0x01 前言

有技术交流或渗透测试培训需求的朋友欢迎联系QQ/VX-547006660

0x02 资产收集到脆弱系统

在某src挖掘过程中，本人通过ssl证书对域名资产进行了收集，通过计算域名对应ip段的权重
整理出其C段资产，进行了批量目录扫描

查看目录扫描结果后，发现了一个有趣的文件

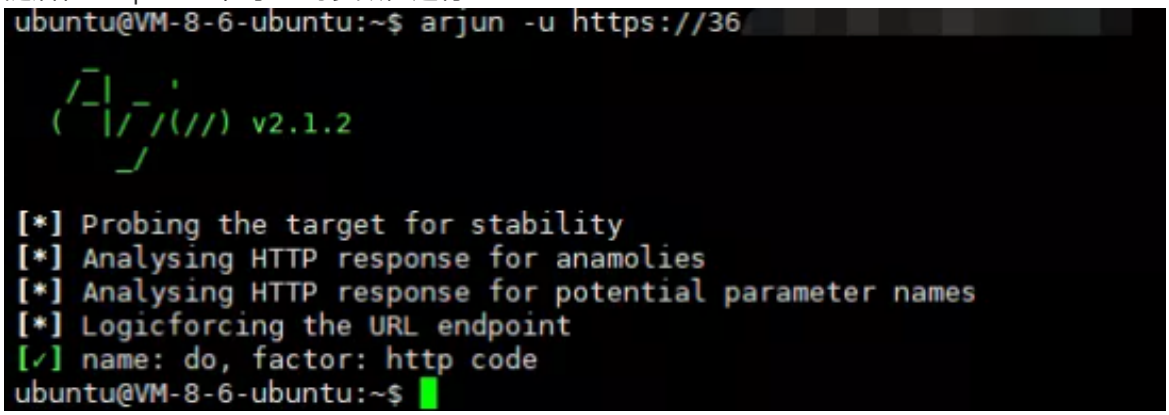
http://36...*/upload_image.php

对于这种页面，毫无疑问，要对参数进行FUZZ

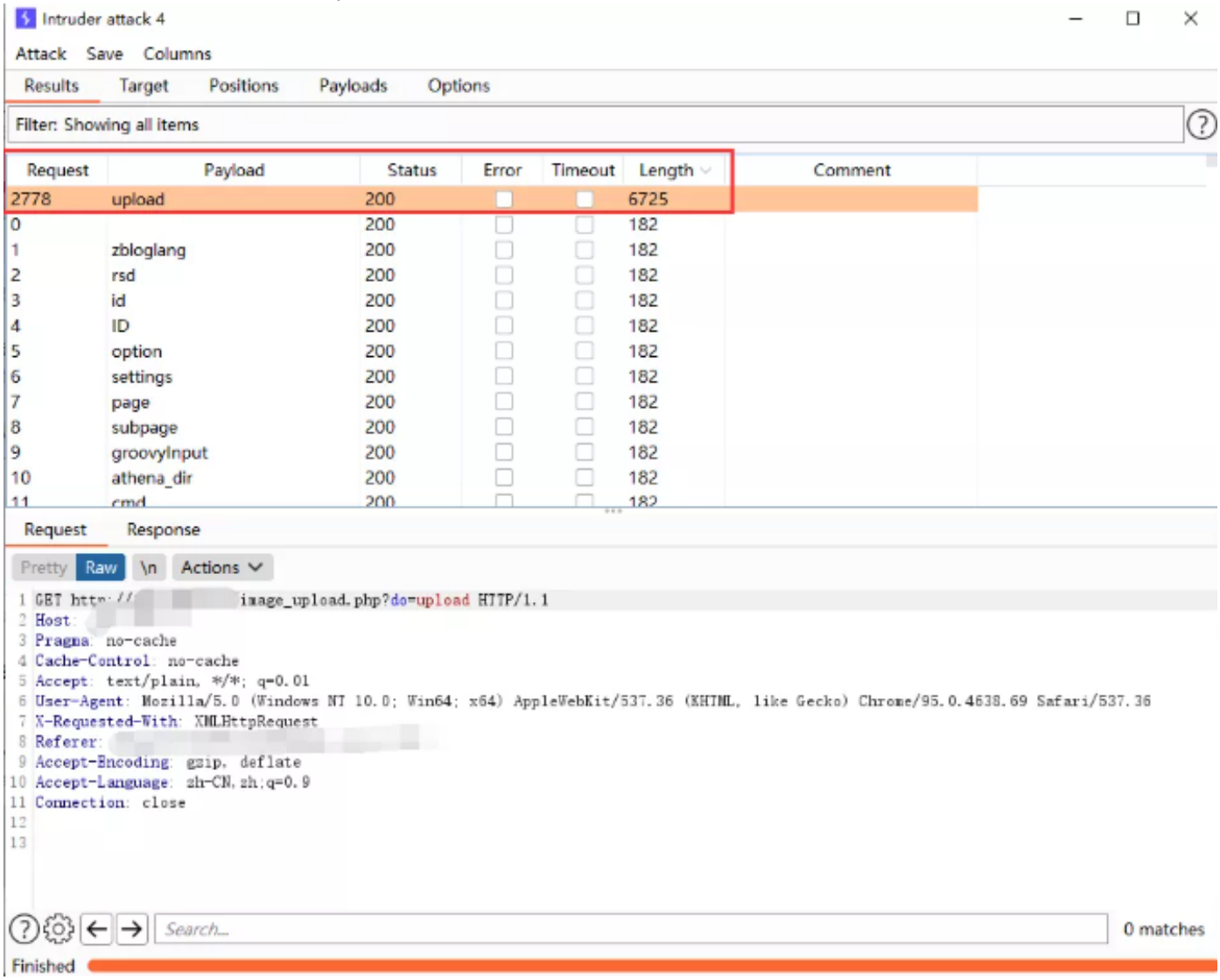
0x03 FUZZ参数+表单上传

使用arjun工具对其参数进行fuzz，发现了一个参数字段为do

随后在burpsuite中对do的参数值进行fuzz

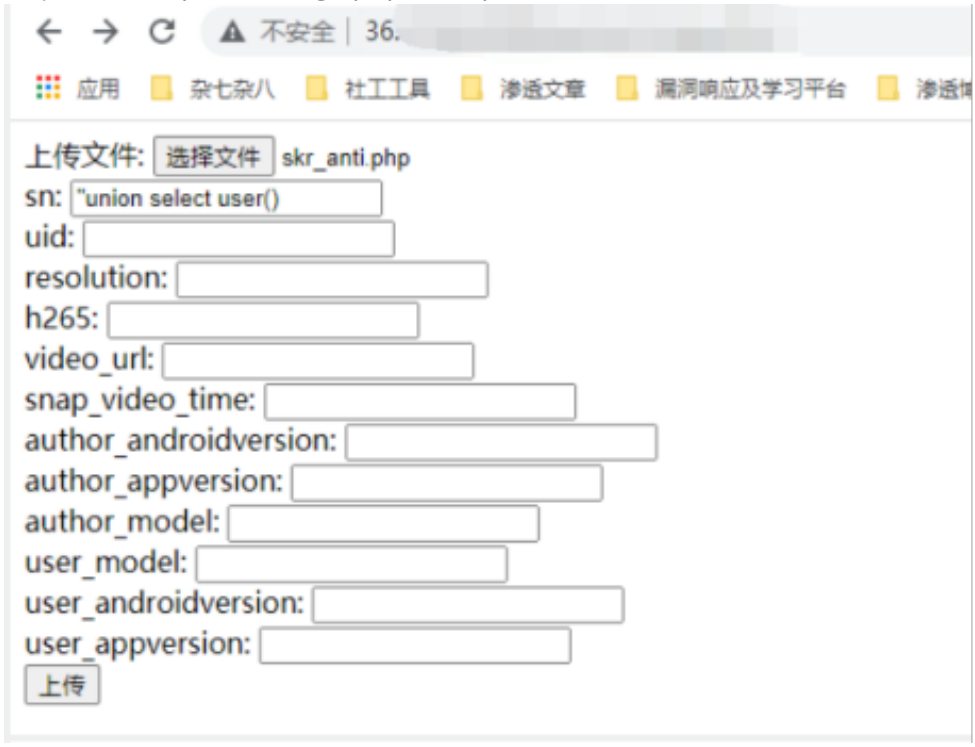


成功fuzz出一个do的参数值，upload



构造url

http://36...*/upload_image.php?do=upload，成功出现上传表单，

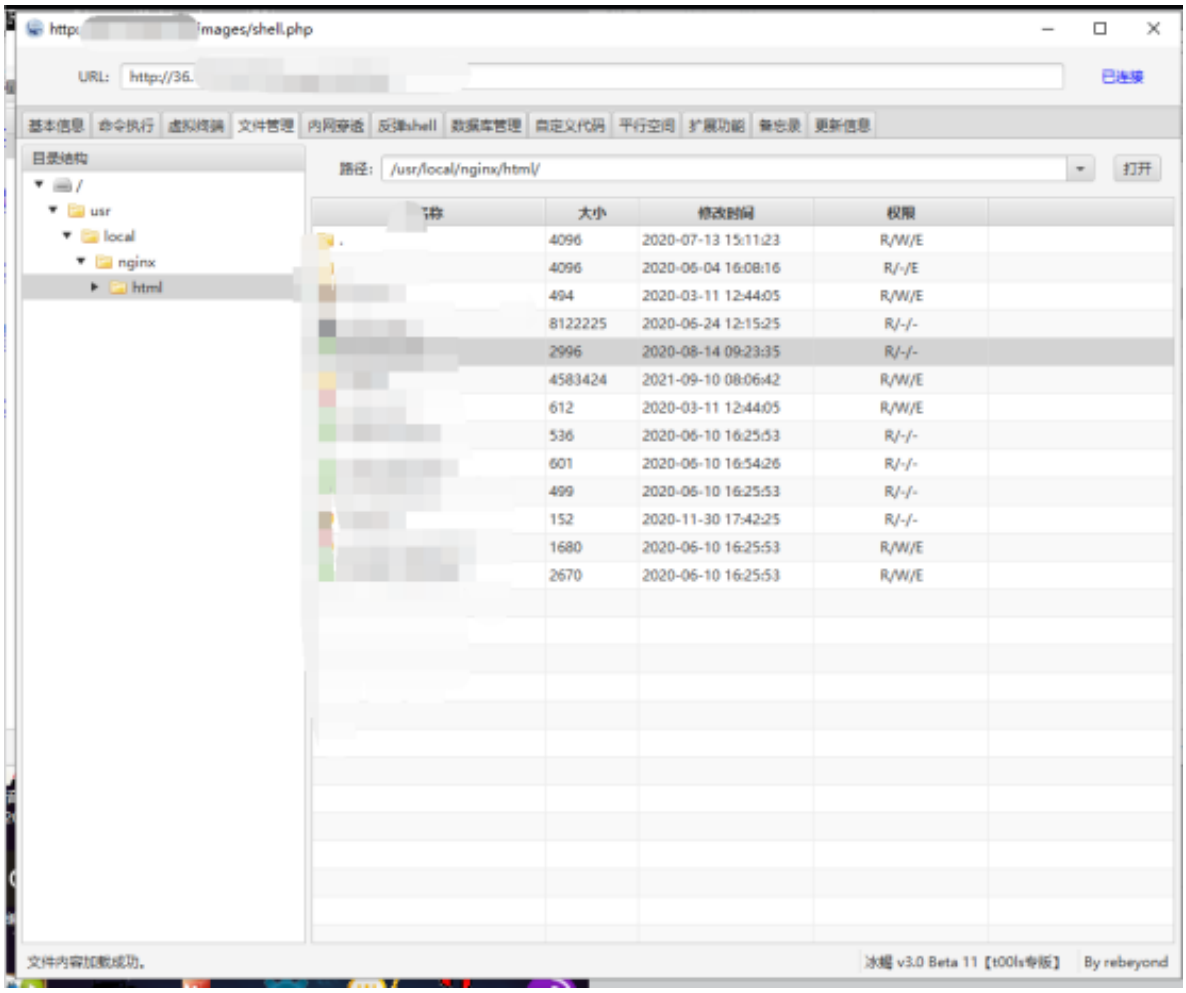


webshell名skr_anti.php

选择我们的webshell直接上传

上传后fuzz上传路径

```
http://36.*.*.*/upload  -------->  403
继续fuzz
http://36.*.*.*/upload/images  -------->  403
构造url
http://36.*.*.*/upload/images/skr_anti.php
```



赶上双倍活动，8000块钱到手

0x04 总结

我说这个漏洞有手就行，大家应该没意见吧
综合来说学习思路点如下：

1.遇到空白敏感页面/api，FUZZ参数和参数值

2.上传没返回路径不要慌，用聪明的大脑去FUZZ

3.SRC测试的时候不要上传webshell，传phpinfo就行，不然会被降赏金，我就是吃了哑巴亏。。。第一次遇着不让传webshell的

4.资产收集是红队还有渗透测试的核心