i春秋 afr1 解题过程 题解 原理 PHP伪协议 文件包含漏洞

原创

AAAAAAAAAAAA66 于 2021-11-20 00:21:29 发布 215 收藏
分类专栏： CTF -WEB 学习 文章标签： php apache 网络安全

知识面决定攻击的广度，知识链决定攻击的深度。

最近尝试了一下挖洞，捣鼓了一天还是啥都没有，没有头绪后，还是去写点CTF题，扩充下知识面，2个方向算是互补吧。

目录

工具

dirsearch（目录扫描工具）

火狐

hackbar

知识点

php://伪协议

*php://filter:php中独有的一个协议，可以作为一个中间流来处理其他流，可以进行任意文件的读取；根据名字，filter，可以很容易想到这个协议可以用来过滤一些东西；

*php://filter是元封装器,设计用于数据流打开时的筛选过滤应用，**允许访问对本地磁盘文件进行读写。**

格式：

```
?filename=php://filter/read=convert.base64-encode/resource=xxx.php
```

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。

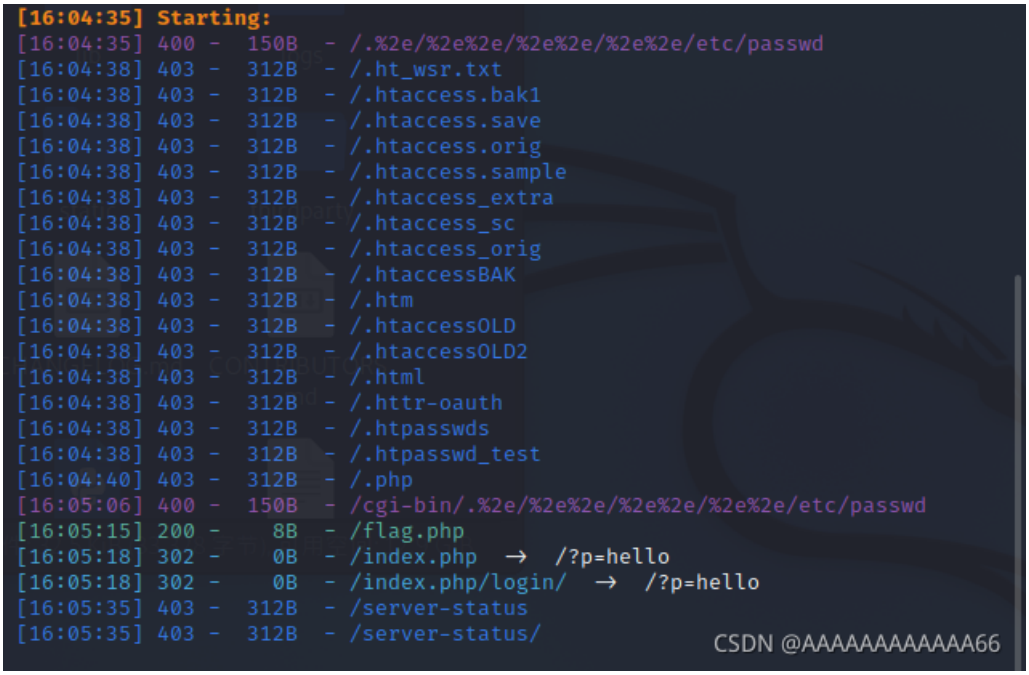
文件包含漏洞

文件包含漏洞的产生原因是在通过 PHP 的函数引入文件时，由于传入的文件名没有经过合理的校验，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入。

解题过程

题目：

老规矩，dirsearch扫一波



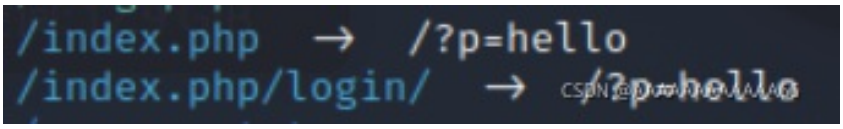
可以看到有个flag.php文件

直接访问，页面为空。

利用php伪协议读取文件

构造payload（失败）：

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



在URL后加上index.php 页面跳转道p=hello页面

尝试index.php/login 也是一样。

而之前?p=hello 访问出页面

想到这里可能存在后缀拼接，服务器后台将输入p的值加上.php（没错，就是这么神奇）

（坑点）

服务器将你输出的后缀加上.php (卡在这很久了）

所以我们把payload 中的点php删除。

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

读取了flag文件

PD9waHAKZGllKCdubyBubyBubycpOwovL24xYm9va3thZnJfMV9zb2x2ZWR9

Base64（看多了有这个直觉）

Base64在线解码

得到flag.

思考

总结思路（要点）：

1.题目首页url p=hello (联想到文件包含漏洞)

2.dirsearch发现flag.php得想办法读取（php伪协议）

3.服务器后台对文件后缀名的过滤

因为基础太差，这里是我的自己的一些思考（看write up 一把过绝对很容易，但其实自己写博客慢慢思索细节发现这道题对我这种新手坑的很）

*php:filter//一般会与文件包含漏洞一起出现。

比如说本题中的参数p （可能是英文page的缩写）实际上就是起作为filename的作用，要自行填入输入的文件名。

那么单单仅凭传入一个参数p，提交一个文件名，服务器是怎么把它当成文件执行的呢，（首先是你输入的文件名在服务器存在）

这里就要出现一个include()函数了。比如说我在首页，你传入一个p值，假设p=xxx.php,因为这个函数的存在，服务器直接会执行xxx.php(当然，这道题目是执行在服务器上的flag.php文件，本地文件包含)这样是不是很方便！！！通过p传进来的文件名，如果在服务器有，就执行，没有就不执行。

那么就算执行了flag.php文件，但这个文件执行了什么都不显示，怎么办，那么php:filter伪协议就上场了，注意到我们这道题的payload

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

有2个等于号，第一次看到的朋友可能和我一样，p是一个参数，怎么传这么长，=php://filter/read=convert.base64-encode/resource（注意到这个等于号）暂且可以理解用这个协议的格式。

话说回来，利用这个协议，可以让flag.php文件不执行，直接能获取源码。

当然，利用同样方式我们获取index.php的源码（base 64 解码后）果然验证了我的思路，解决了我的疑惑。

```
if(isset($_GET['p'])) {
    include (string)$_GET['p'] . ".php";
}
else{
    header('Location: p=hello');
}
```

（这里不知道为什么复制到文本上是这样的，也算是个小彩蛋把，哈哈）

if(isset($_GET['p'])) {
    include (string)$_GET['p'] . ".php";
}
else{
    header('Location: 🧐p=hello');
}

看到这里如果有不懂的地方，希望回过头多看下，思考下，多查阅下相关的知识点。

（TMD 本来看了些write up 自己顺着来写，8点就写完了，后面自己从头到尾琢磨一下，结果发现很多细节没有写，其实是自己也没想明白为什么这么做，结果加班快1点，好吧，我承认我菜）

其实对于我这样的知识面不广新手来说，不了解题目的知识点是很难做出来了，当然可能这题目有很多不同的解法。如果要想打CTF，感觉多种思路是重要的，不可能每道题目都能一下找到正确思路，都是要不断用自己的知识与题目联系起来，不断尝试。

----------作者水平有限，不当之处欢迎指正。