

0x01 前言

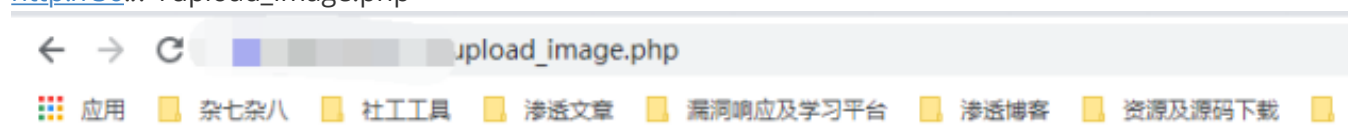
有技术交流或渗透测试培训需求的朋友欢迎联系QQ/VX-547006660

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

```
ubuntu@VM-8-6-ubuntu:~$ arjun -u https://36...

  /-|_/_/ (/_/_/ v2.1.2

[*] Probing the target for stability
[*] Analysing HTTP response for anamolies
[*] Analysing HTTP response for potential parameter names
[*] Logicforcing the URL endpoint
[✓] name: do, factor: http code
ubuntu@VM-8-6-ubuntu:~$
```

成功fuzz出一个do的参数值, upload

Intruder attack 4

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
2778	upload	200			6725	
0		200			182	
1	zbloglang	200			182	
2	rsd	200			182	
3	id	200			182	
4	ID	200			182	
5	option	200			182	
6	settings	200			182	
7	page	200			182	
8	subpage	200			182	
9	groovyInput	200			182	
10	athena_dir	200			182	
11	cmd	200			182	

Request Response

Pretty Raw \n Actions

1 GET http://... image_upload.php?do=upload HTTP/1.1
2 Host: ...
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Accept: text/plain, */*; q=0.01
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
7 X-Requested-With: XMLHttpRequest
8 Referer: ...
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
13

0 matches

Finished

构造url

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

← → ↻ ⚠ 不安全 | 36.

应用 杂七杂八 社工工具 渗透文章 漏洞响应及学习平台 渗透

上传文件: 选择文件 skr_anti.php

SN: "union select user()"

uid:

resolution:

h265:

video_url:

snap_video_time:

author_androidversion:

author_appversion:

author_model:

user_model:

user_androidversion:

user_appversion:

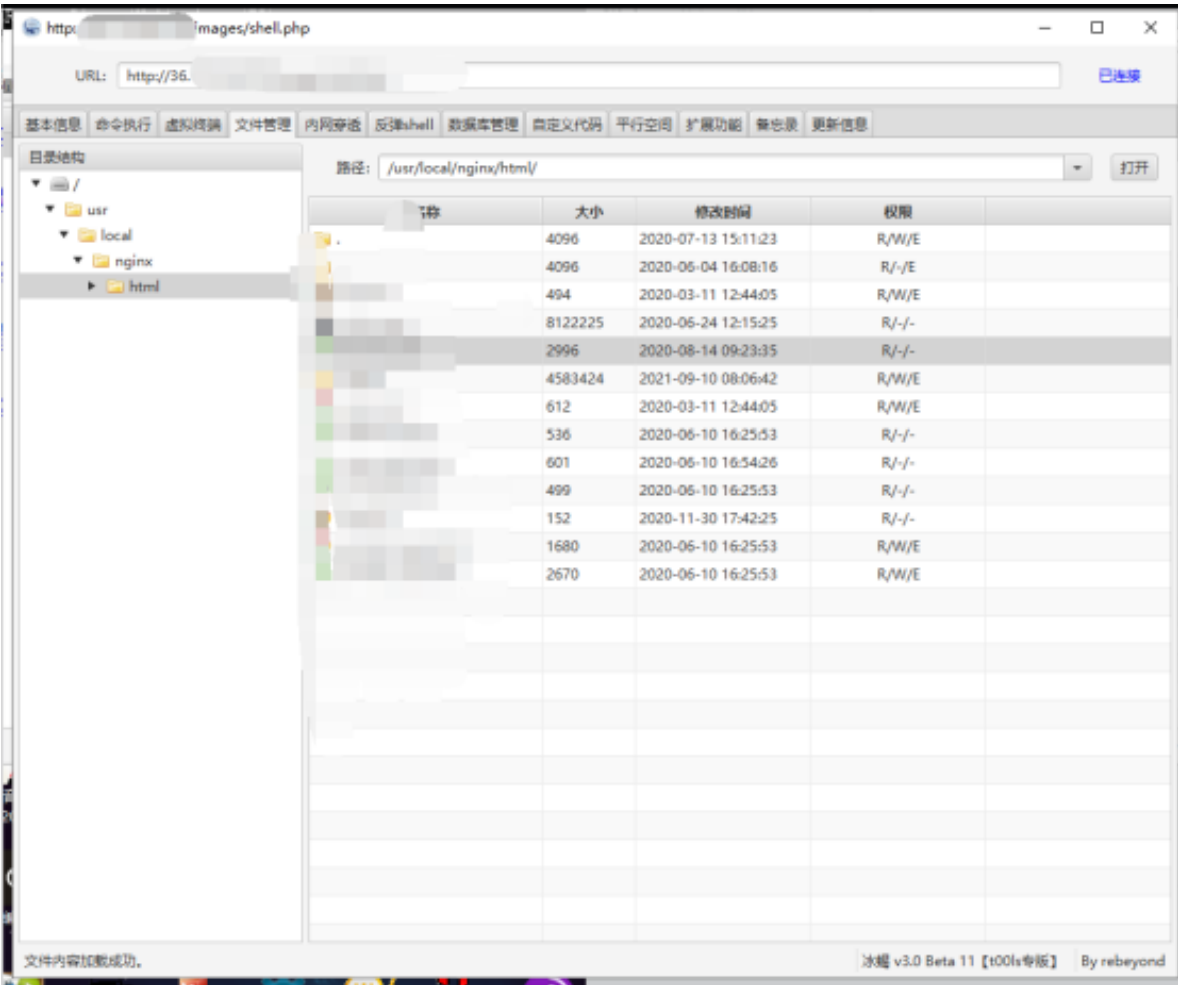
上传

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