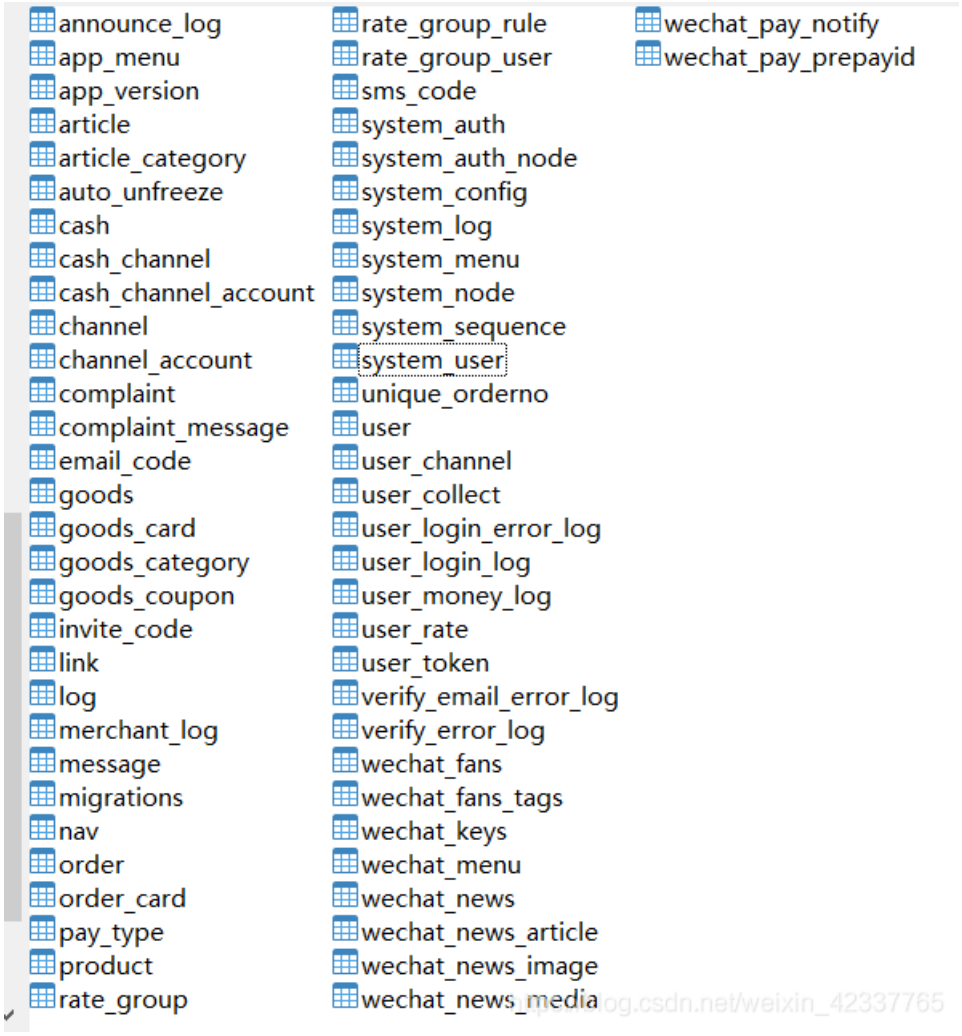
WEB2 FAKA

先部署代码到本地，并导入sql文件。代码目录



根目录robots.txt 里提示1.txt，1.txt里面是注册邀请码，根据提示注册，是一般用户，略微审计了下 /application/merchat/ 目录，没啥用。

后台页面在/application/admin目录下，使用的表叫做 system_user



打开system_user表，第一行为账户名为admin，密码为md5的用户。赛前准备了TOP10W密码的哈希值，搜索了下这个哈希值没有搜到。看来需要修改密码或者新增一个用户。

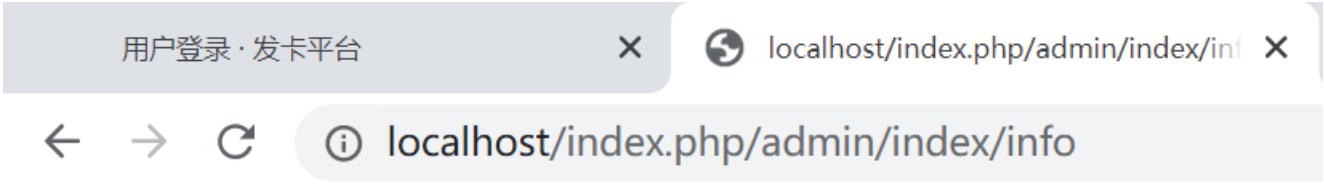
id	username	password	qq	mail	phone	desc	login_num	login_at	status	authorize	is_deleted	create_by	create_at	gooc
10005	admin	81c47be5dc6110d5(	(Null)	12345678@qq.com	12345678	demo	264	2020-03-20 14:38:5(	1	3	0	(Null)	2018-05-02 08:40:0(	(Null)

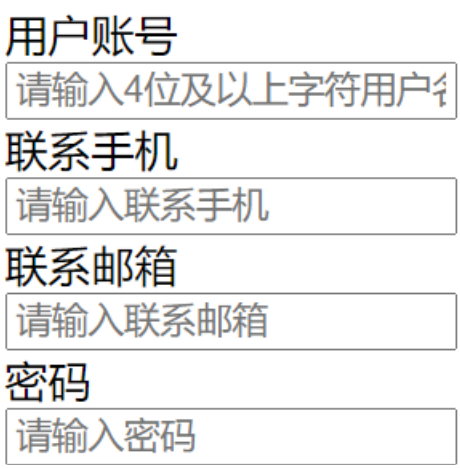
继续审代码，application/admin/index.php 文件下有两个方法：

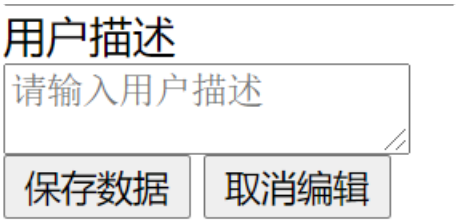
```php
public function pass()
    {
        if (intval($this->request->request('id')) !== intval(session('user.id'))) {
            $this->error('只能修改当前用户的密码！');
        }
        if ($this->request->isGet()) {
            $this->assign('verify', true);
            return $this->_form('SystemUser', 'user/pass');
        }
        $data = $this->request->post();
        if ($data['password'] !== $data['repassword']) {
            $this->error('两次输入的密码不一致，请重新输入！');
        }
        $user = Db::name('SystemUser')->where('id', session('user.id'))->find();
        if (md5($data['oldpassword']) !== $user['password']) {
            $this->error('旧密码验证失败，请重新输入！');
        }
        if (DataService::save('SystemUser', ['id' => session('user.id'), 'password' => md5($data['password'])]))
{
            $this->success('密码修改成功，下次请使用新密码登录！', '');
        }
        $this->error('密码修改失败，请稍候再试！');
    }

    /**
     * 修改资料
     */
    public function info()
    {
        if (intval($this->request->request('id')) === intval(session('user.id'))) {
            return $this->_form('SystemUser', 'user/form');
        }
        $this->error('只能修改当前用户的资料！');
    }
```

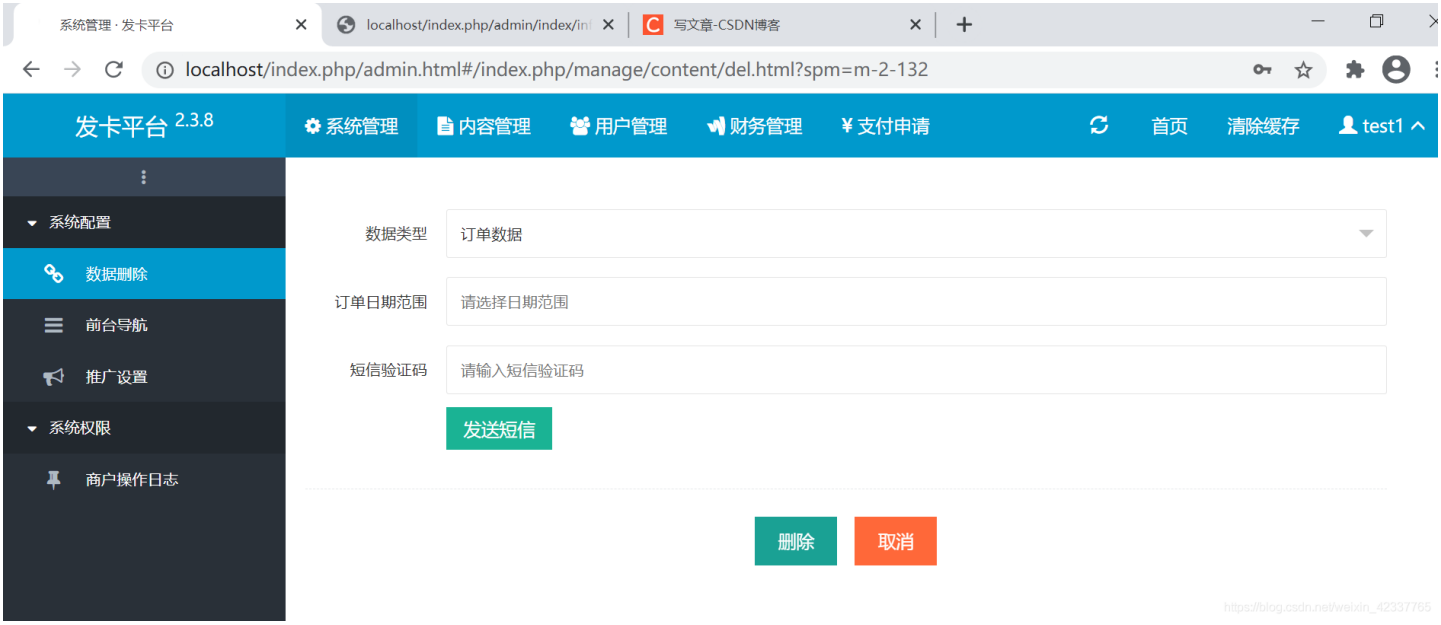
尝试了下，两个路径都可以直接访问。第一个方法是修改用户密码，可以看到代码中验证比较多，没有什么可以利用点；info这个方法直接调用父类的方法，没有什么比对验证，也许可以利用？







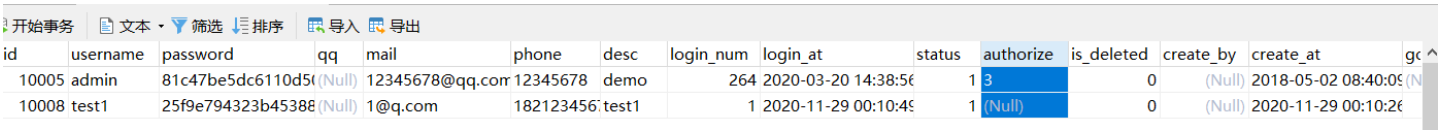
根据提示保存数据，数据库果然新增了一条用户，并在后台页面登录成功。



功能比较少，点击内容管理时，提示没有权限，接下来需要越权。

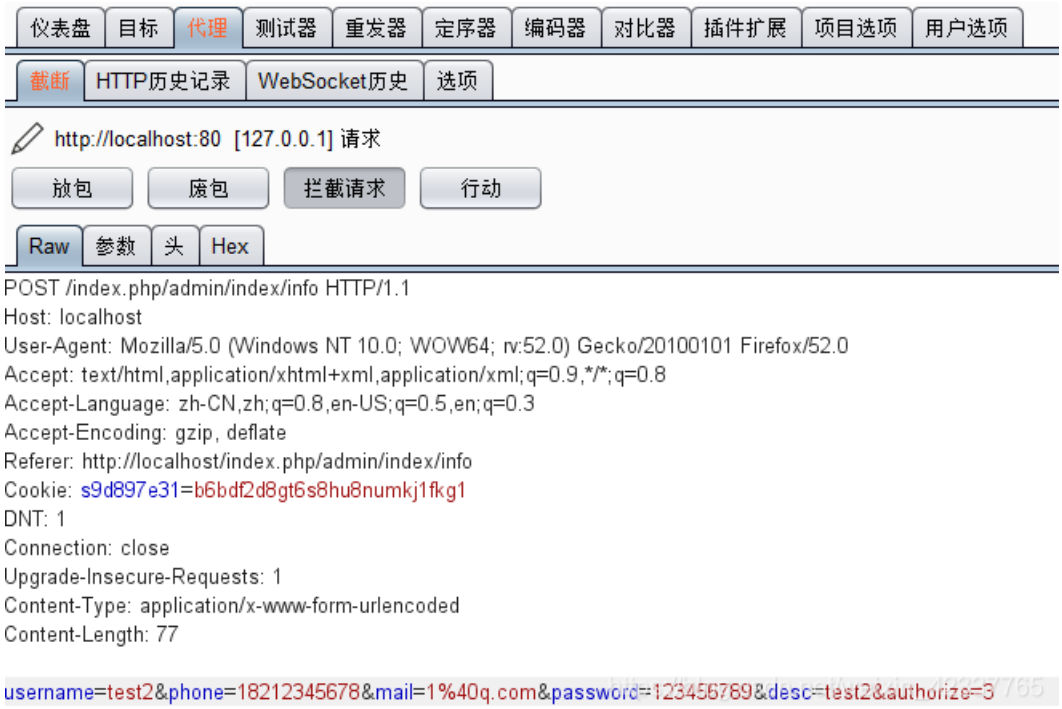
审计了一圈下来，用户信息都存在session当中，没办法直接在页面交互中改权限。

比对数据库发现，自己注册的用户和admin用户的authorize值不一样。



id	username	password	qq	mail	phone	desc	login_num	login_at	status	authorize	is_deleted	create_by	create_at
10005	admin	81c47be5dc6110d5	(Null)	12345678@qq.com	12345678	demo	264	2020-03-20 14:38:56	1	3	0	(Null)	2018-05-02 08:40:09
10008	test1	25f9e794323b4538	(Null)	1@q.com	182123456	test1	1	2020-11-29 00:10:49	1	(Null)	0	(Null)	2020-11-29 00:10:26

而且自己新增的用户authorize值为null。能不能在刚才修改用户的资料里这个页面直接改？



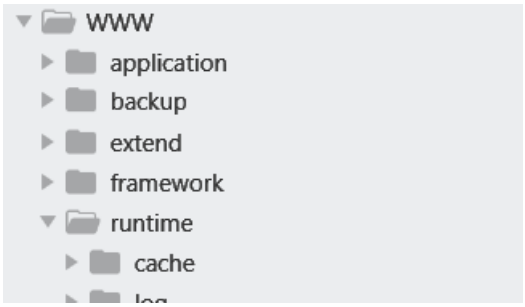
在burp里加入authorize=3，超级用户添加成功

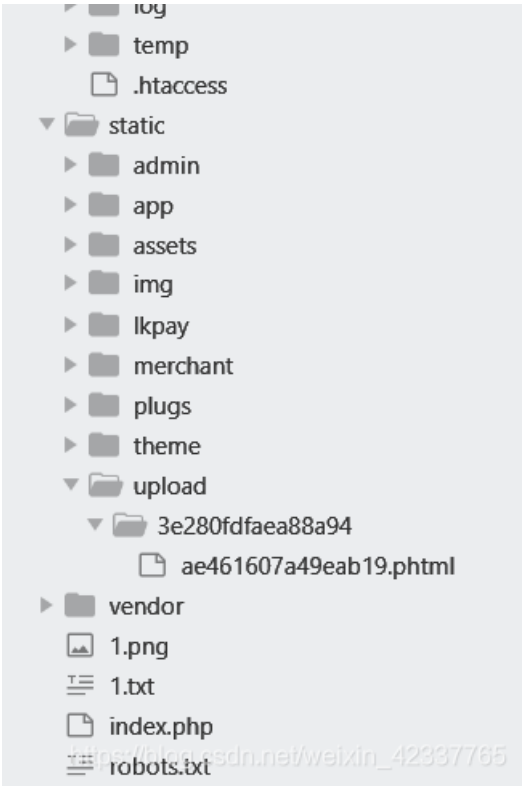
id	username	password	qq	mail	phone	desc	login_num	login_at	status	authorize	is_deleted	create_by	create_at	g
10005	admin	81c47be5dc6110d5	(Null)	12345678@qq.com	12345678	demo	264	2020-03-20 14:38:56	1	3	0	(Null)	2018-05-02 08:40:09	
10008	test1	25f9e794323b45388	(Null)	1@q.com	182123456	test1	1	2020-11-29 00:10:49	1	(Null)	0	(Null)	2020-11-29 00:10:26	
10009	test2	25f9e794323b45388	(Null)	1@q.com	182123456	test2	0	(Null)	1	3	0	(Null)	2020-11-29 00:22:15	

成功登录。

接下来继续找可以利用的点。

在代码中可以找到upload, upfile 等方法，在本地测试中，http://localhost/index.php/admin/plugs/upfile 这个路径可以上传文件，而且，超级用户可以修改白名单，允许phtml这样的后缀。

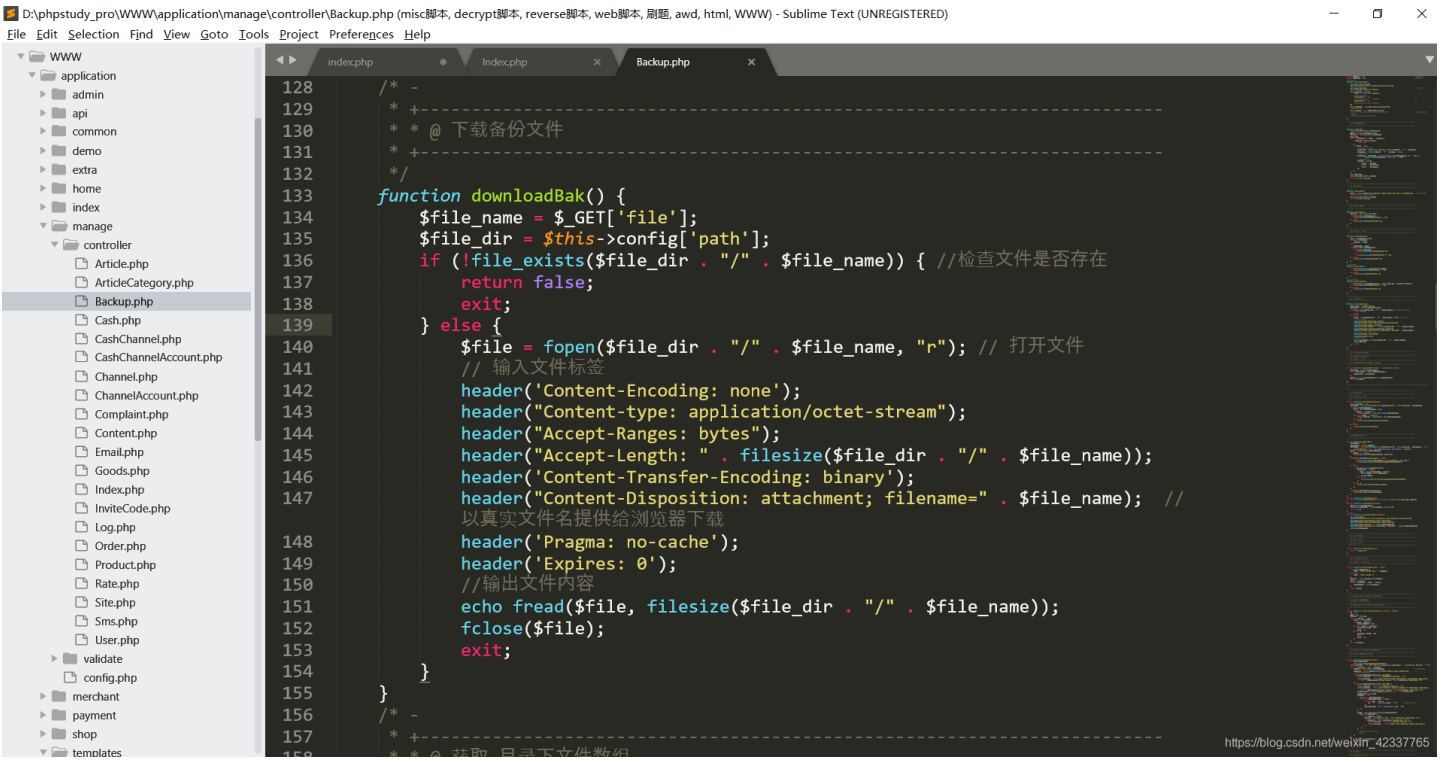




但是！在比赛方的服务器根本上传不了，提示mkdir() permission refuse。 但是比赛平台页面提示中明确写着/var/www/html/static目录可写！本着出题方一般不会出错的想法，尝试修改上传路径直接到/static路径下(路径根据token生成，token可控, …/…/…/往上穿即可)。这一次不提示permission 了, 直接提示 file exits 。 晕。可能比赛方担心选手搞坏docker影响服务器，不希望选手上传shell吧。

好吧，闲话不多说。继续找漏洞。搜索 file_ 一个一个试，此处略过。

最后在application/manage/Backup.php中找到利用点



没有任何检查，任意文件读。最终payload:

http://localhost/index.php/manage/backup/downloadBak?file=…/…/…/…/flag

小问题

这个源码是基于thinkphp 5.0.14的，众所周知这个版本有个RCE漏洞。尝试利用没有成功，有同学利用成功的吗?

下载网鼎杯网络安全夺旗赛 题目源码