干货 | 文件上传绕过的一次思路总结学习

adminxe HACK学习呀 *2022-06-27 09:53 发表于广东*

前言

我是来总结的，嘀嘀嘀开车了！！！

原文：文件上传绕过的一次思路总结（两个上传点组合Getshell）

0x00 测试上传正常文件

这里可以判定文件名虽然是重命名，但是可控的，因为我们上传的文件名被带进去了(*_1.txt)这里利用的思路主要:

1.目录没有执行权限（通过控制文件名进行../../跳目录，跳到可以执行脚本语言的目录）

2.上传文件找不到路径（通过控制文件名进行../../跳目录，层级跳到根目录进行访问）

3.上传白名单截断 （有些文件上传处是白名单，后缀名不可以绕，可以利用控制文件名截断的方式去绕过白名单，例如1.jsp%00.jpg）

4.截断文件前置名（这里后面会详细讲）

0x01 测试上传非正常文件

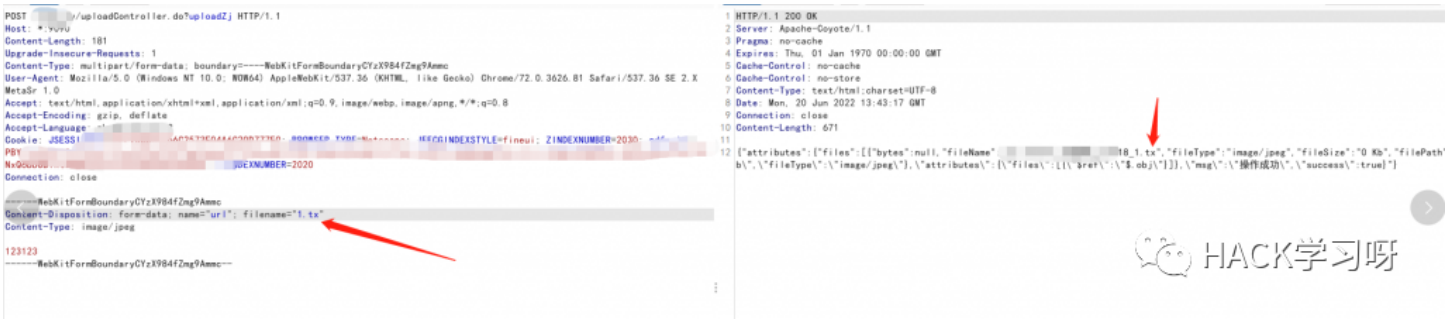
这里主要观察是不是黑名单，或者说是没有限制名单，下图可以看到，上传tx格式是可以正常上传的，但是上传jsp文件就上传不成功

如果上传tx可以上传，但是jsp不可以，可以判断为上传黑名单，这里可以尝试绕黑名单的一下后缀格式，常见的绕黑名单的后缀格式有：

```
aspx&asp：ashx、asa、asmx、cerphp：php3、phtmljsp：jspx、jspf
```

这里简单列举几个，具体详细的我之前发的文章有，这里补充一个小知识点，假如站点为php的站点，但是只限制了php的后缀格式，我们这里可以利用别的脚本语言都测试一下，因为可能这个服务器可以运行多种语言，虽然概率比较低，但是没有好的绕过办法的时候可以试一下，万一成功了呢，我在项目中就碰到过这种情况

上传tx后缀，上传成功：



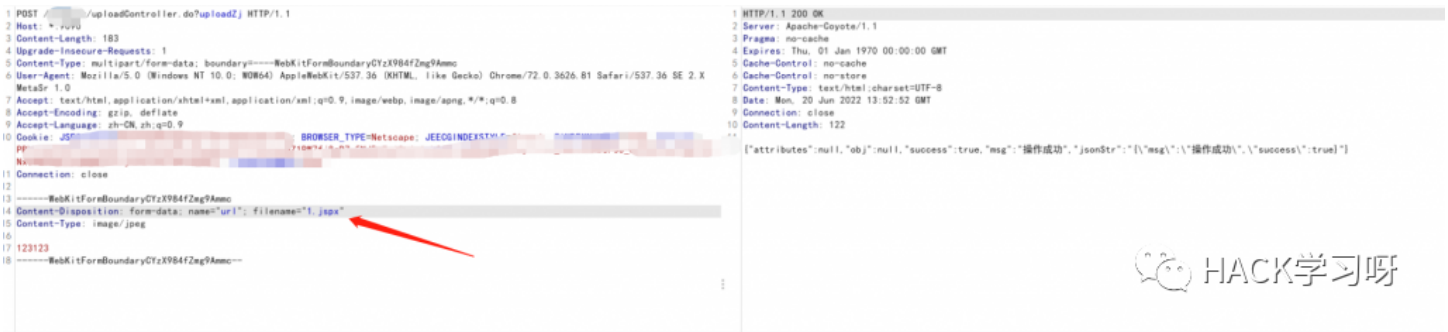
上传jsp 上传失败：

0x02 绕过测试

这里主要讲一下常见的一些绕上传的方法，这个是朋友给的站，我也不知道能不能绕过去，我也是一边绕一边记录着，是我绕上传的一个基本的思路，给大家学习一下

上面测试了，上传黑名单，我们就先测试一下绕上传后缀

1.jspx绕过，失败，测试了别的php什么的都不可以，限制的比较全，html都不可以。



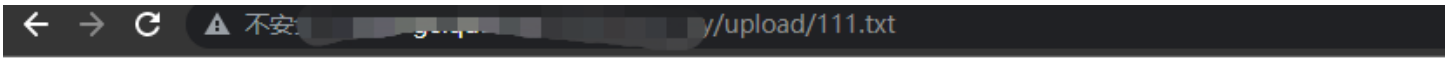
2.截断绕过

这里可以尝试：，；、%00、’、^ 等都可以，这几种方法在windows服务器上成功率是比较高的，因为windows在创建文件的时候这些特殊字符是不允许出现的

最后测试利用 “：”截断成功了，但是很遗憾，虽然传上去了，也可以访问到，但是内容没有写进去，这就是利用：截断的一个弊端，只有文件，没有内容

3.利用跳目录

因为文件名可以控制，我们就可以利用../跳目录的方式去截断代码本身给添加的前置名，就此系统为例，我们上传1.txt，代码会自动给我们添加2022_06_20_1.txt,这里的利用思路就是上传配合解析的配置文件，例如上传.htaccess配合解析，当然这里实战应用的场景还有很多，只是提供一个思路



123123

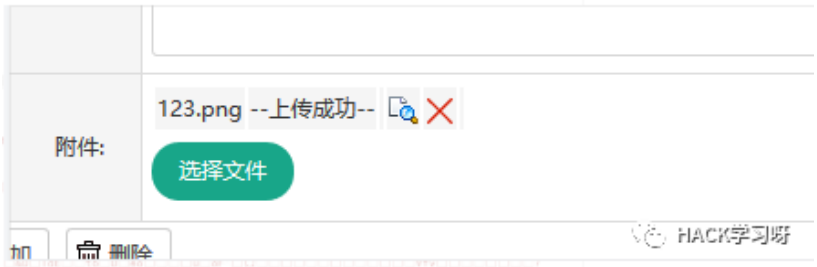
我们这里也是成功截断前置名，并且跳到上层目录了，但是在此服务器这种方法并不是很好用，因为是java的站，利用此方式暂时没有好的getshell的方法，这里只是提供一下思路

0x03 其他上传点继续测试

饶了半天始终是绕不过去，也不想绕了，但是文章都写到这里了，不能白白写啊，又问朋友要了个账号，测试一下后台有没有别的上传

功夫不负有心人，文章得以继续了

确实发现了另一个上传点

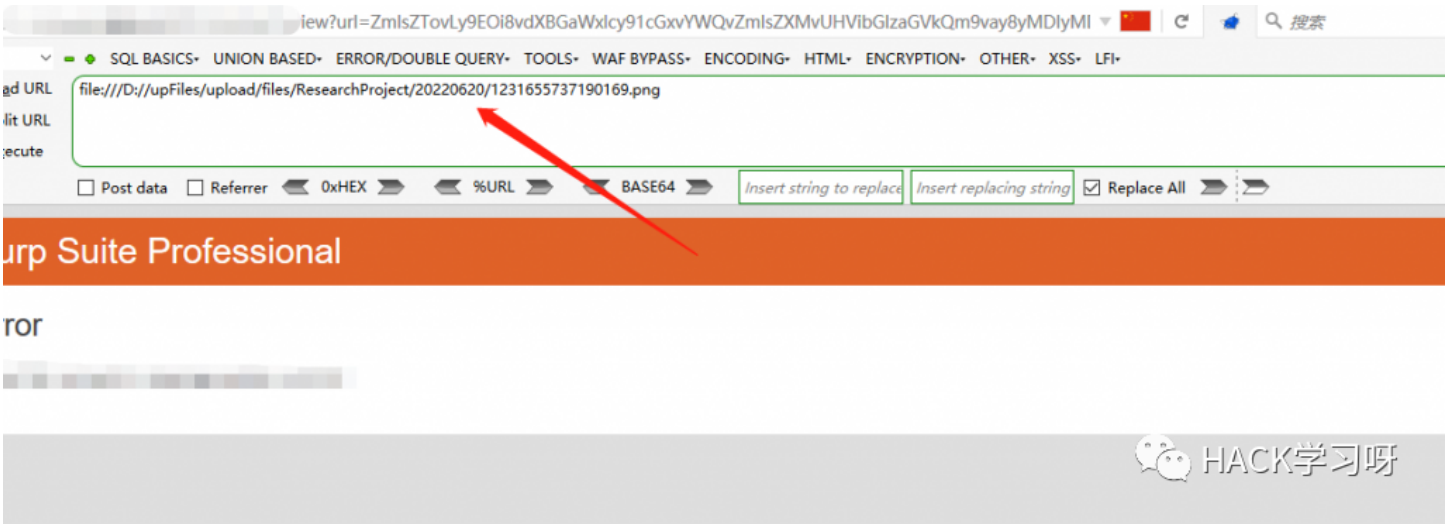


这个上传点比较有意思，后缀可以用大小写直接绕过

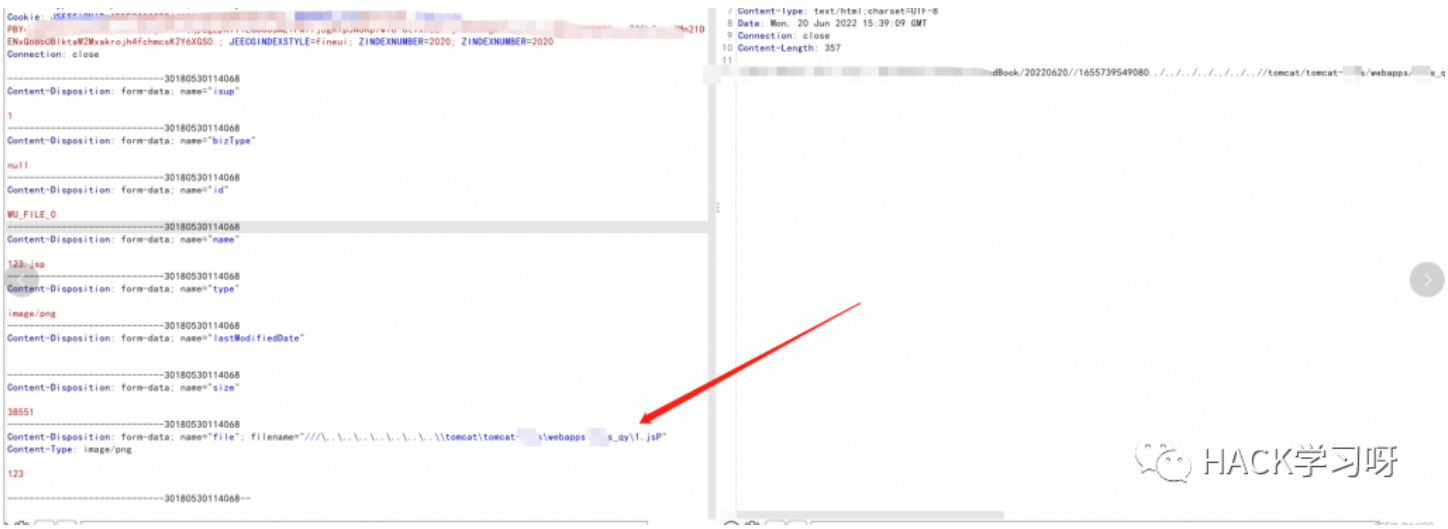
这不直接get了吗？

然而并不是，访问文件目录404？

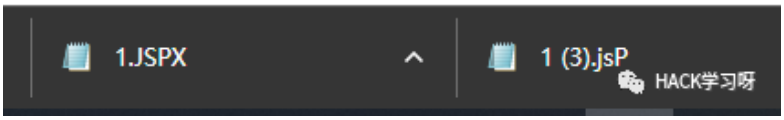
通过查看附件的功能发现，查看附件处是用base64加密的一个绝对物理路径



这里就直接运用我们之前的跳目录，通过报错找到网站的真实路径（也有其他方法查找真实路径，我这里是用的报错），直接上传



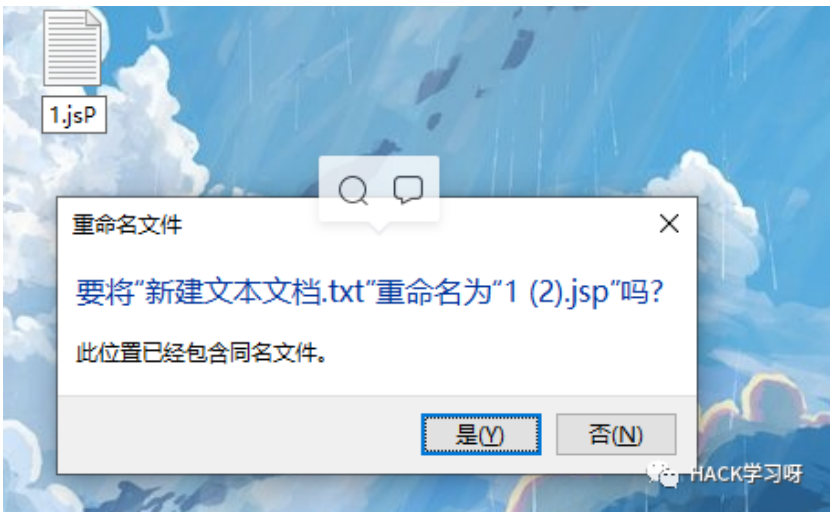
但是不妙呀！1.jsP访问直接下载呀！JSPX也是



这里就体现出我们之前跳目录加截断文件前置名的作用了

之前我们第一个上传点，可以利用：截断，上传jsp，但是文件内容传不上去，然后利用第二个上传点再上传一次同样文件名的文件 （1.jsp|1.jsP）

因为windows不区分大小写，所以就导致我们后面上传的1.jsP直接就把内容覆盖到1.jsp上面去了



最终获得大马一枚

0x04 总结

对此篇文章做个学习总结：

1、上传绕过中，分清楚是代码级限制，还是WAF级限制，进行不同方式的绕过

一些基础的WAF绕过手法，可以看下AZ师傅写的文章：

```
1 （1）https://blog.csdn.net/weixin_44578334/article/details/112393475 （Bypass WAF） （2）https
```

2、注意一些细节点：

（1）在目录跳跃时，注意使用”///”，进行防止转移，细节拿捏。

```
1 upload1:Content-Disposition: form-data; name="file"; filename="///..\..\..\..\333.jsp:.txt"
```

（2）目录跳跃时，这里配合一个伪协议点：file，在渗透过程中遇到了，可以尝试别的协议是否能直接shell，如果不能shell，尝试获取网站的根目录，如果不细心，这个站的目录，就会以为时站和文件目录分离。

（3）上传绕过配合，两个小点，第一个上传点能使用冒号”:”，进行截断，然后上传成功jsp文件，但是缺陷就是，截断后的文件，内容无法post上去，配合第二个上传点（即使不解析，但内容可被送达文件），windows下不区分大小写，所以会进行内容覆盖，正好两个上传点配合，使上传点二的内容恰好覆盖到上传点1上传的正常文件里，完美解决上传问题。