

BUUCTF Web [ACTF2020 新生赛]Include

原创

[士别三日wyx](#) 于 2021-10-27 14:11:22 发布 10313 收藏 5

分类专栏: [靶场通关教程](#) 文章标签: [渗透测试](#) [网络安全](#) [java](#) [python](#) [安全性测试](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/wangyuxiang946/article/details/120990784>

版权



[靶场通关教程](#) 专栏收录该内容

10 篇文章 3 订阅

订阅专栏

「[作者主页](#)」: [士别三日wyx](#)

此文章已录入专栏 [《网络攻防》](#), 持续更新热门靶场的通关教程

「**未知攻, 焉知收**」, 在一个个孤独的夜晚, 你完成了几百个攻防实验, 回过头来才发现, 已经击败了百分之九十九的同期选手。

[ACTF2020 新生赛]Include

一、题目简介

二、思路分析

三、解题步骤

- 1) 包含 flag.php
- 2) PHP伪协议编码文件
- 3) 解码文件内容

四、总结

一、题目简介

进入题目链接后只有一个「[链接](#)」

tips

点击链接后来到了 flag.php 页面，里面是一句作者深情的「[问候](#)」。

← → ↻ ⚠ 不安全 | 01f6f854-6022-434c-aabb-1e6fe3588e17.node4.buuoj.cn:81/?file=flag.php

Can you find out the flag?

二、思路分析

这一关是「[文件包含](#)」漏洞，推荐使用「[PHP伪协议](#)」读取文件源码。

在tips页面，右键查看页面源代码

```
1 <meta charset="utf8">
2 <a href="?file=flag.php">tips</a>
```

是一个 a 标签，通过 file「[参数](#)」传递了一个「[文件名](#)」flag.php。点击链接后会进入 flag.php 文件的页面，很明显是一个文件包含的功能，根据点击后的url可以验证这一观点

← → ↻ ⚠ 不安全 | 01f6f854-6022-434c-aabb-1e6fe3588e17.node4.buuoj.cn:81/?file=flag.php

Can you find out the flag?

CTF有个不成文的「[规矩](#)」，如果有一个文件以flag命名，那么flag大概率就在这个文件里面。右键查看「[页面源码](#)」，检查是否存在信息泄露。

自动换行

```
1 <meta charset="utf8">
2 Can you find out the flag?
```

很明显，前端源码没有flag，那只能在后端源码里面了。文件包含功能有个「[特性](#)」，对于被包含的文件，「[代码](#)」部分会直接执行，不会在页面中显示；「[非代码](#)」部分（即不能执行的内容）则会在页面中显示。针对这一特性，我们可以将被包含文件的内容「[编码](#)」为不可执行的内容，让其在页面中显示，再将页面中的内容在本地「[解码](#)」，就可以拿到文件的后端源码了。这里我们可以使用PHP伪协议对文件内容进行base64编码，[点我进入PHP伪协议参考文章](#)

三、解题步骤

1) 包含 flag.php

点击 tips 「[链接](#)」进入另一个页面，即包含 flag.php 文件

tips

← → ↻ ⚠ 不安全 | 01f6f854-6022-434c-aabb-1e6fe3588e17.node4.buuoj.cn:81/?file=flag.php

Can you find out the flag?

2) PHP伪协议编码文件

使用PHP伪协议对文件内容进行base64 「[编码](#)」，将url中file参数替换为以下payload

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

编码后的文件内容会在页面中输显示

← → ↻ ⚠ 不安全 | 01f6f854-6022-434c-aabb-1e6fe3588e17.node4.buuoj.cn:81/?file=php://filter/read=convert.base64-encode/resource=flag.php

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7OWMxYWY2OWMtNTA1OC00Zjg1LWlwZDEtZjBkZTFINmMwZTlmfQo=

3) 解码文件内容

将页面中的文件内容复制下来，本地进行base64 「[解码](#)」，base64解码参考[连接](#)

DES,AES等对称加密解密 MD5加密/解密 URL加密 JS加/解密 JS混淆加密压缩 ESCAPE加/解密 **BASE64** 散列/哈希 迅雷, 快车, 旋风URL加密

```
<?php
echo "Can you find out the flag?";
//flag(9c1af69c-5058-4f85-b0d1-f0de1e6c0e9f)
```

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7OWMxYWY2OWMtNTA1OC00Zjg1LWlwZDEtZjBkZTFINmMwZTlmfQo=

需要解码的内容放右边

多行

flag就在解码的内容中，提交即可

四、总结

喜欢一个东西首先要先学会「[尊重](#)」，虽然网络安全的圈子不乏各种灰产，以及高调宣传自己是黑客的脚本小子，但不可否认，这个圈子仍有不少人保持着「[举世皆浊我独清，众人皆醉我独醒](#)」的心态，努力磨砺技术，提升自身修养，让互联网变得更加安全