BUUCTF上传漏洞复现集合

原创

fly夏天 于 2020-12-10 15:44:26 发布 216 收藏

分类专栏： ctf 文章标签： web ctf

1.你传你□呢

简简单单一道题，点进去看见天皇，我决定要把这个□骨灰给给扬了。
首先bp抓包，测试一下普通的后缀名修改，无效。尝试.htaccess文件上传，发现并没有被过滤。

简单的原理介绍

注：

- .htaccess是一个纯文本文件，它里面存放着Apache服务器配置相关的指令。
- 利用.htaccess文件可以指定文件以什么类型访问，简单来说就是可以让jpg以php的方式运行，这样就可以达到绕过的目的。
- .htaccess文件需要httpd.conf中启用AllowOverride为前提。
- .htaccess文件中的配置指令作用于.htaccess文件所在的目录及其所有子目录，但是很重要的、需要注意的是，其上级目录也可能会有.htaccess文件，而指令是按查找顺序依次生效的，所以一个特定目录下的.htaccess文件中的指令可能会覆盖其上级目录中的.htaccess文件中的指令，即子目录中的指令会覆盖父目录或者主配置文件中的指令。

.htaccess文件的写法

```
<IfModule mime module>
SetHandler application/x-httpd-php .png
#AddType application/x-httpd-php .png
</IfModule>
```

- 这种写法下所有的png都会被解析成php文件
- #后的写法也有一样的效果
- 如果不加后面的 .png，则所有目录下的文件都会按照php格式来解析。

```
<FilesMatch "1.png">
SetHandler application/x-httpd-php .png
#AddType application/x-httpd-php .png
</FileMatch>
```

这种写法就可以实现对符合一定条件的文件单独进行解析，避免大范围的执行。

然后上传php一句话，蚁剑连接，即可轻松拿到flag
理论上是这样，但测试时死活连接不上去，不管了，暂时就这样把，我也没辙了。