Table of Contents

[5.1 Tool Setup: 2](#__RefHeading___Toc266_1258578044)

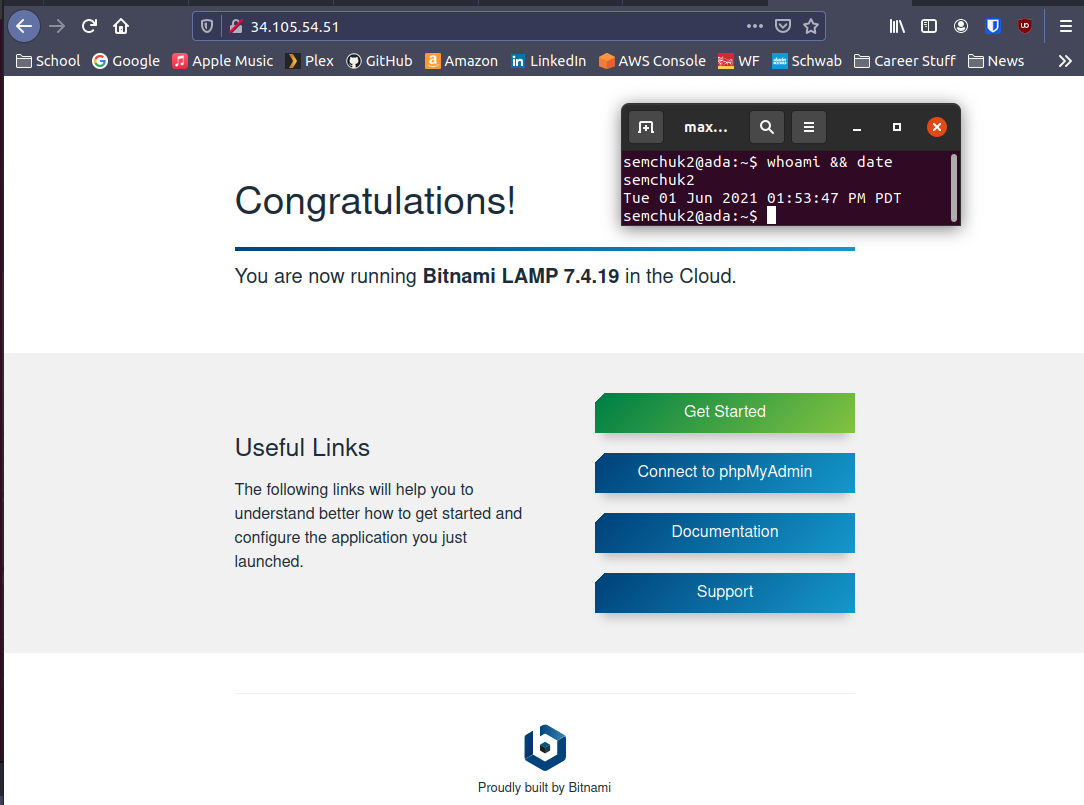
[5.2 wfuzz, nmap, bucket-stream 5](#__RefHeading___Toc268_1258578044)

[5.3 wpscan 18](#__RefHeading___Toc270_1258578044)

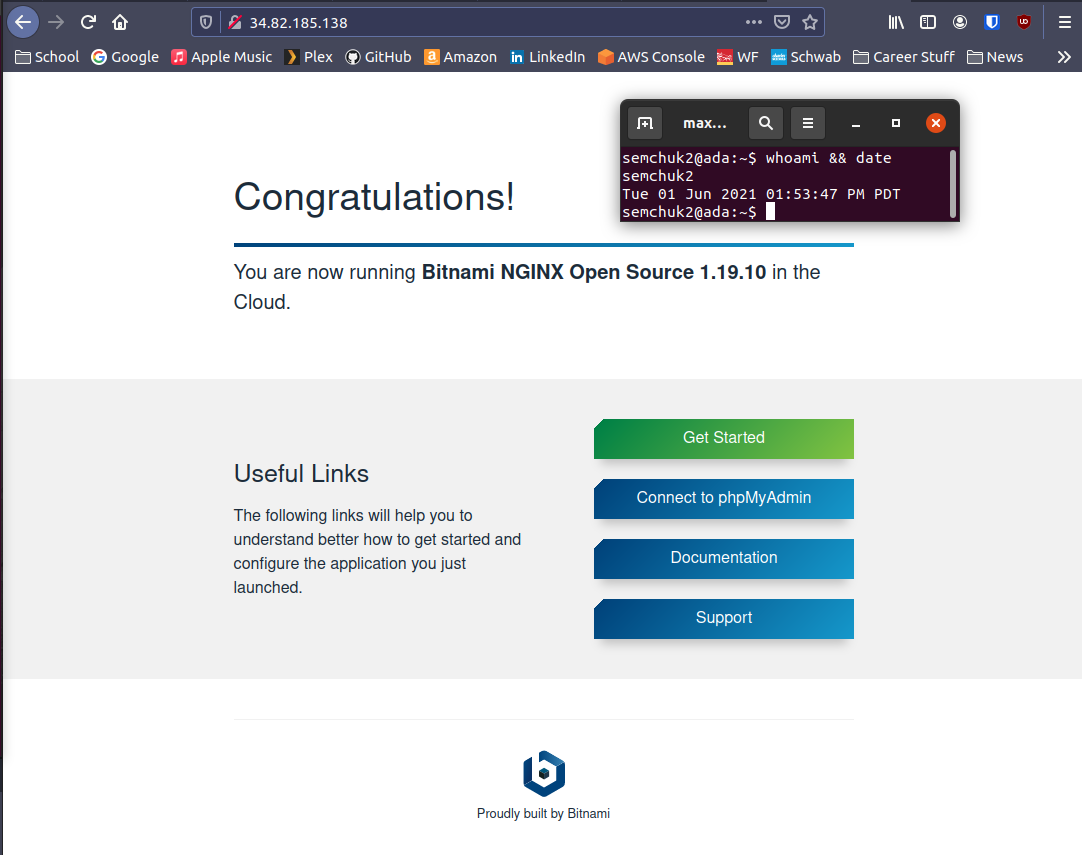
# 5.1 Tool Setup:

5.1.3 Linux Deployments (lamp, nginx)

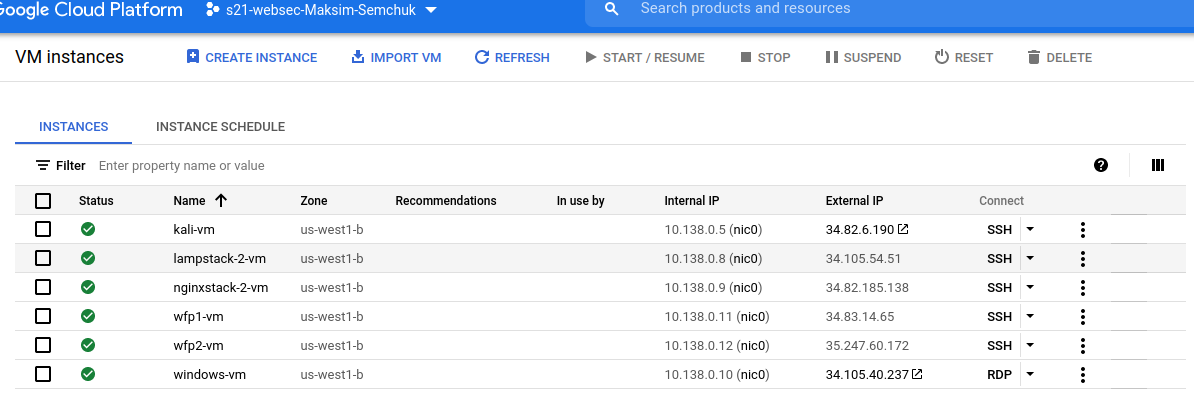
Lampstack Screenshot:



Nginx screenshot:



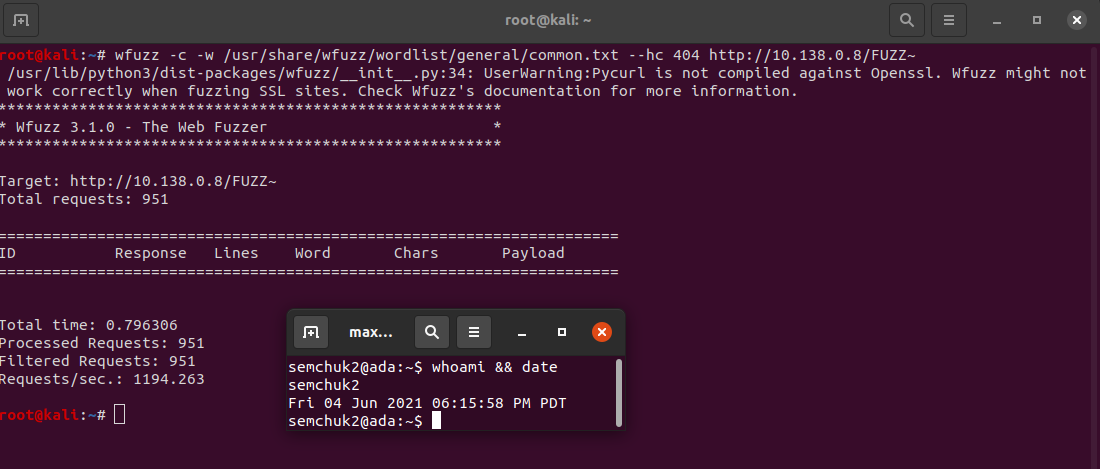
5.1.7 Internal IP addresses:



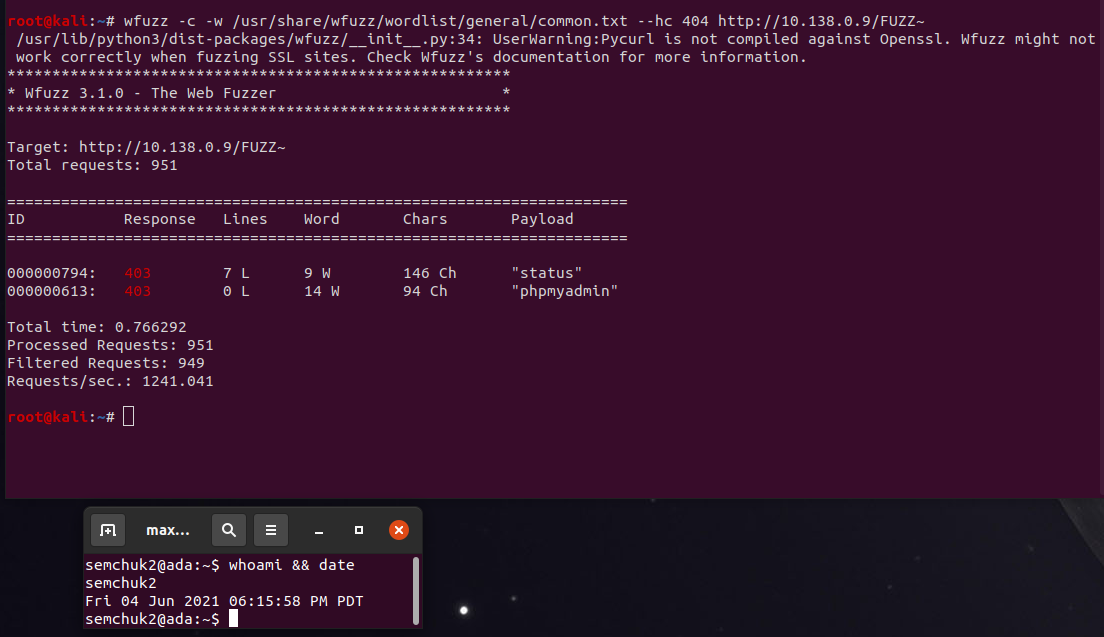
# 5.2 wfuzz, nmap, bucket-stream

5.2.1 wfuzz

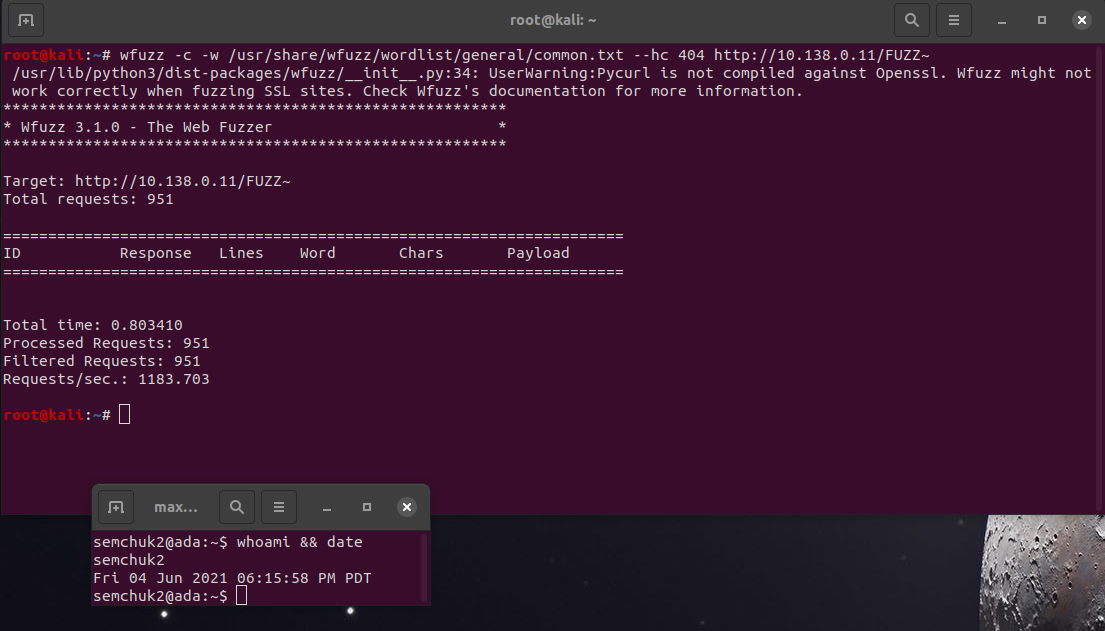
lampstack:



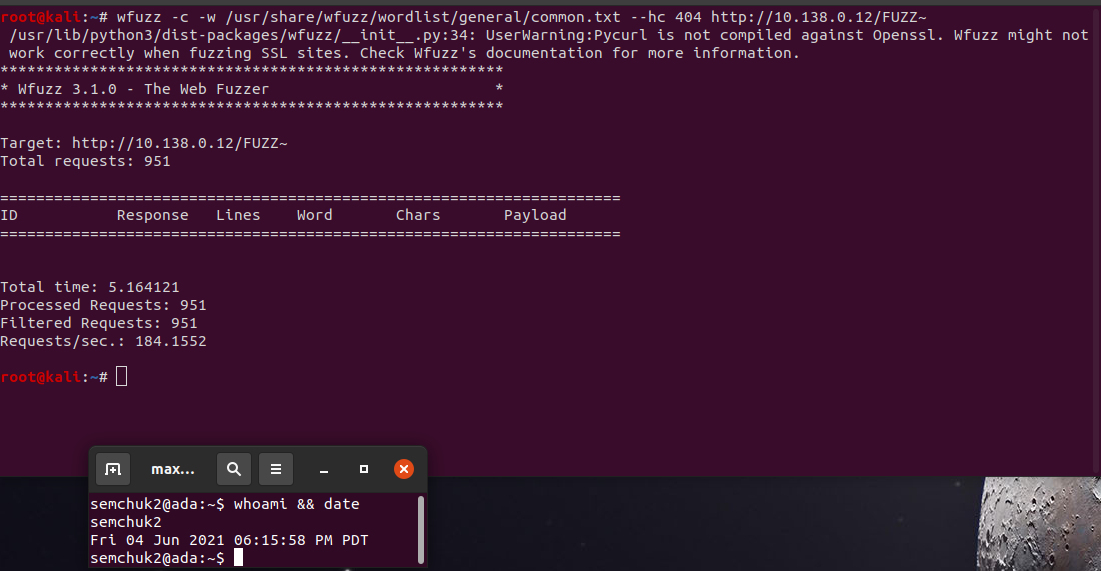
nginx:



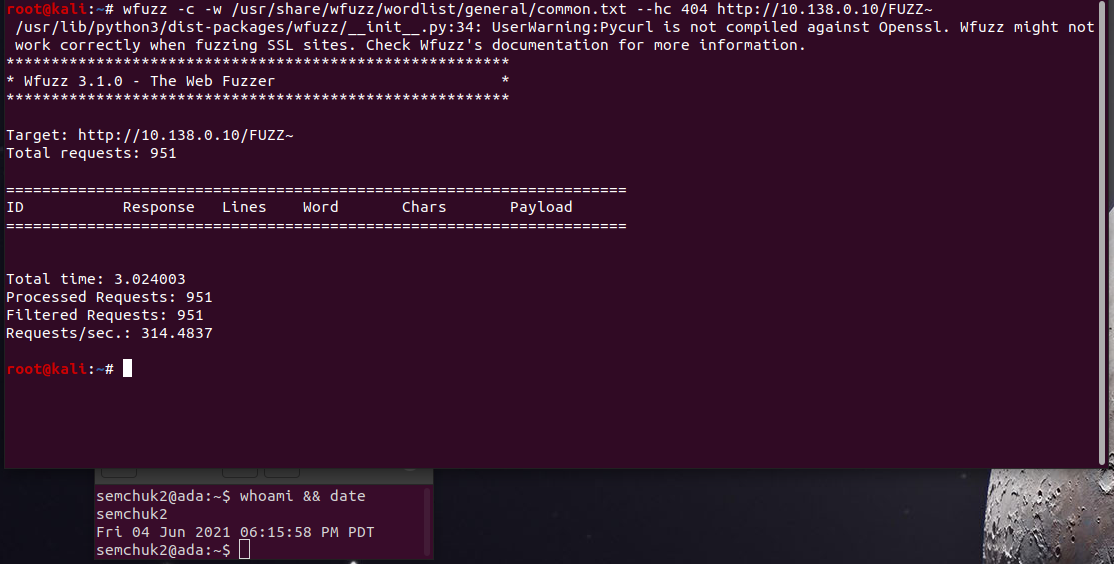
wfp1:



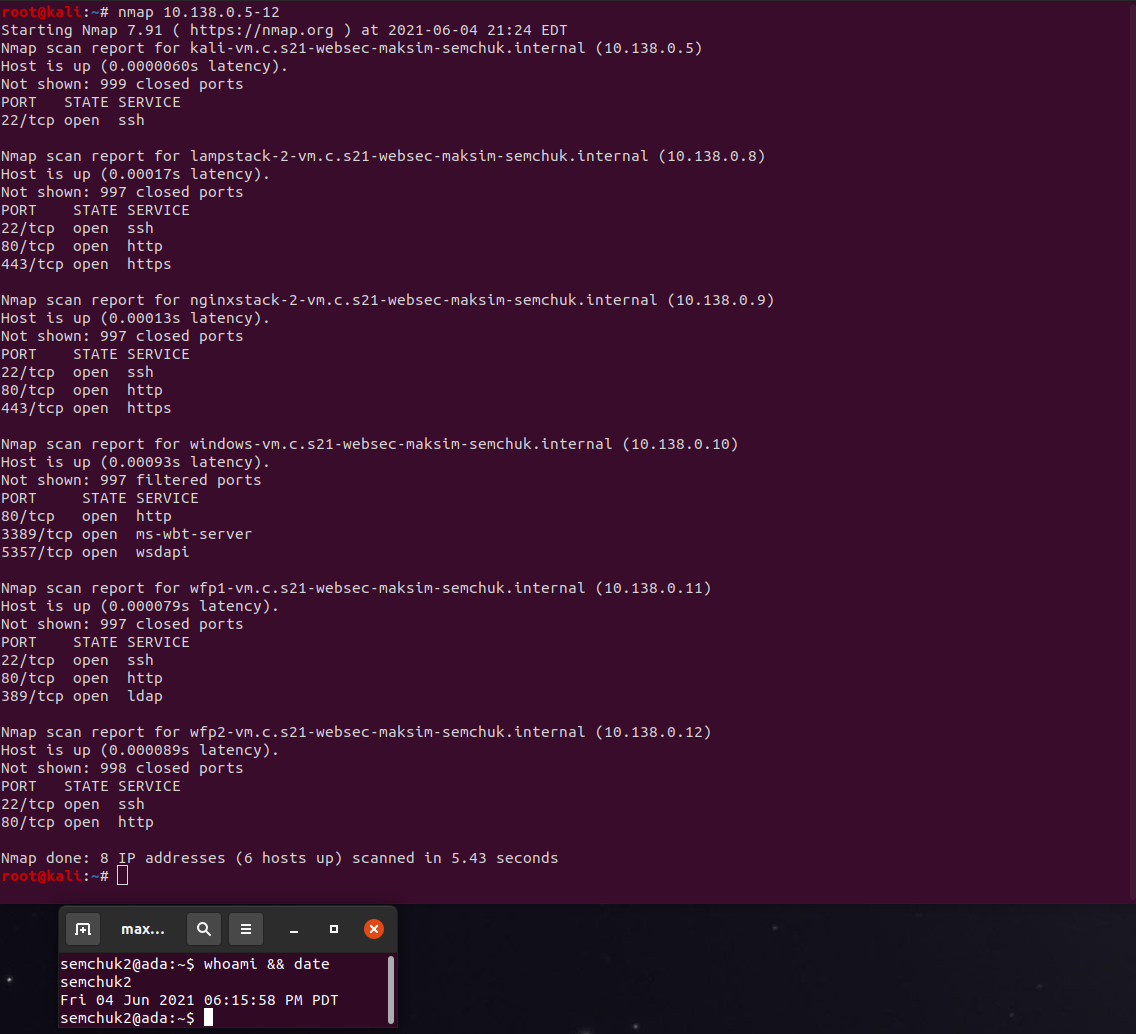
wfp2:



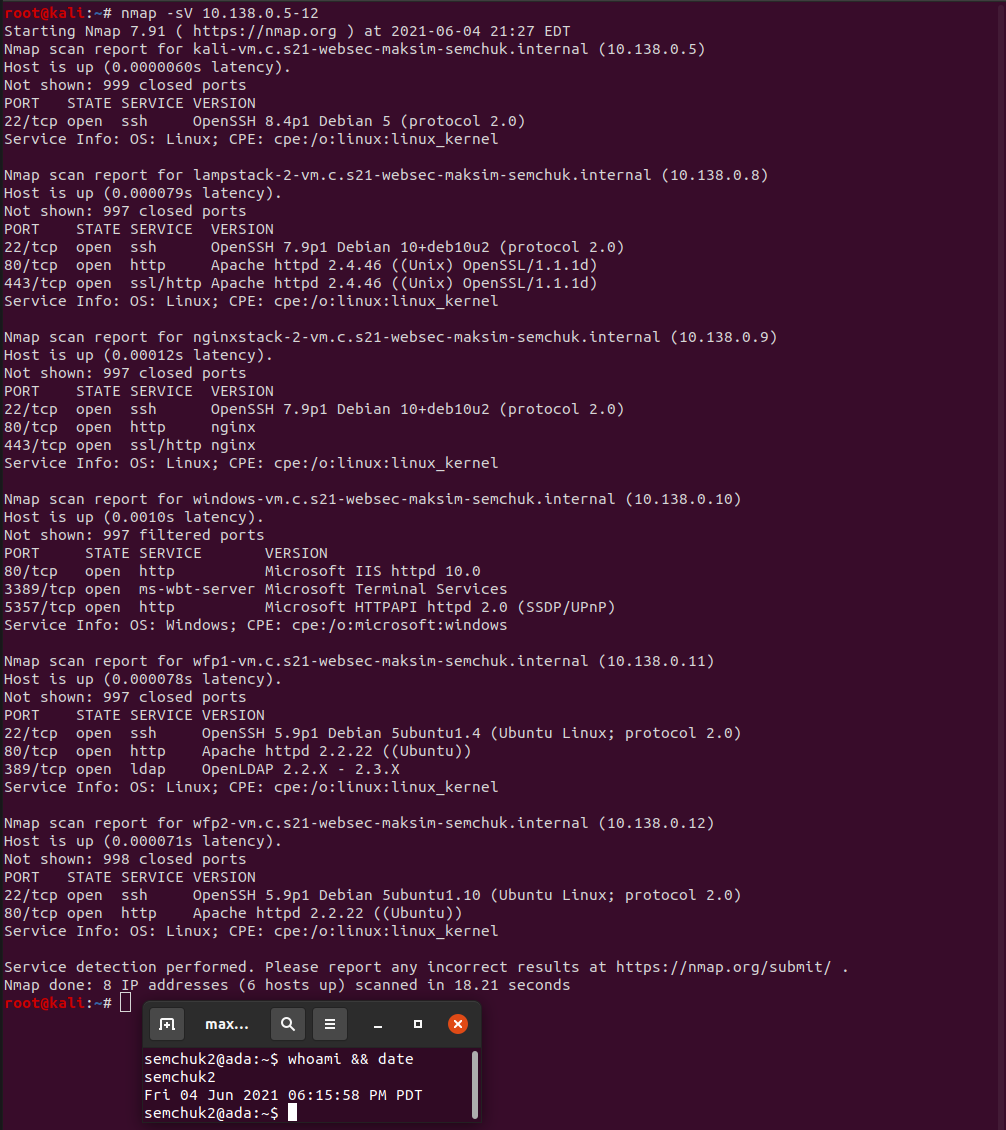
windows:



5.2.3 nmap:

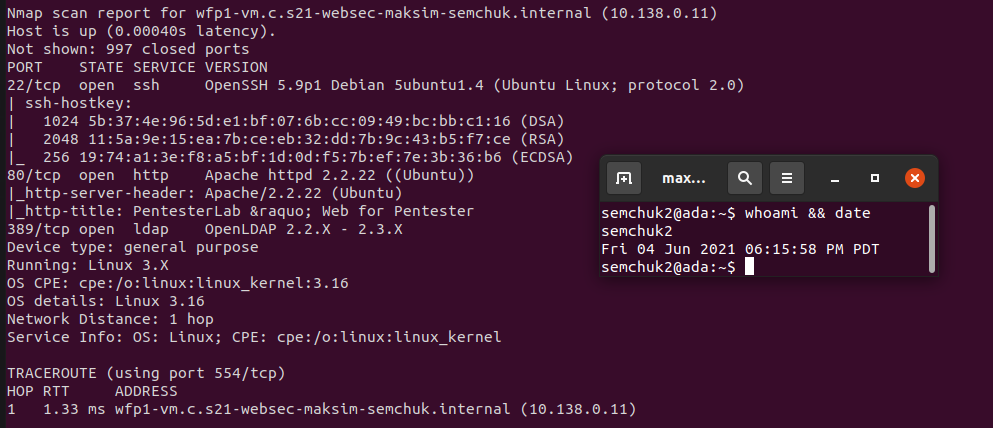


Based on the reported versions on the WFP1 VM, how old do you think the distribution being used is?



It is very old, it is a debian 5, which was released in 2012.

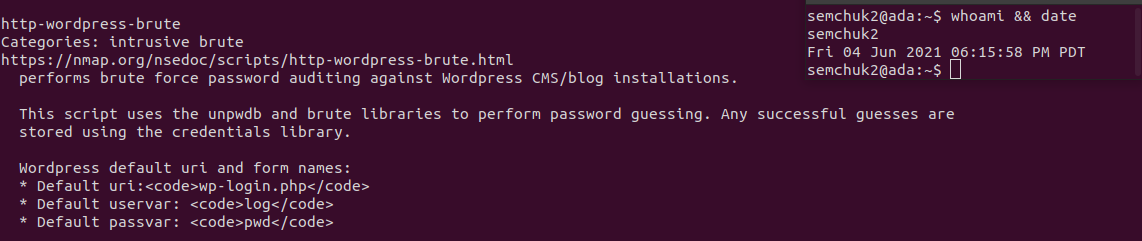
What additional kinds of information is returned when adding the -A flag versus the previous?



It returns more detailed information about the system

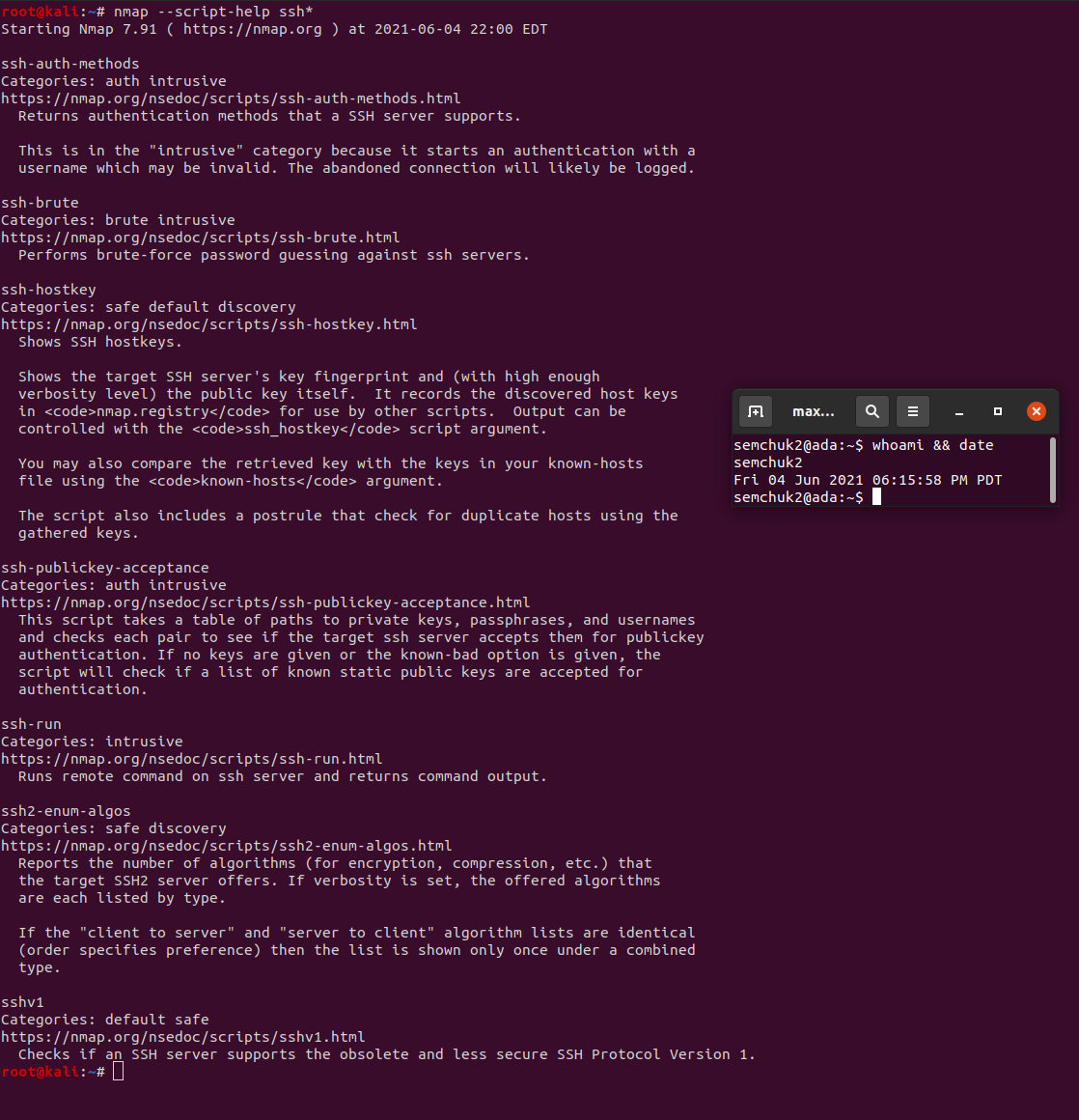
5.2.4 nmap script library

Then, find the name of the script that performs a brute-force attack on WordPress users and include it in your lab notebook.



Then, find the name of the script that checks the authentication methods supported by a server and include it in your lab notebook.

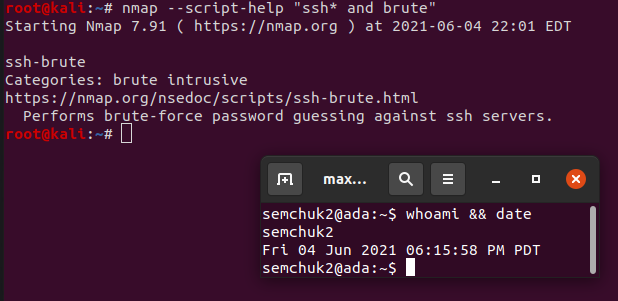
Ssh\*



http\*

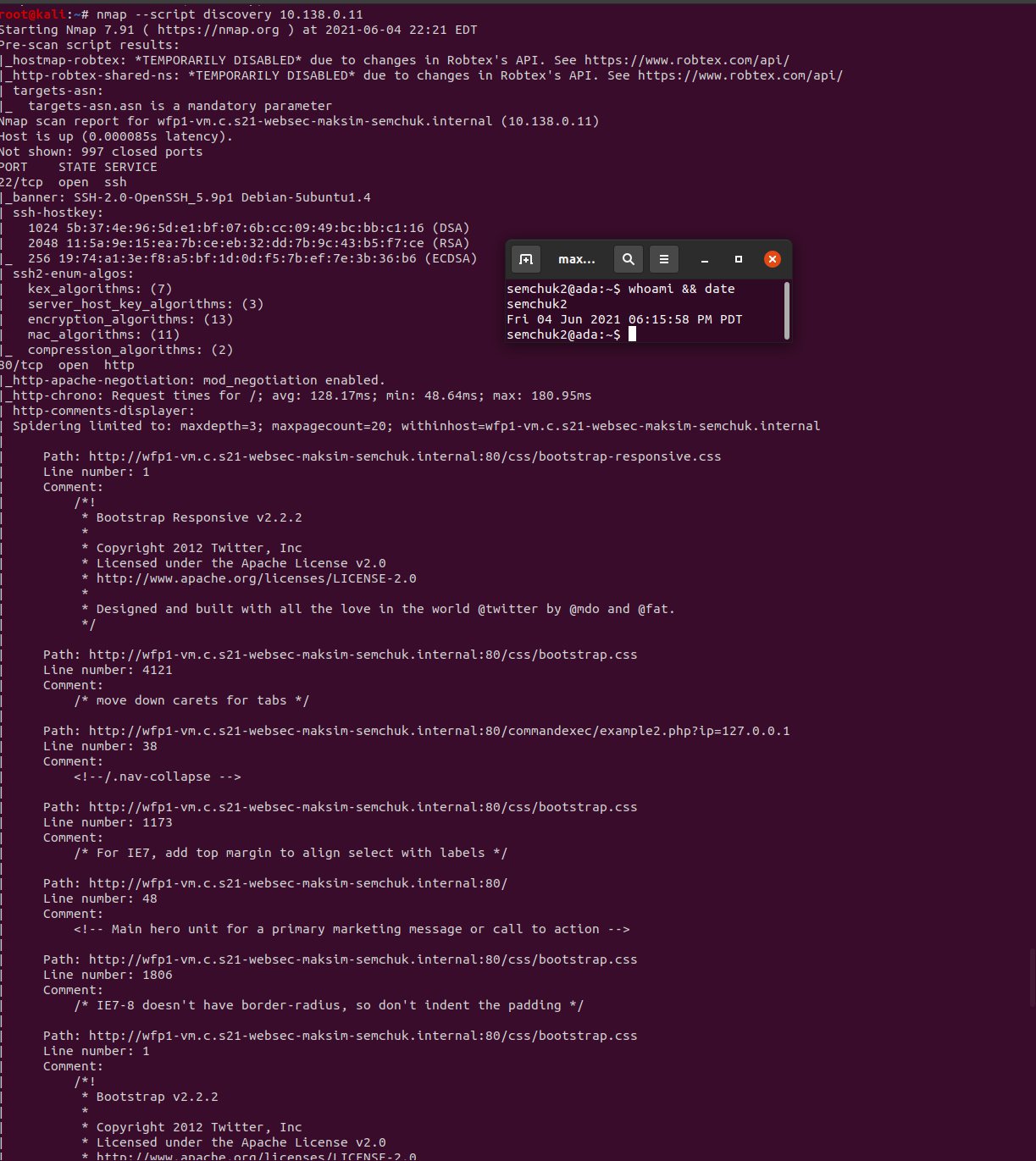


Run the example below to find the name of the script that performs a brute-force attack on ssh and include it in your lab notebook

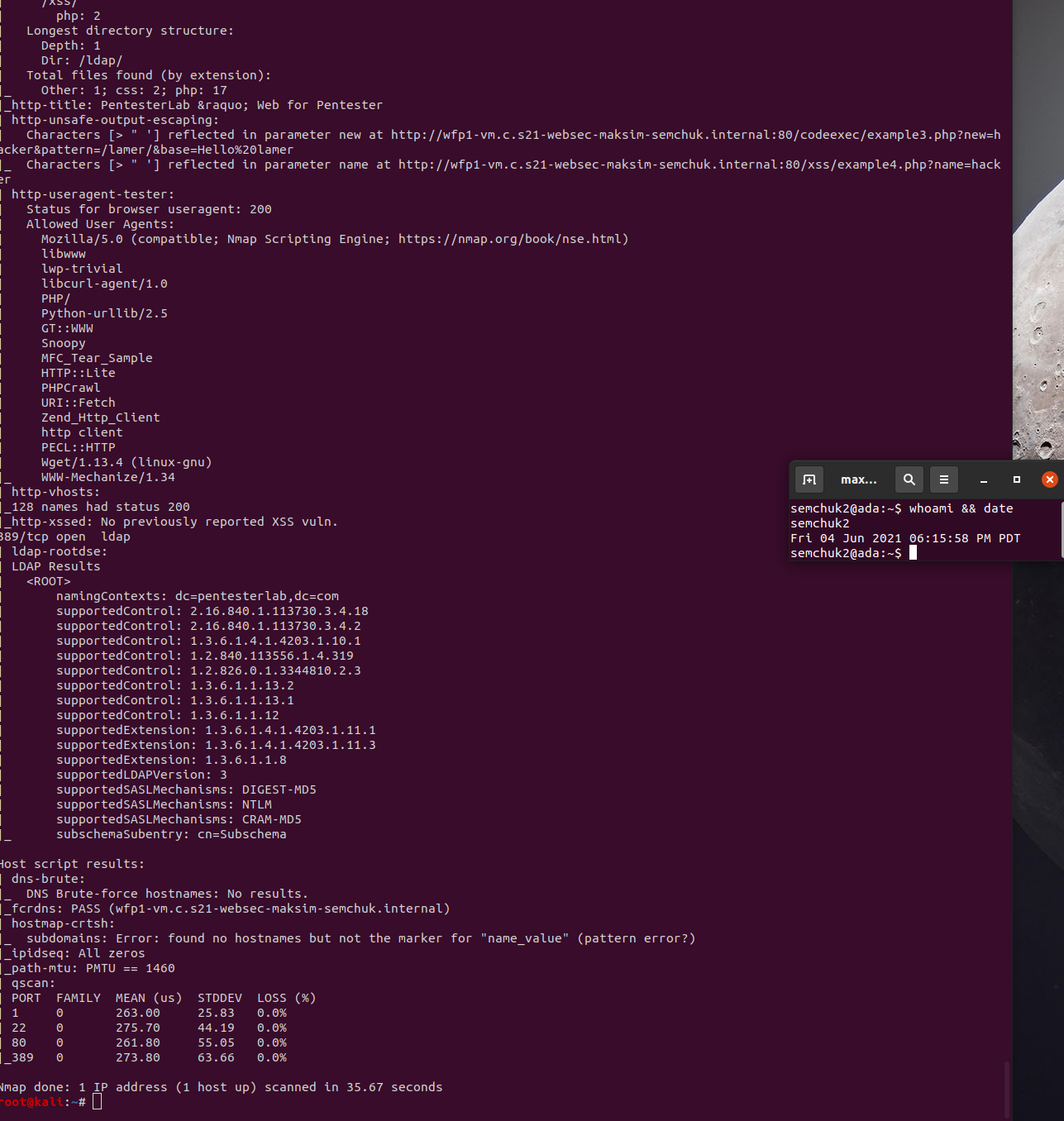


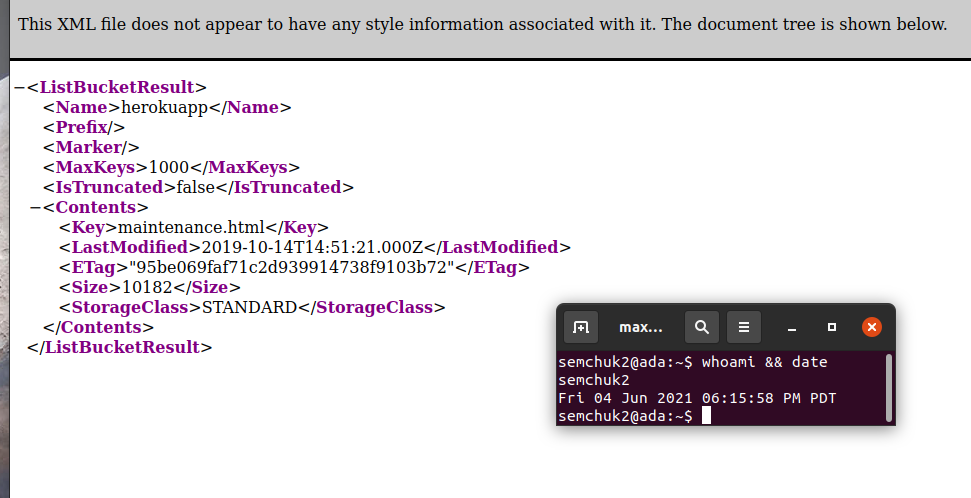
5.2.5 nmap script execution:

What is the name of the script that corresponds to the same function that wfuzz provides? Show a screenshot of its section of the nmap output. Did it find the same directories that wfuzz did for WFP1?



What is the name of the script that reveals parameters that are reflected back in the output? Show a screenshot of its section of the nmap output including the vulnerable URLs that it discovers.



Show a screenshot of the file key in the manifest

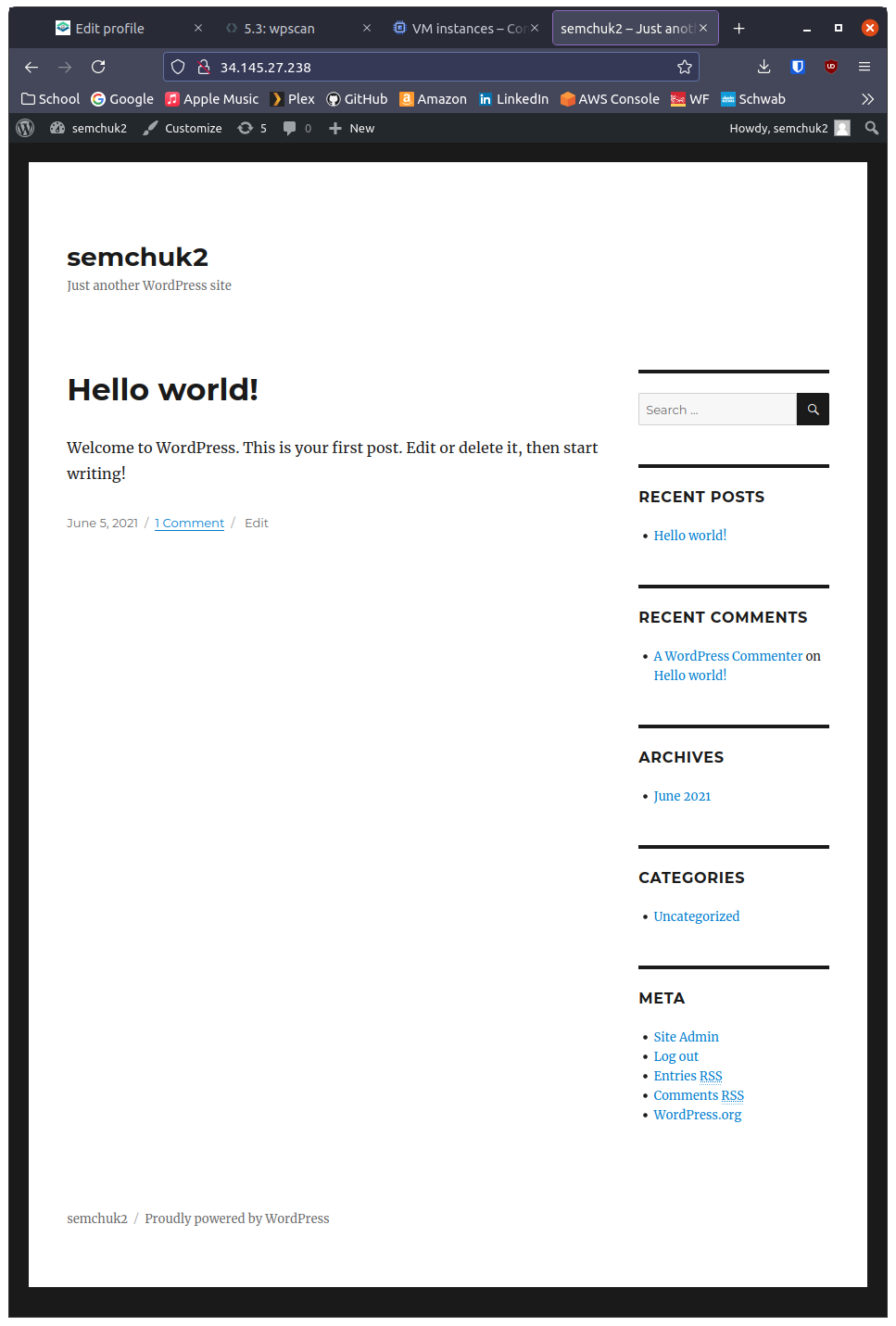
.

# 5.3 wpscan

API Token: apgkErsMmzKCdBRJL0al61bmi2aZZjMlkMhVit9T0NY

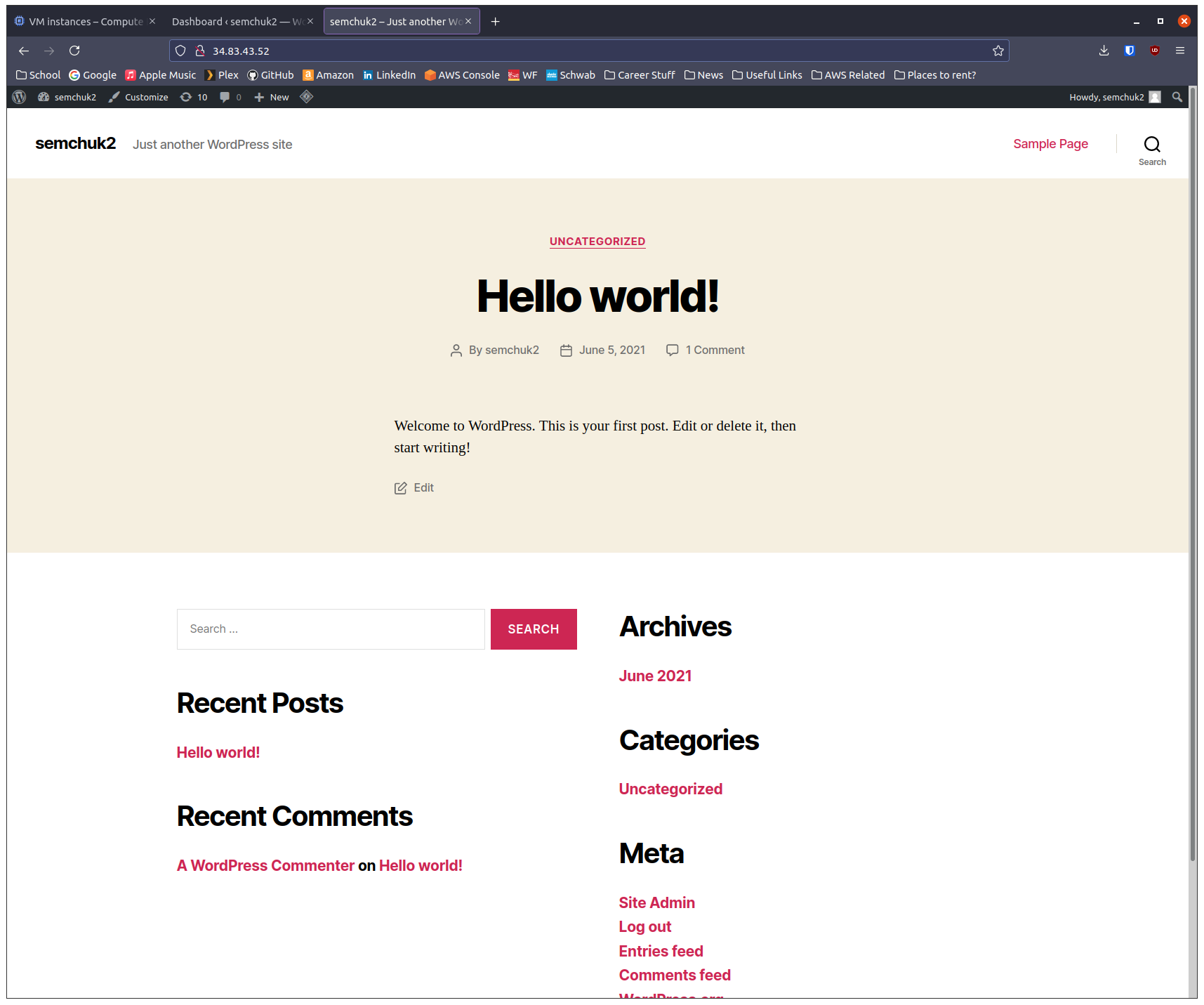
username: semchuk2

password: se3ZW^Ur1a7c^6O&oA

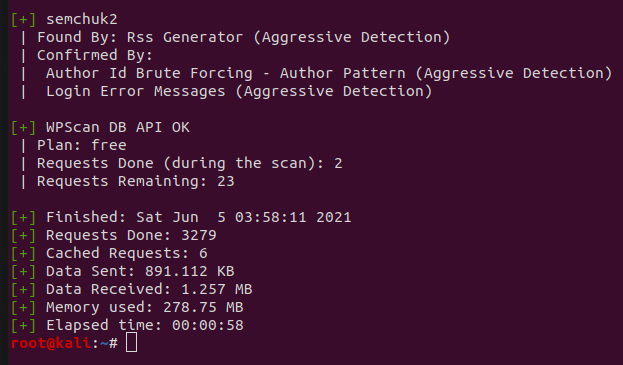


5.3.3

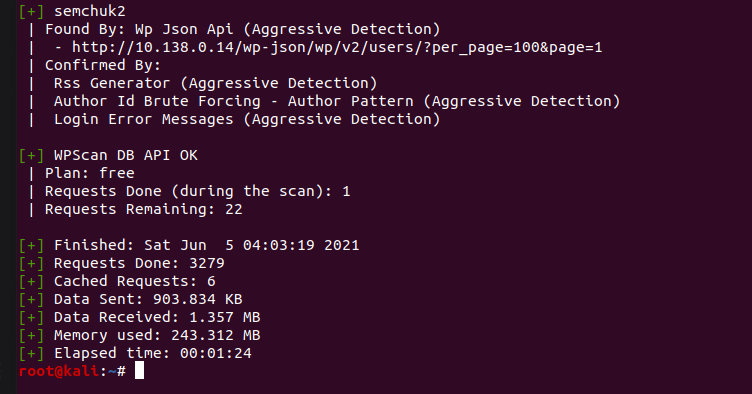
Take a screenshot of it with its address.



Wordpress46: 10.138.0.13

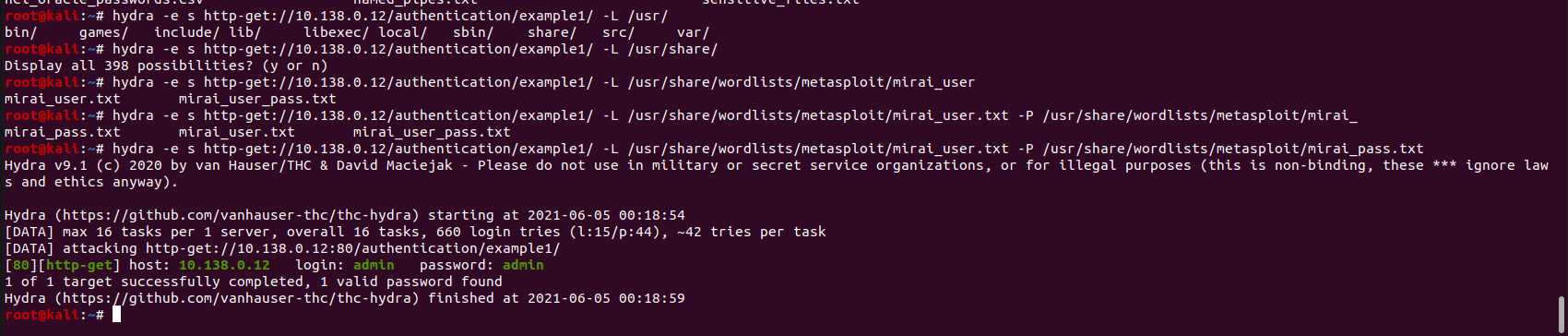


openlitespeed-wordpress: 10.138.0.14:



# 5.4 hydra, sqlmap, xsstrike, commix:

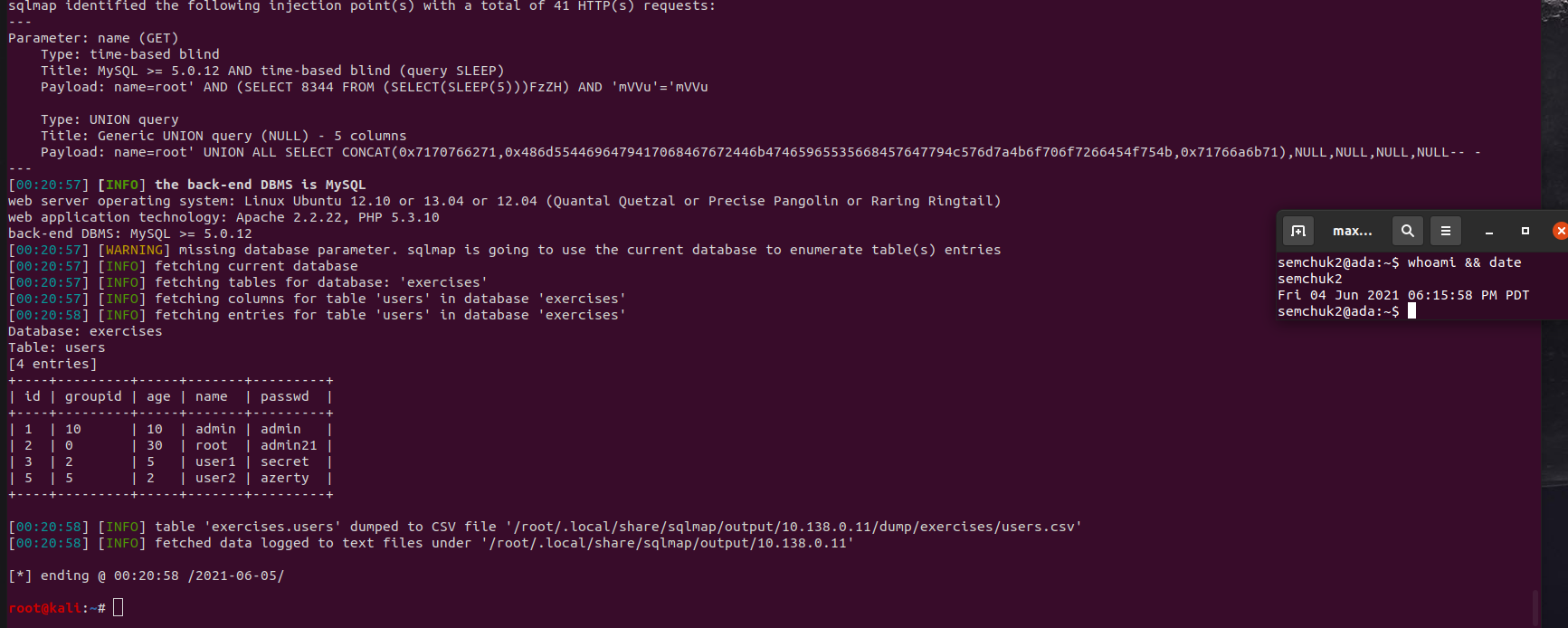
5.4.1



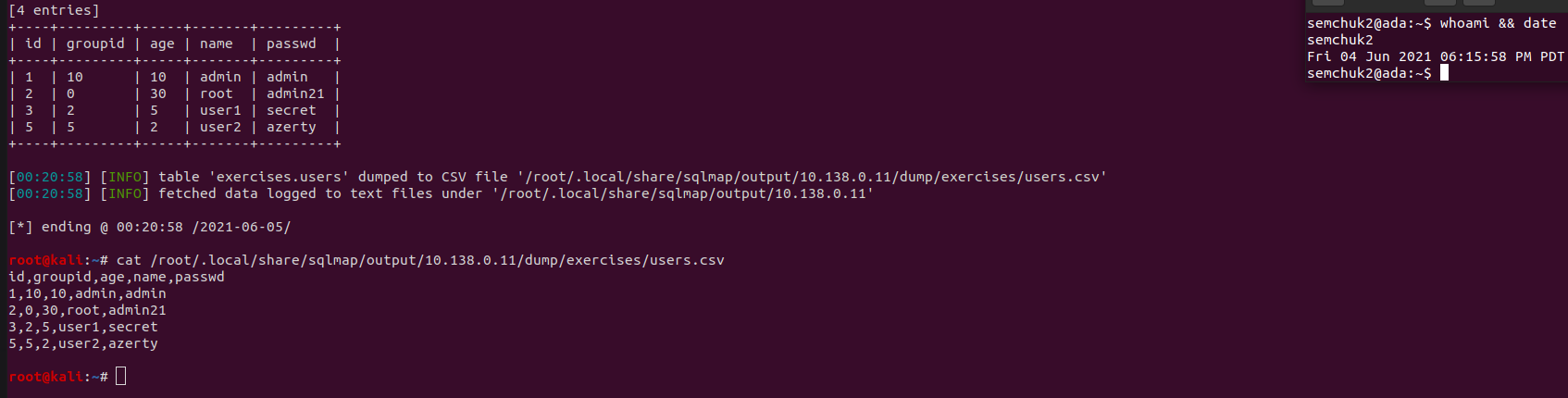
admin:admin is login for examples1

5.4.2 sqlmap:

Show screenshots of the injection points discovered and the payloads used to exploit them



Show the dump of the user table



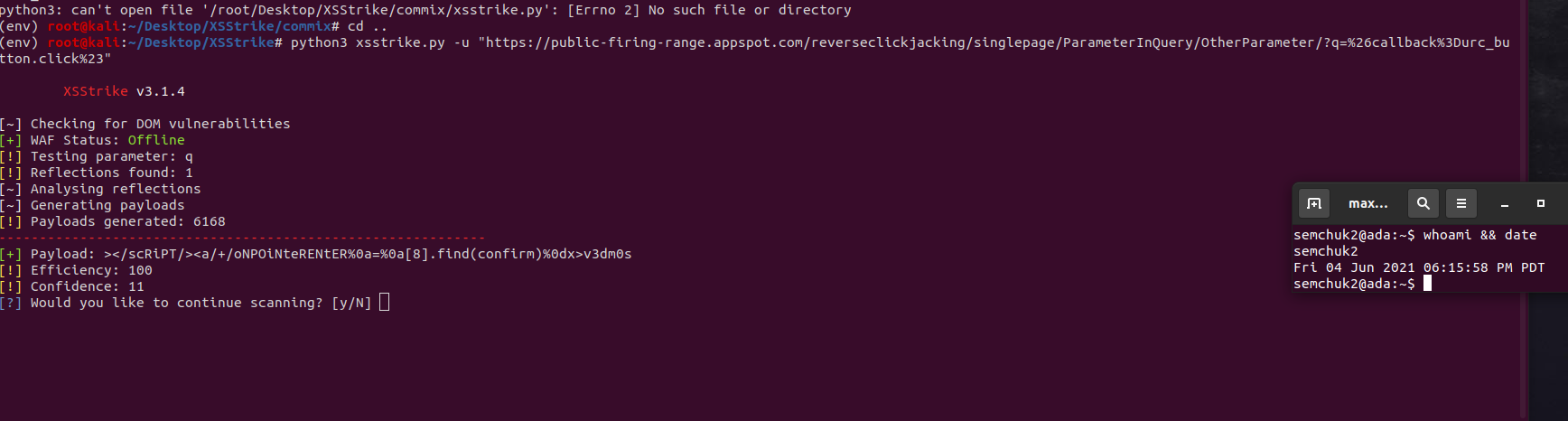
5.4.3 xsstrike:

Show a screenshot of the payload that the tool finds to exploit the vulnerability with as close to 100% efficiency as possible. Copy and paste the payload into the URL and trigger the XSS. Show a screenshot of the successful exploit.

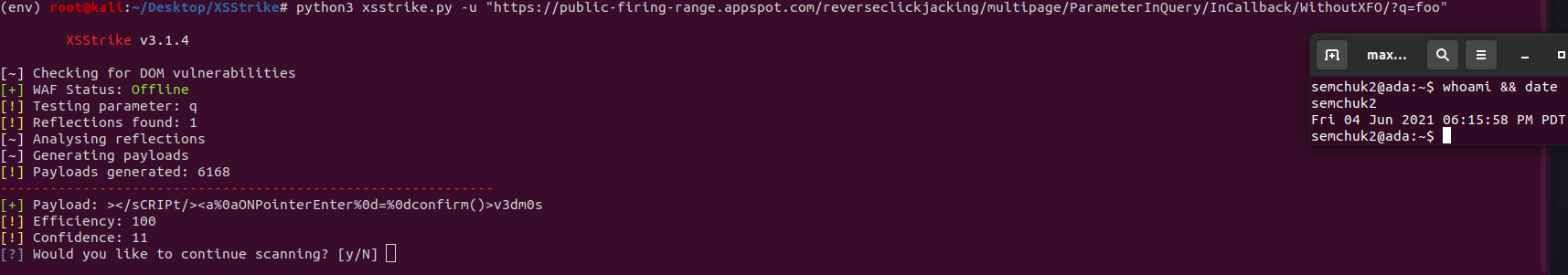


Show a screenshot of each payload and the URL it exploits

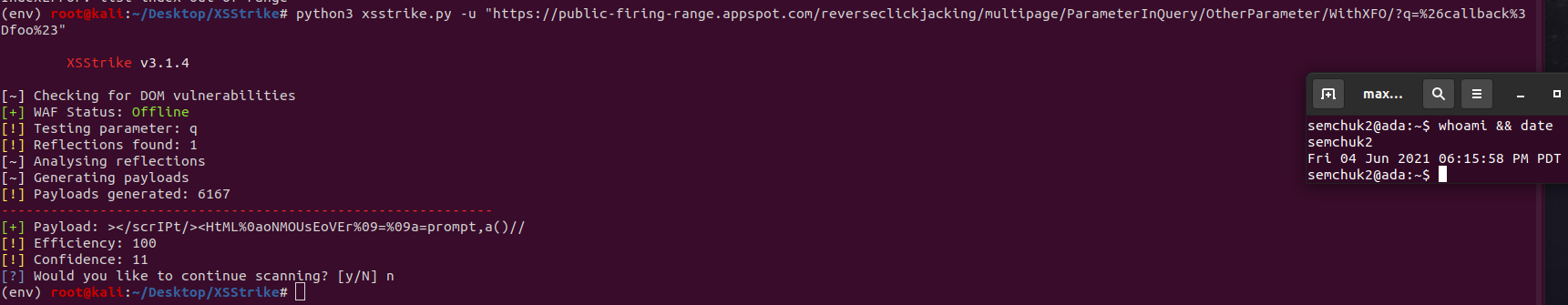
1



2

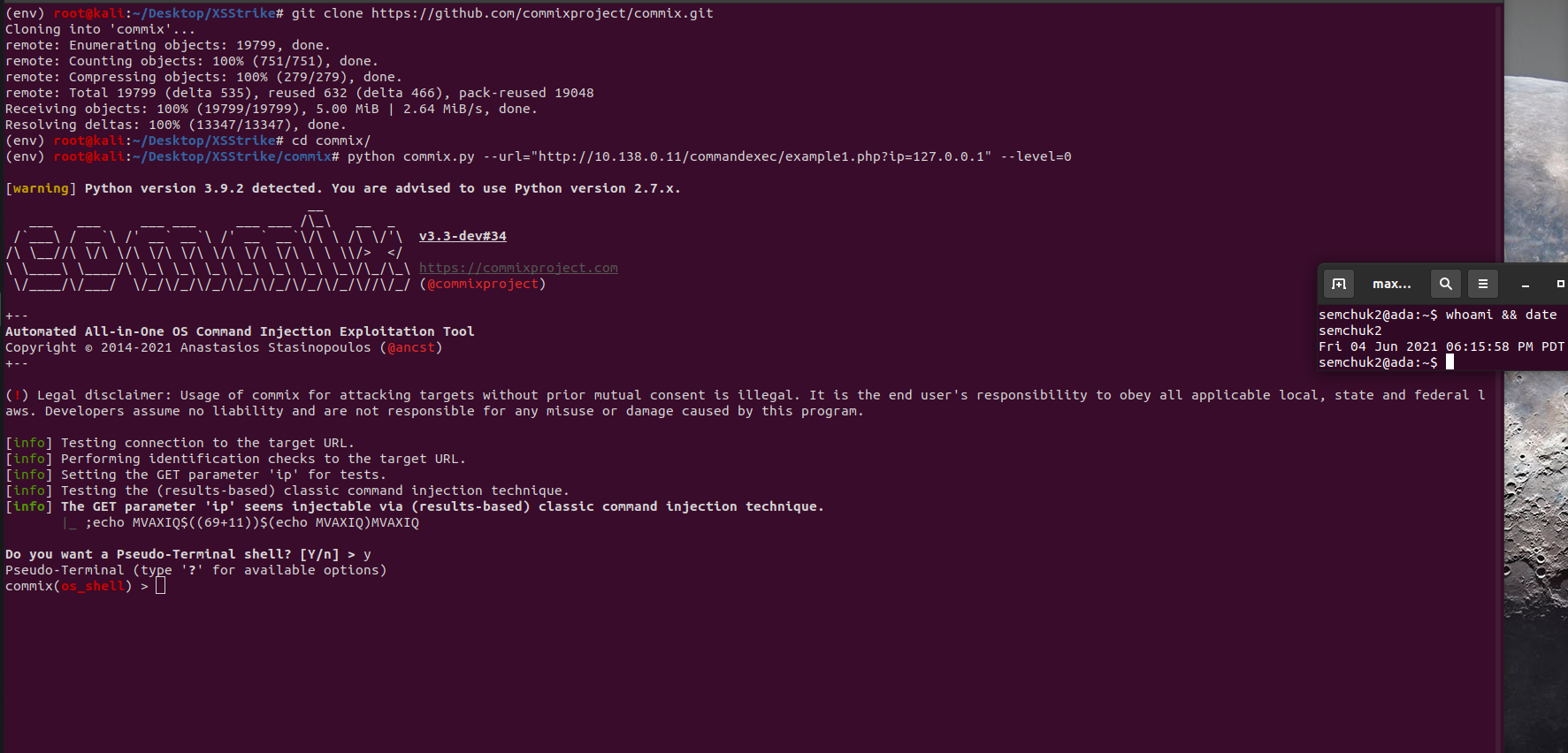


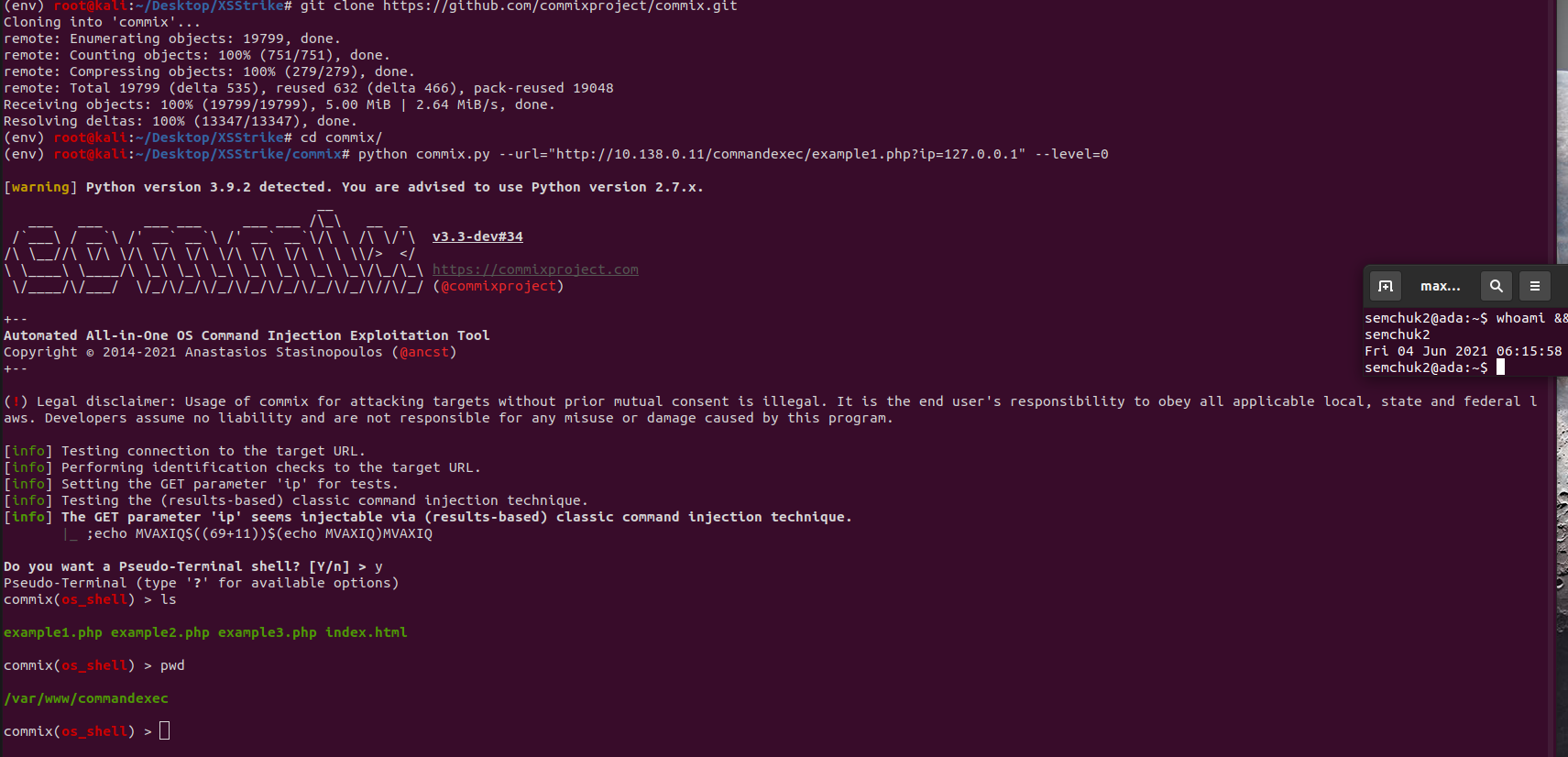
3



5.4.4 commix:

Show a screenshot of the payload that the tool finds to discover the vulnerability.



 Perform an 'ls' and a 'pwd' and show the results in screenshots showing you have obtained access.

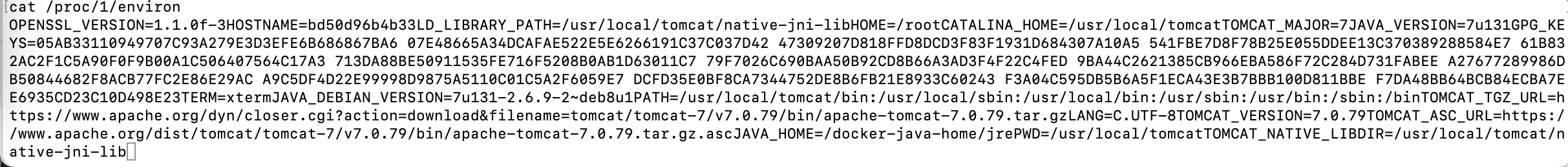
# 5.5 metasploit:

5.5.2

Graphical user interface, text, application, letter, email

Description automatically generated

Pwd, ls, id, ps auxww command results.



For the process that launched the server, show a screenshot of its environment variables as revealed via /proc

5.5.3

A picture containing graphical user interface

Description automatically generated

Results of running dir scanner

A picture containing text

Description automatically generated

Result of running Metasploit http credentials stuffing: found admin:admin as user:password.