How [not] to suck at CTF

Olivier Bilodeau

Warning

You are about to enter a mystical universe filled with inconsistencies and various types of abuse.

You have been warned.

CENTAURICORN

The galaxy's greatest warrior

VERY DEMOTIVATIONAL .com

OWASP
Open Web Application
Security Project

Avertissement

Présentation surchargée d'anglicismes!

OWASP
Open Web Application
Security Project

Avertissement

- Stressez pas a prendre des notes de tools, y'a pas de contenu pertinent dans cette présentation.

$ whoami

- Cybersecurity Researcher at GoSecure
- Co-founder MontréHack (hands-on security workshops)
- VP Training and Hacker Jeopardy at NorthSec

GoSecure

nsec

OWASP
Open Web Application Security Project

CTF Experience

I'm off the Previous Generation of CTF players

- Founder Amish Security
- Founder CISSP Groupies

Anonymous

Troll

Monocle

Nyan cat

Grognons

Cuir cuir cuir moustache

un CTF c'est quoi?

CTF ⇒ Capture The Flags

Non pas comme ça…

Plutôt comme ça

Dans les faits ce sont...

- hacking games
- hacking puzzles
- computer science puzzle
- nerd puzzles

Myth: CTF are about information security

comment ça marche?

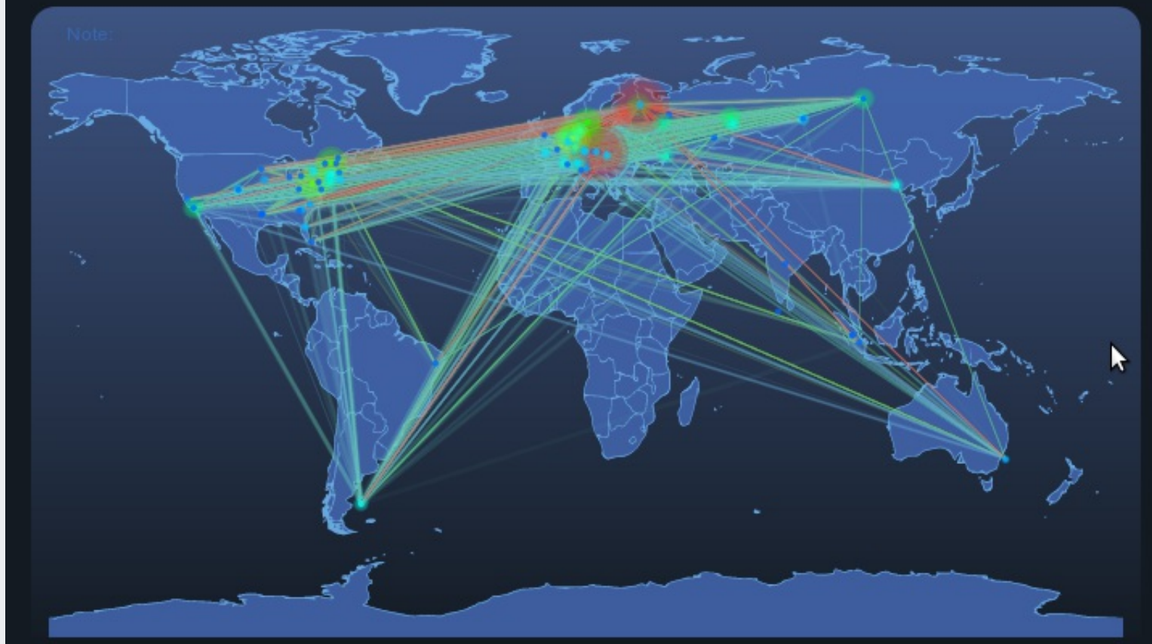
- des gens créatifs et généreux font des scénarios et défis
- les participants arrivent (ou se loggent)
- on cherche des flags
- on soumet les flags à un système de pointage

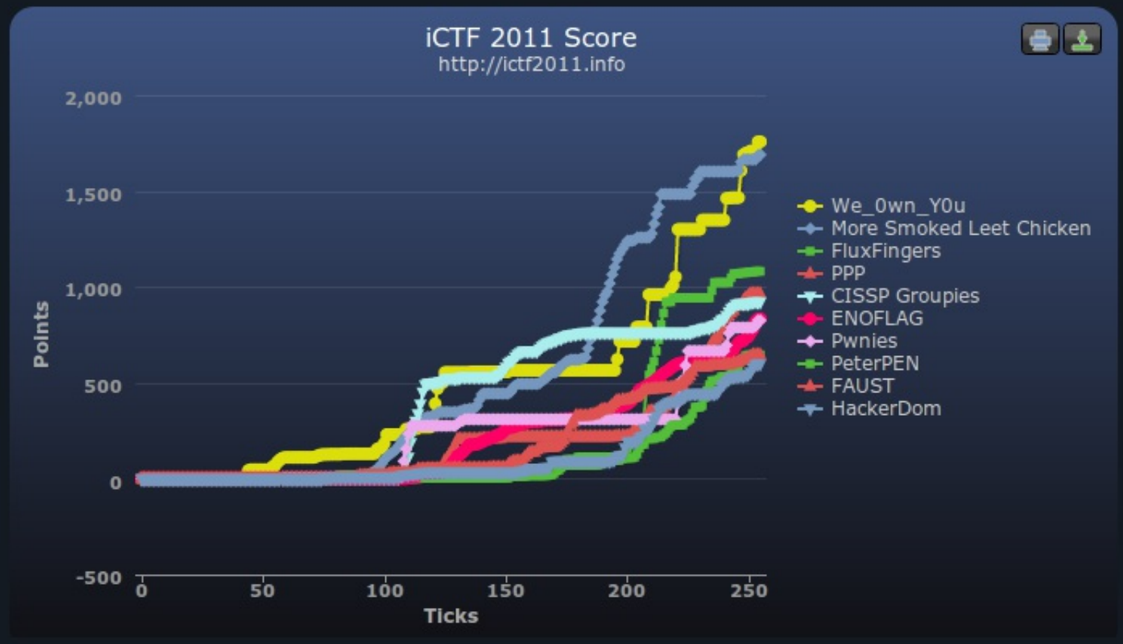
scoreboard.ictf2011.info - Google Chrome

chal 48 - olivier.bilo | Snitch | iCTF2011 - Groupie | Who Solved What | iCTF 2010 - Challen | mule company - Re | challenge_21 | best mule company | scoreboard.ictf201

scoreboard.ictf2011.info

iCTF 2011 Scoreboard





#	Team	Country	Points	Money	convic..	egoats	mailga..	msgdis..	mulead..	mulema..	mulema..	muleus..	sendal..	smsgat..
1	We_0wn_Y0u	AT	1757.2	67	✗	✓🔒	✓🔒	✓🔒	✗	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒
2	More Smoked Leet Chicken	RU	1688.3	27	✗	✗	✗	✓🔒	✗	✓🔒	✓🔒	✗	✓🔒	✓🔒
3	FluxFingers	DE	1081.1	150	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒	✗
4	PPP	US	965.4	35	✗	✗	✓🔒	✓🔒	✗	✓🔒	✓🔒	✗	✓🔒	✓🔒
5	CISSP Groupies	CA	923.1	30	✗	✓🔒	✗	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒	✓🔒
6	ENOFLAG	DE	834.1	0	✓🔒	✓🔒	✗	✓🔒	✗	✗	✓🔒	✗	✓🔒	✓🔒
7	Pwnies	DK	827.4	199	✗	✓🔒	✗	✓🔒	✗	✗	✓🔒	✗	✓🔒	✓🔒

chart.pdf | network1.pcap | challenge_23.html | reverse1.exe

Afficher tous les téléchargements...

Les "fameux" flags

- parfois sous la forme FLAG:abcdefgh...
- sinon {FLAG:...}
- ou encore The flag is: abcdefgh...
- ou juste: 112f3a99b283a4e1788dedd8e0e5d35375c33747
- ou même: ceciestunfantastiqueflag
- mais après ont les voit partout!

La vie est un CTF

— Benjamin Vanheuverzwijn

Pourquoi participer?

- apprendre!
- sortir de sa zone de confort, constamment!
- se trouver une job le fun
- trouver du talent passionné
- les contacts

Plus de la moitié des chercheurs dans notre équipe ont été rencontrés dans des compétitions de type "CTF". Le contexte de compétition nous permet rapidement de voir les compétences techniques et sociales d'un candidat. ...

Plusieurs de nos chercheurs ont des problèmes de comportement et de consommation d'alcool mais c'est tout de même grâce à eux que nous pouvons nous vanter d'avoir la meilleure équipe de recherche en sécurité au Québec.

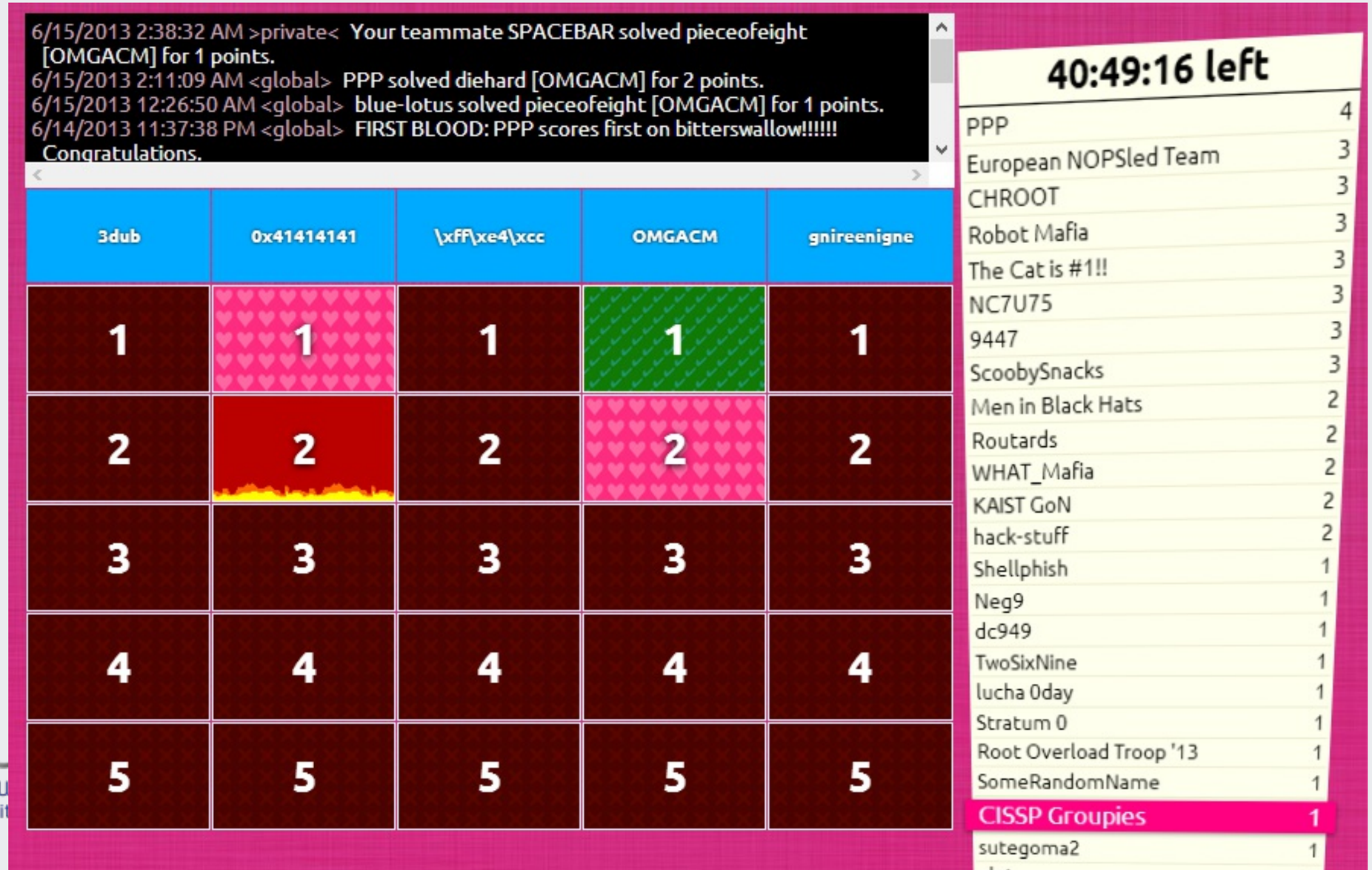
— Pierre-Marc Bureau en 2013 chez ESET Canada

OWASP
Open Web Application
Security Project

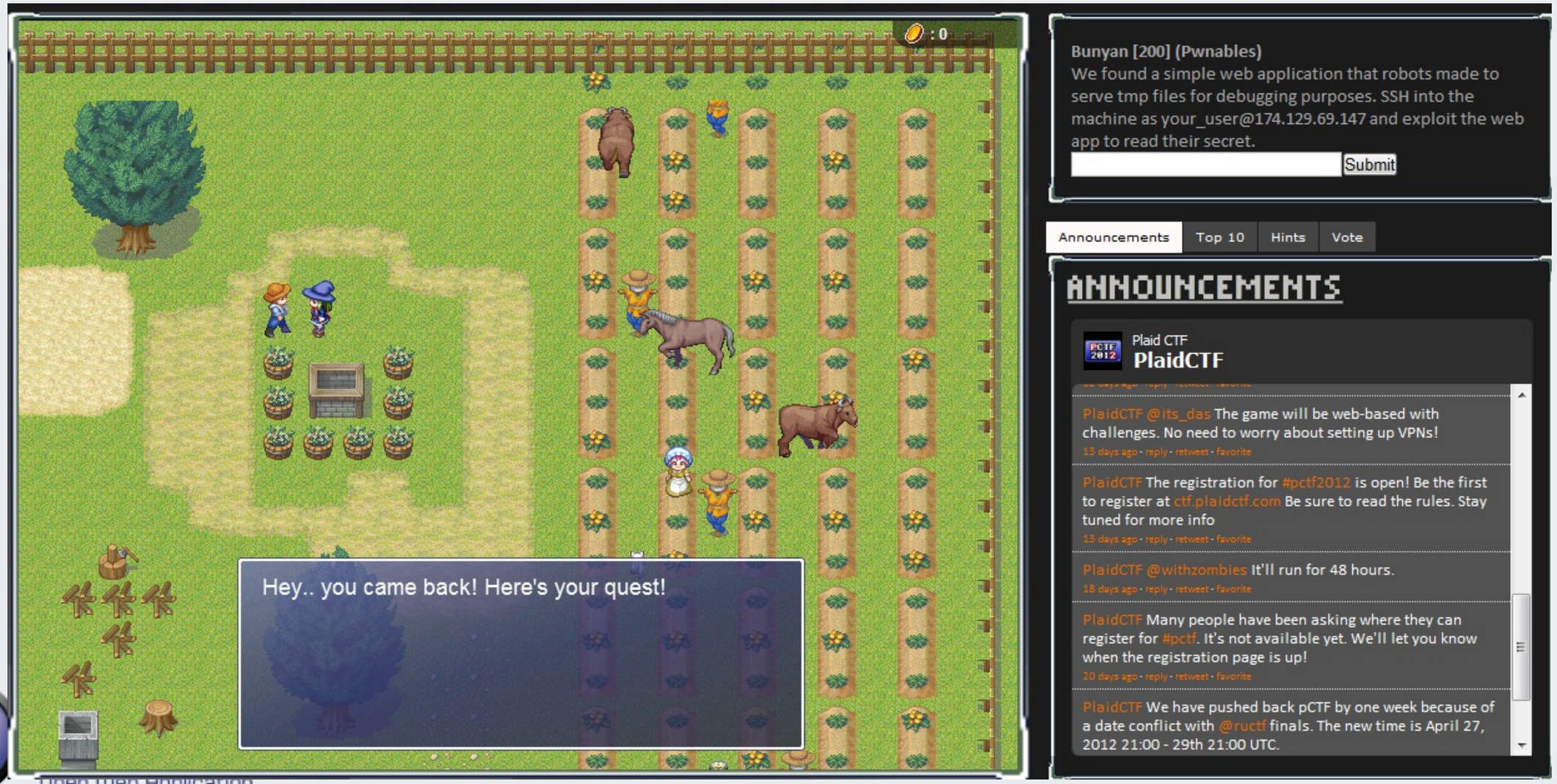
Variantes

- Cyberwar (managed, unmanaged)
- Red vs Blue
- Jeopardy board
- Javascript-RPG
- Batshit insane (iCTF)
- ...

Jeopardy Board



Javascript RPG



Perks

- on-site || off-site || hybrid
- besoin d'affiliation académique
- limite de membres

Exemples de sujets explorés

- Exploitation
  - Web
  - System
  - hw

Sujets explorés (suite)

- Cryptographie
  - 1st gen: craptographie, enigma
  - 2nd gen: hashs, puzzles, small-RSA, password cracking, etc.
  - current-gen: crypto-oracle, big int maths

Sujets explorés (suite)

- reverse-engineering
- forensic
- réseautique
- stégano

Sujets explorés (suite)

- recon
- system hardening
- algo
- lock-pick
- specialized platforms (Android, iOS, haiku, BSDs, VMS, ...)

mais attention!

C’est de plus en plus dur

Tout le monde a une histoire

La mienne a commencé a la Boule de cristal du CRIM

Cipher CTF 4

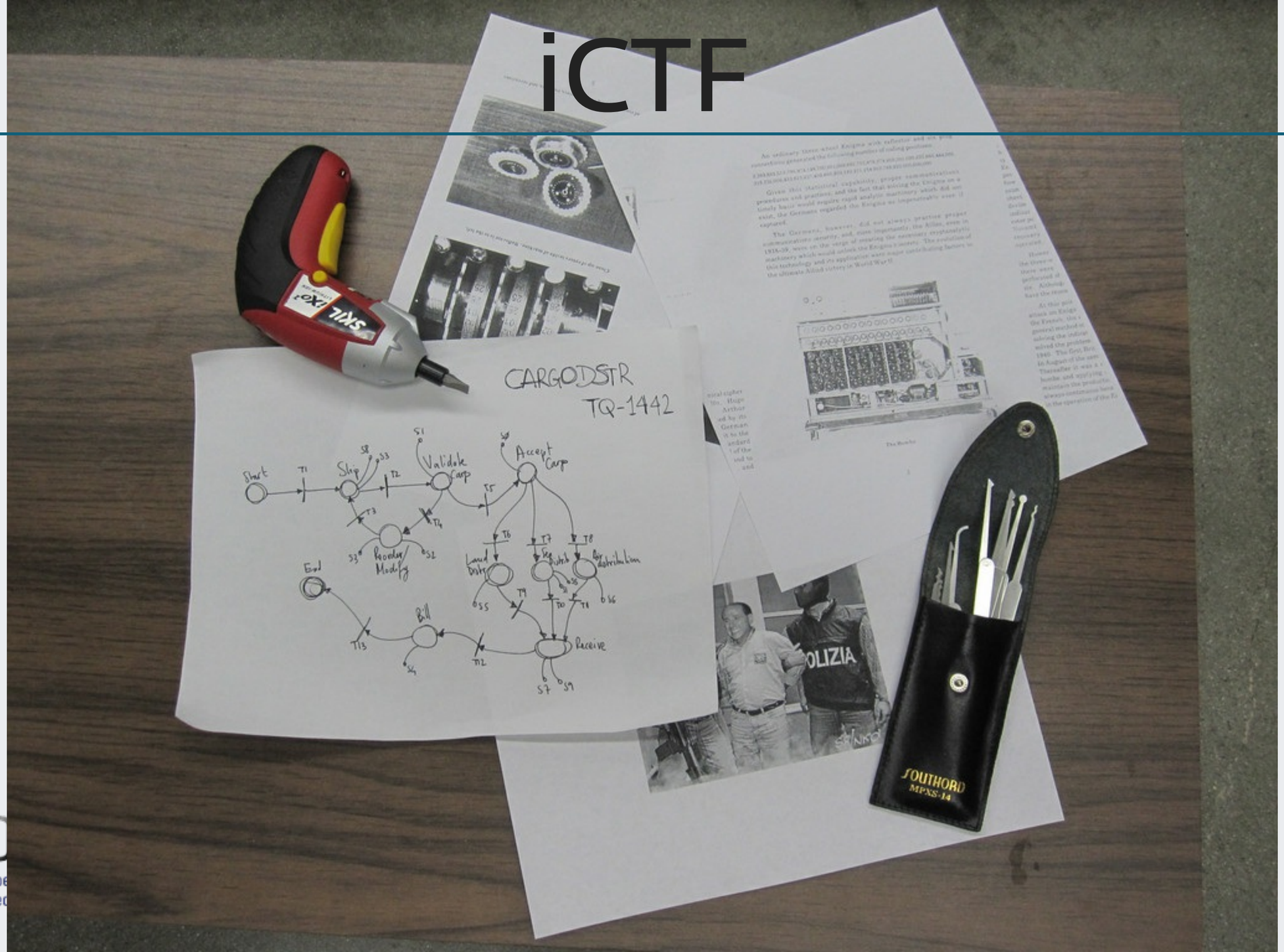
Hey les enfants vous êtes a un vrai CTF


Nous somme
team 19
range 10.1.1-32 x
NAT

Ensuite, un bel âge

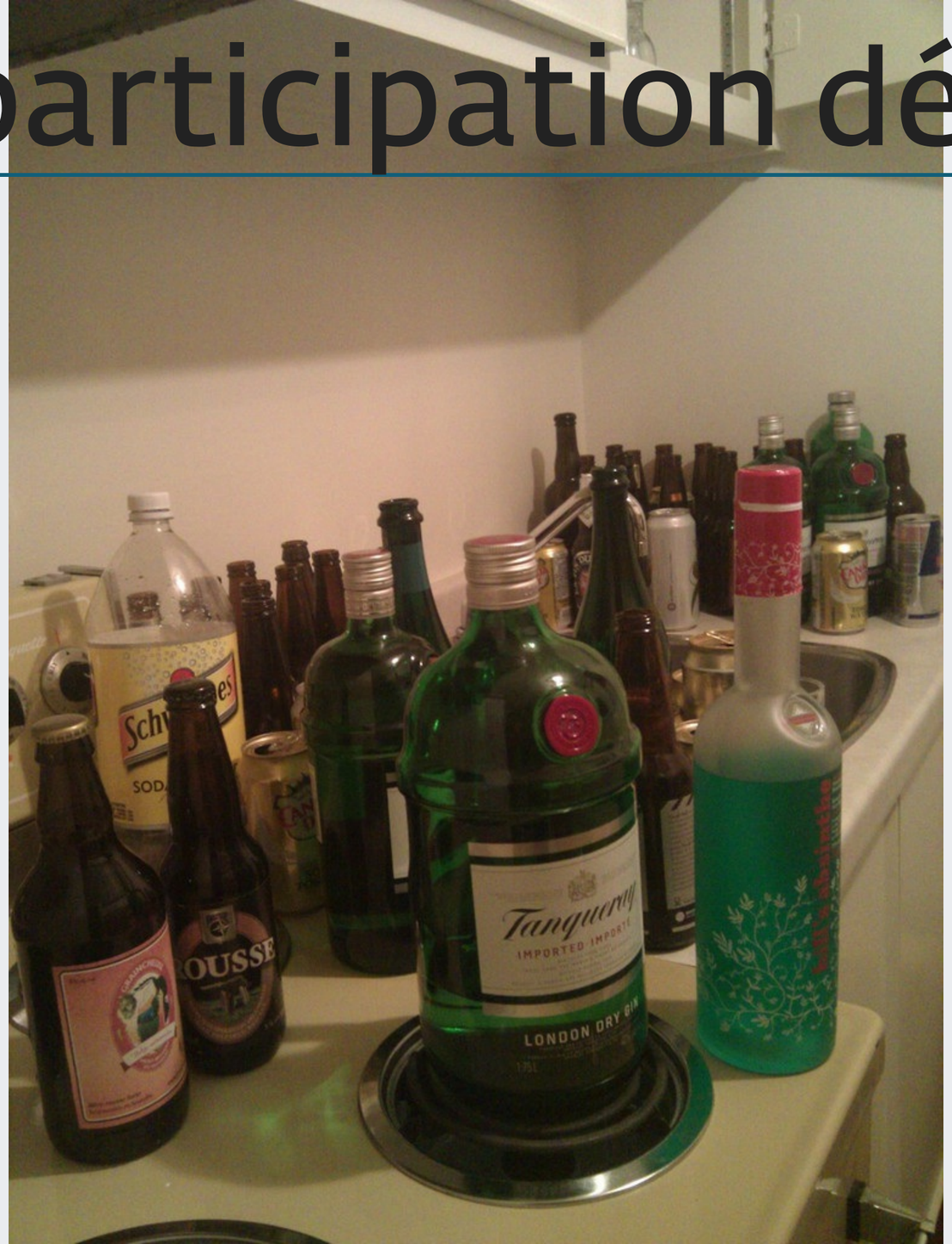
- HackUS, Hackfest
- Defcon Quals 18
- iCTF, CSAW
- … (iterate)
- hack.lu
- plaidctf
- mozilla ctf
- NorthSec

iCTF

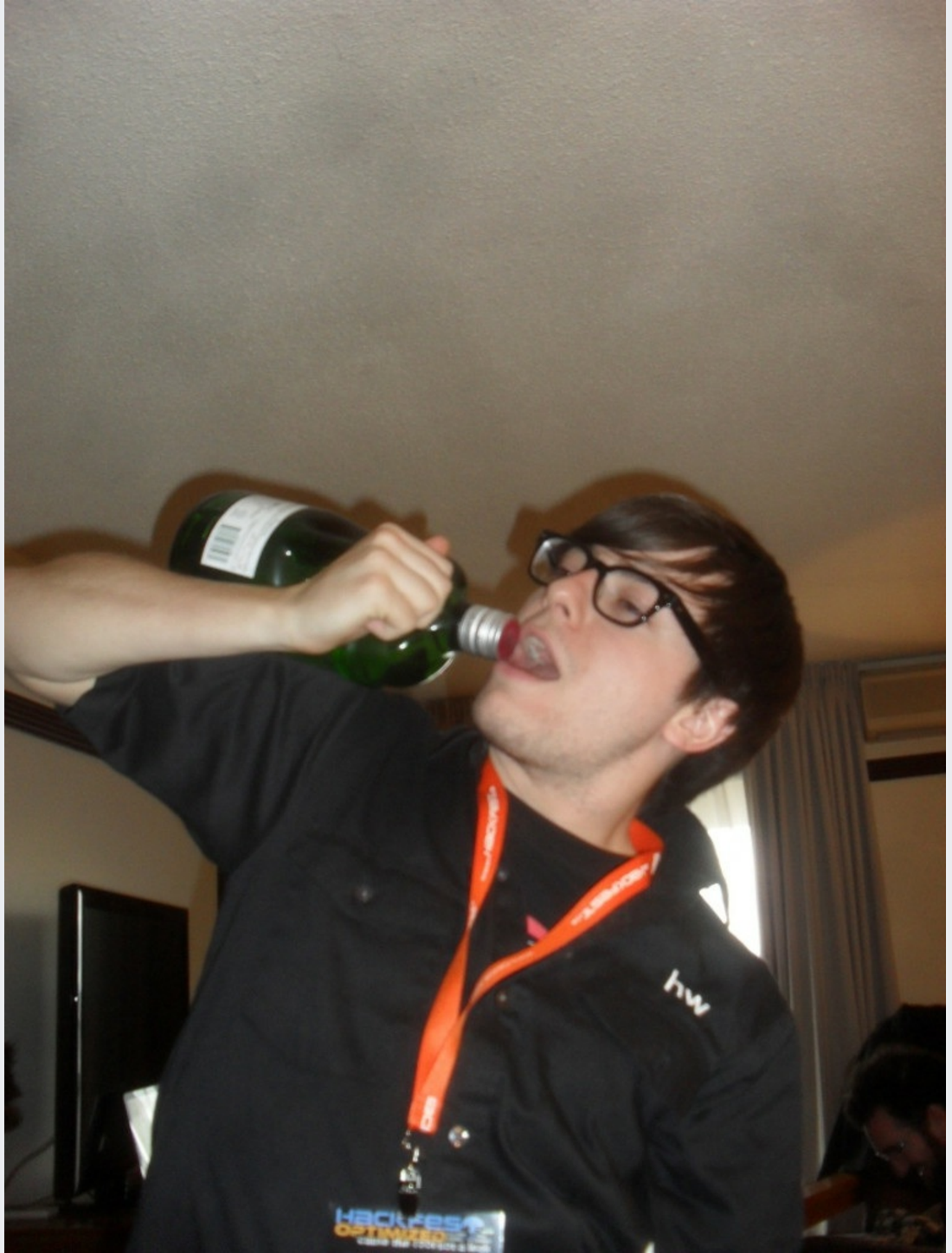

SKIL
CARGODSTR
TQ-1442
Start
Ship
Validate Cargo
Accept Cargo
Receive
Bill
End
SOUTHBEND
MPXS-14

Ope
Sec

Notre participation dégénéra



OWASP
Open Web Application
Security Project



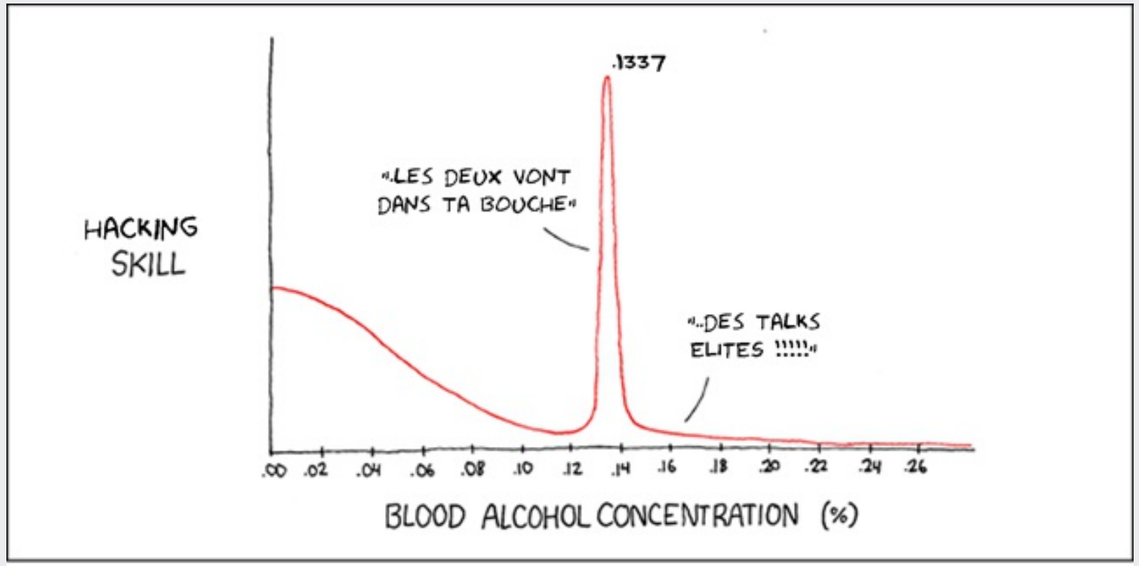
OWASP
Open Web Application
Security Project

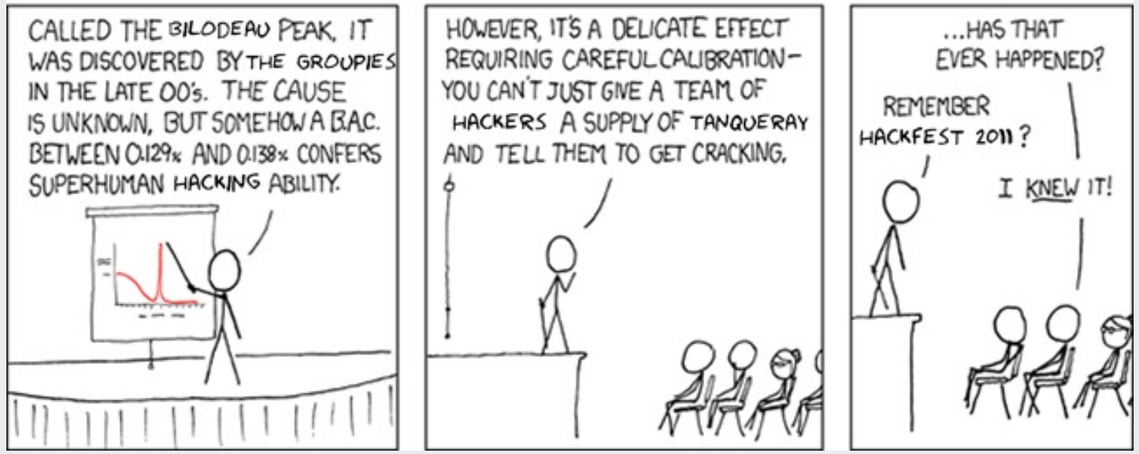

LG
No Signal


OWTEK

Tellement que...

le "Bilodeau" peak — hackfest 2011

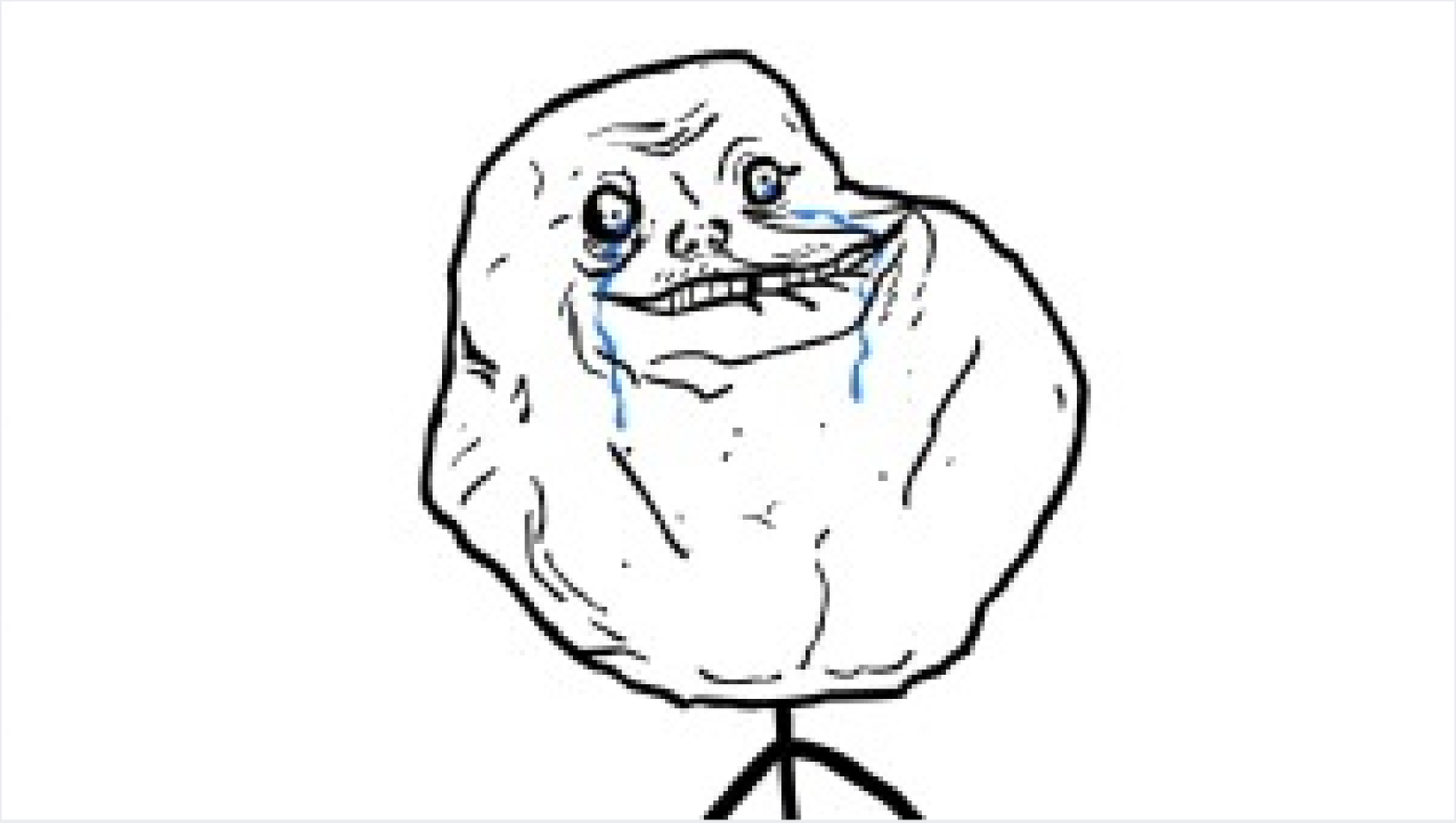




OWASP
Open Web Application Security Project

Pour perdre tout CTF…

Rester seul



skiddie tools only

- nmap
- metasploit
- Backtrack / Kali

Never read write-ups!

Never train.

Parce que le talent c’est inné

Never bookmark good tools

or never share them with your team

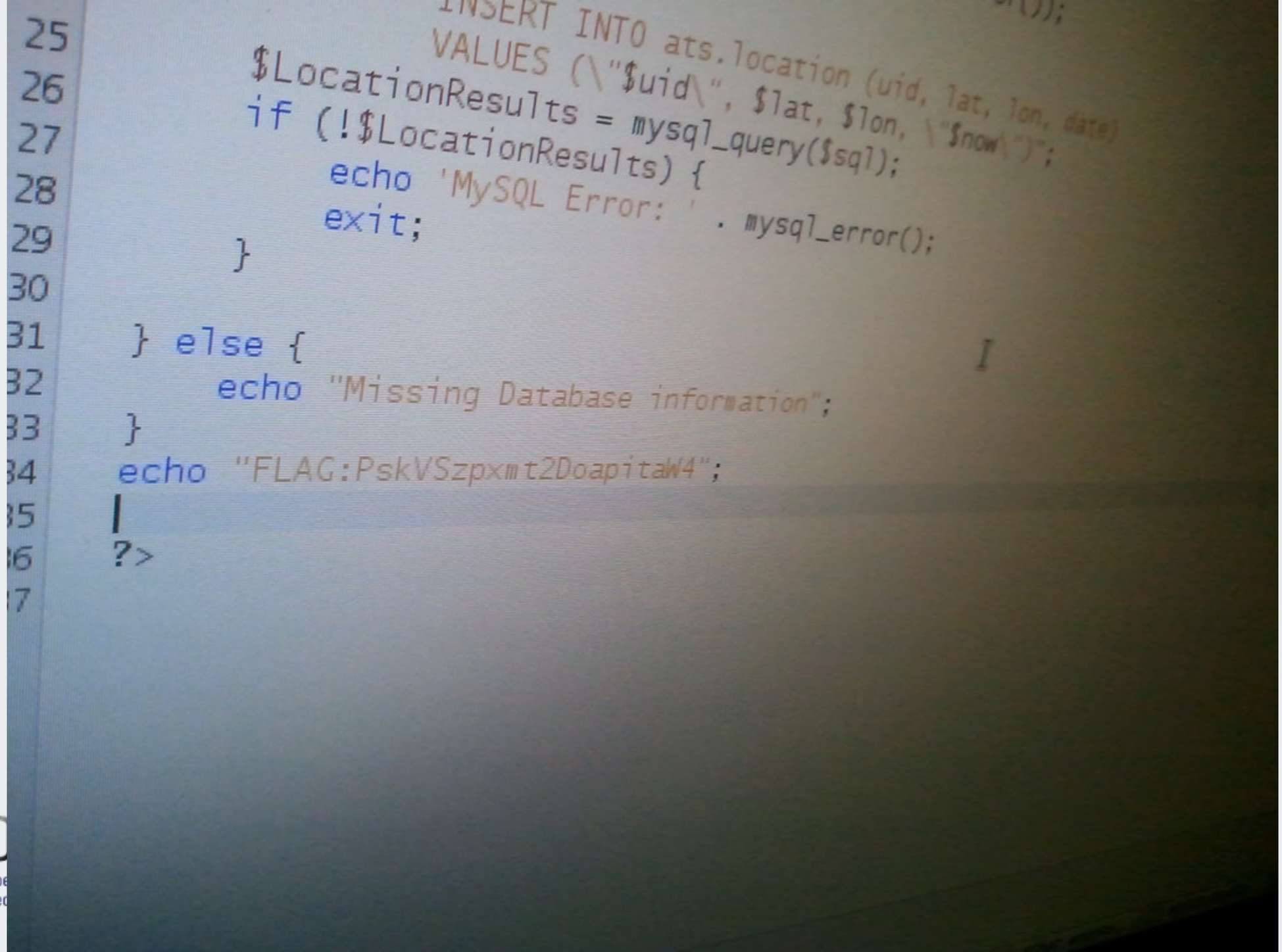
Communication

- Ne jamais parler aux autres équipes pour discuter des épreuves
- Ne jamais participer sur IRC, Slack (RingZero, Northern Coallition)

Ne jamais imiter ses héros


CSAW CTF
YOU WILL NEED ALL THE
CLONES YOU HAVE
DIYLOL.COM

Ne jamais sortir des sentiers battus


INSERT INTO ats.location (uid, lat, lon, date)
VALUES (\"$uid\", $lat, $lon, \"$now\")";
$LocationResults = mysql_query($sql);
if (!$LocationResults) {
echo 'MySQL Error: ' . mysql_error();
exit;
}
} else {
echo "Missing Database information";
}
echo "FLAG:PskVSzpxmt2DoapitaW4";
?>

Jamais ça non plus...

Never code or learn to code

Jamais se fier aux outils ou aux notes des autres

- http://pinboard.com/u:plaxx/t:security

Participer seulement si vous êtes certain de gagner!

On n’apprends pas en perdant.

Plus sérieusement

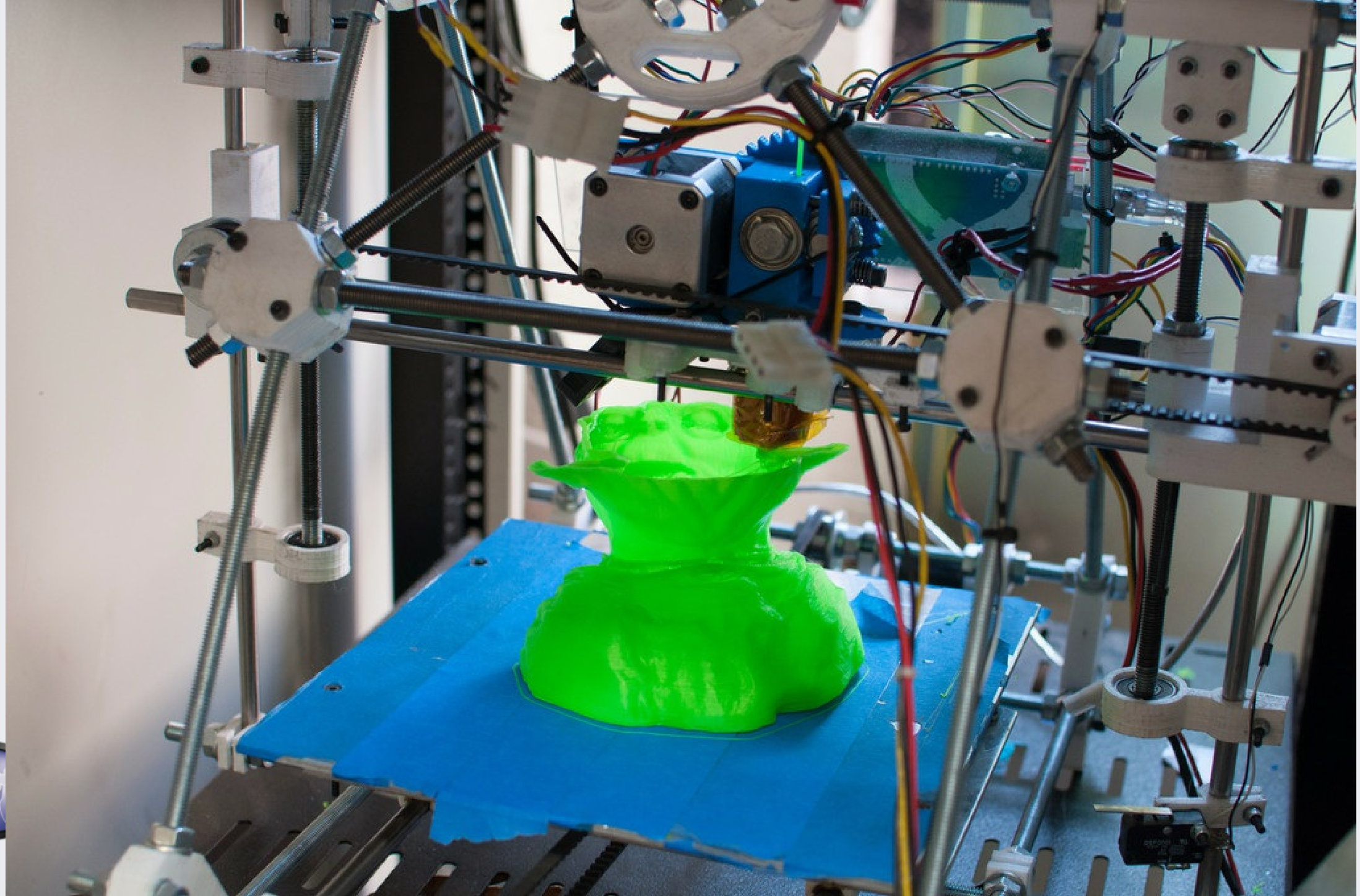
perdre c’est mieux!

Avoir une muse

OWASP
Open Web Application
Security Project

trouver vous un spot

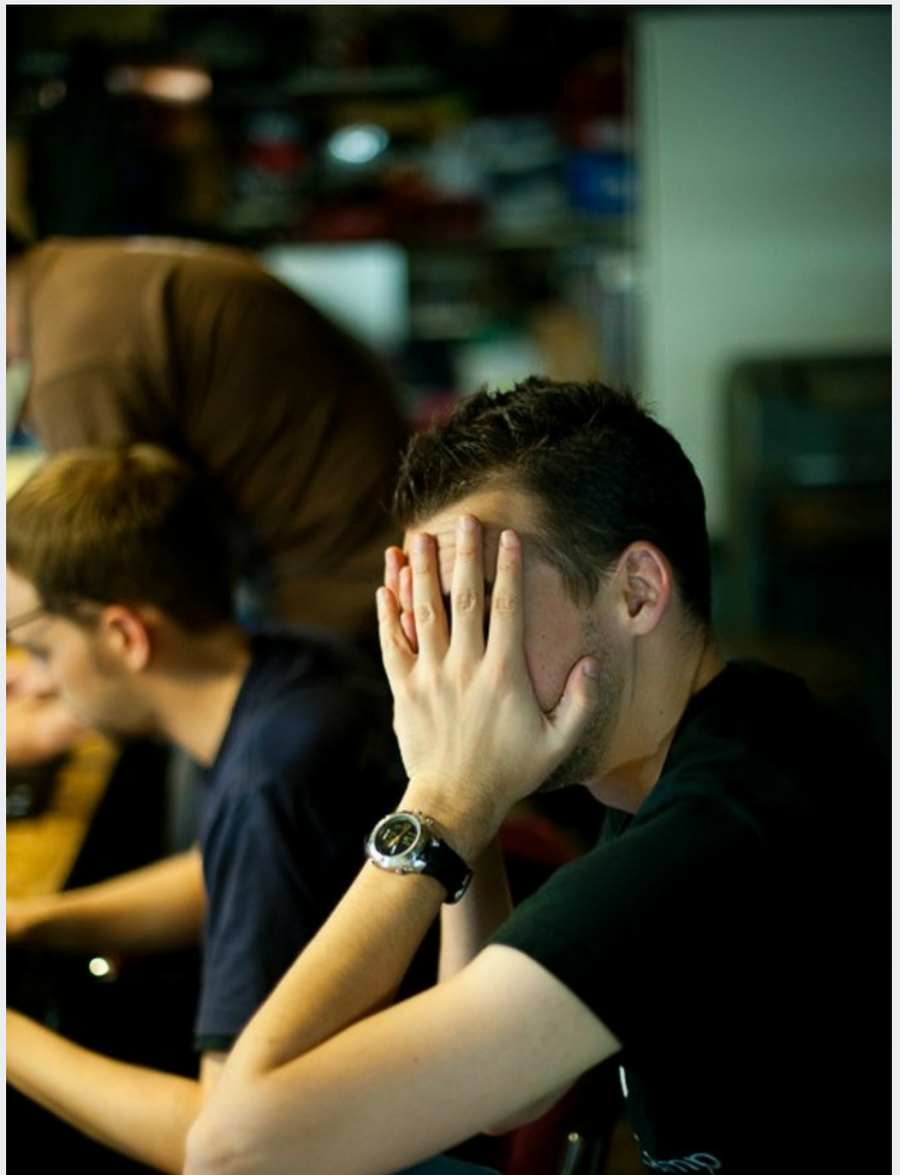
N’importe lequel!… Litéralement




DELL
HARP


Tanqueray
Leffe
eat fresh
mango

Ne pas se décourager



OWASP
Open Web Application
Security Project

Expliquer son 'challenge' a ses pairs

Causes désespérés

Avoir un département des causes désespérés.

Soyez proactifs pour batir une équipe

Batissez-vous un toolchain

- https://github.com/obilodeau/scratchpad
- https://pinboard.in/u:plaxx/t:security

my programming / infosec scratchpad

Add topics

55 commits | 1 branch | 0 releases | 1 contributor

Branch: master | New pull request | Create new file | Upload files

obilodeau added a lot of infosec/ stuff — Lat

C	some old C code lying around
R	Some R code from 2013
asciidoc	Vim and AsciiDoc old notes
asm	had some fun with assembly
bench	benchmarking ways to benchmark
infosec	added a lot of infosec/ stuff
java	patched-up Java Exception test code
media	ffmpeg command to speedup videos, useful for pitivi montage
moose	subclass attribute override vs builder override tests
perl	old code done when debugging problems with Tk fonts
php	another round of perl, bash and php
python	python: custom exceptions in python3
raspi	RaspPi: more idiomatic way of referring to button pressed
shell	A handful of shell reminders
.gitignore	did some Java.. MessageFormats and Exceptions
LICENSE	initial import
README.md	copyright year bump and minor text improvements
docker-cheatsheet.adoc	Some docker / vagrant devops stuff
docker.adoc	Some docker / vagrant devops stuff
hard-drive-recovery.adoc	Here's the latest installment of hard drive recovery weekly
vagrant.ad	Some docker / vagrant devops stuff
vim.adoc	Vim and AsciiDoc old notes

Branch: master ▾ scratchpad / infosec / Create new

obilodeau added a lot of infosec/ stuff

..	
crypto	added a lot of infosec/ stuff
csrf	CSRF sample payload and SQLi tips
exploitation	Exploitation: old notes and notes from montrehack's ROP
java	added a lot of infosec/ stuff
malware/tactics	server side malware tactics
post-exploitation	added a lot of infosec/ stuff
reversing	added a lot of infosec/ stuff
web	added a lot of infosec/ stuff
xss	added a lot of infosec/ stuff
android.adoc	added a lot of infosec/ stuff
bro.adoc	added a lot of infosec/ stuff
crypto.adoc	added a lot of infosec/ stuff
dump-process-memory.sh	added a lot of infosec/ stuff
elf.ad	added a lot of infosec/ stuff
embedded.adoc	added a lot of infosec/ stuff
firmware-analysis.adoc	added a lot of infosec/ stuff
forensic.ad	added a lot of infosec/ stuff
gdb-tricks.ad	added a lot of infosec/ stuff
gpg.ad	added a lot of infosec/ stuff
hardware.ad	added a lot of infosec/ stuff
ics-scada.adoc	added a lot of infosec/ stuff
ida.txt	added a lot of infosec/ stuff
ios.ad	added a lot of infosec/ stuff
irc.adoc	added a lot of infosec/ stuff
linux-dmsetup-luks-cryptsetup.ad	added a lot of infosec/ stuff
linux-exfil.adoc	added a lot of infosec/ stuff
linux-memory.ad	added a lot of infosec/ stuff
linux-priv-escalation.ad	added a lot of infosec/ stuff
linux-syscall.c	added a lot of infosec/ stuff
magic-bytes.adoc	added a lot of infosec/ stuff
malware.ad	added a lot of infosec/ stuff
password-cracking.adoc	added a lot of infosec/ stuff
pe-dump.py	added a lot of infosec/ stuff
pe.txt	added a lot of infosec/ stuff
pefile.ipynb	added a lot of infosec/ stuff
perl.adoc	added a lot of infosec/ stuff
php.ad	added a lot of infosec/ stuff

Pinboard (plaxx) 0.919 s history · network · notes · popular

Searched for **security** in your bookmarks. Found 1,000 results

« earlier later » edit

docker/docker-bench-security: The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in production.
docker security auditing containers
22 days ago by plaxx edit delete

Node Security Platform | Home
verifies security of nodejs dependencies
security verification npm build integration javascript nodejs dependency
24 days ago by plaxx edit delete

Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist
nist osx macos hardening guide reference security guidelines sysadmin
26 days ago by plaxx edit delete

graniet/chromebackdoor: Chromebackdoor is a pentest tool, this tool use a MITB technique for generate a windows executable ".exe" after launch run a malicious extension or script on most popular browsers, and send all DOM datas on command and control.
security man-in-the-browser attack tool post-exploitation pentest
27 days ago by plaxx edit delete

Hacking Slack using postMessage and WebSocket-reconnect to steal your precious token
abusing postMessage
browser bug vulnerability pentest security javascript post-message websocket slack
4 weeks ago by plaxx edit delete

Flipping Bits and Opening Doors: Reverse Engineering the Linear Wireless Security DX Protocol | Duo Security
hacking hardware radio how-to wifi
4 weeks ago by plaxx edit delete mark as read

Ben Hayak - Security Blog: Same Origin Method Execution (SOME)
Same Origin Method Execution (SOME)
pentest web some javascript technique
4 weeks ago by plaxx edit delete

SQL injections on stack overflow
php security database fun
5 weeks ago by plaxx edit delete

trailofbits/algo: 1-click IPSEC VPN in the Cloud
ipsec vpn linux ansible security
6 weeks ago by plaxx edit delete

Perdre aux compés difficiles

Pour être meilleurs aux compés plus faciles

- Développez des "réflexes"
- Voyez venir les tendances

Realité

Ce sont des exercices. Ce n’est pas réel. Il faut penser au-delà de ce qu’on voit [en entreprise] ou lit.

Admins

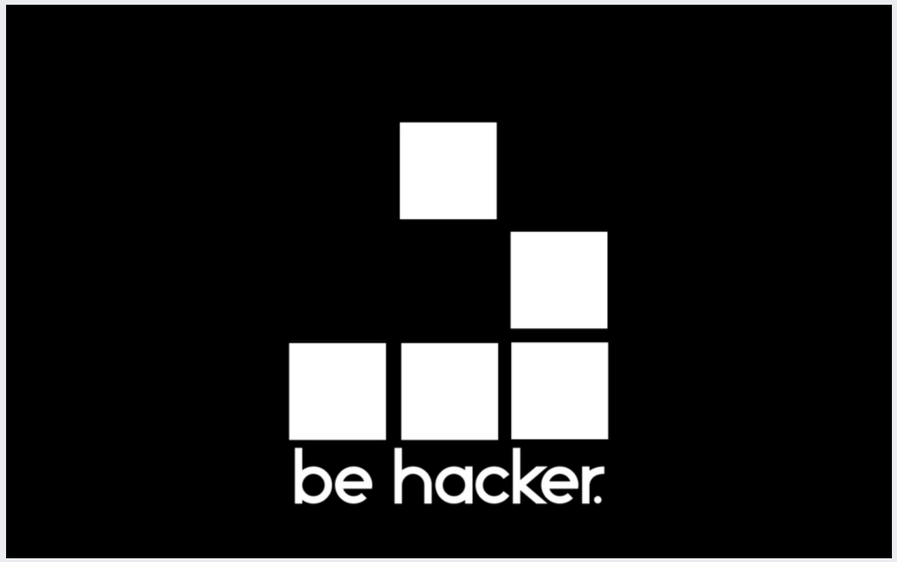
Les 'admins' veulent que vous réussissiez.

Aller plus loin

et former la relève de nos équipes

Montréhack

- 3e lundi du mois
- http://montrehack.ca

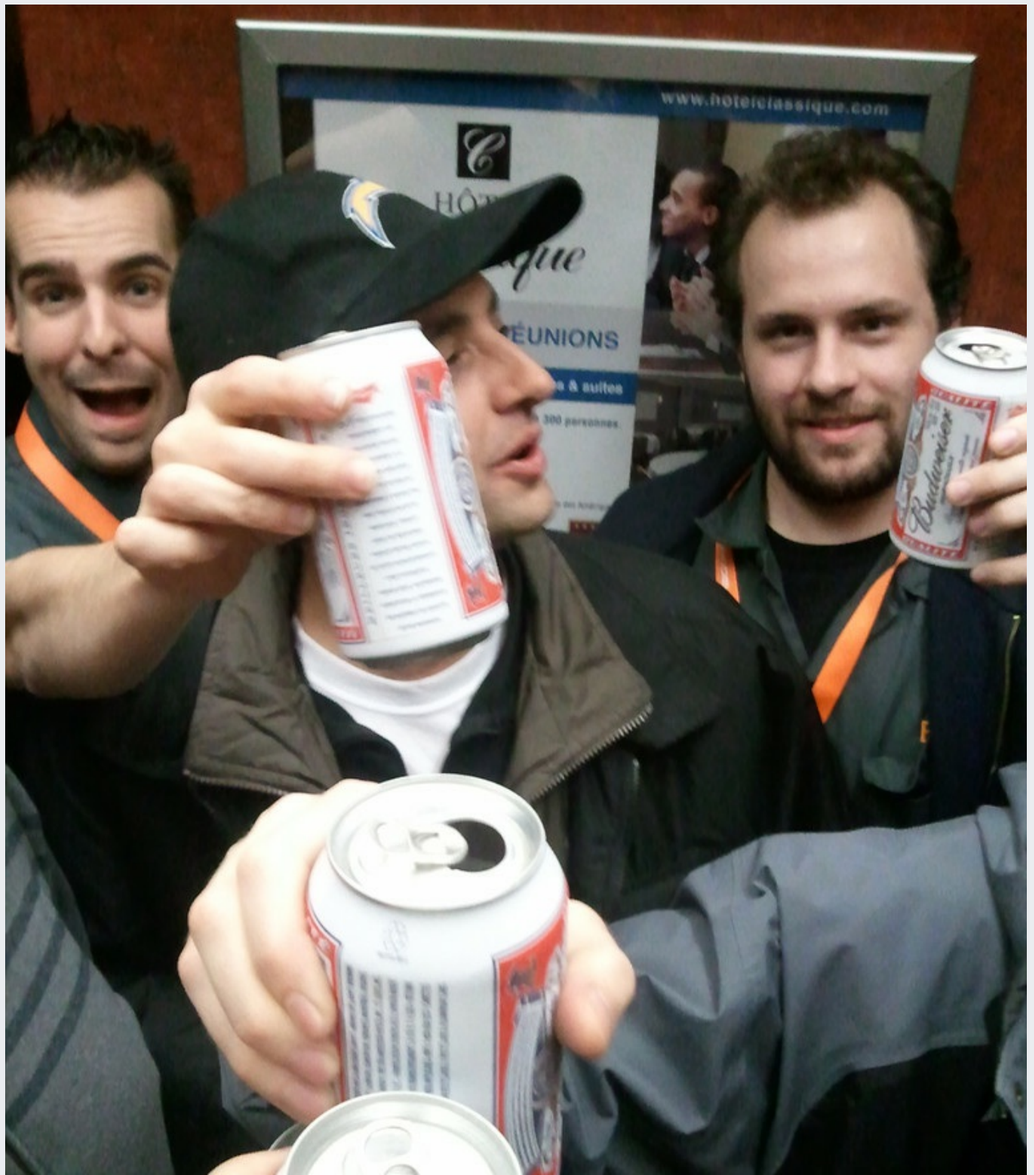


HackFest Hackerspace

- 4e jeudi du mois au Cégep de Sainte-Foy
- http://www.hackfest.ca/hackfest-community/hackerspace

OWAS
Open Web Applica
Security Project

Enfin… s'amuser!!!



OWASP
Open Web Application
Security Project

CTF Generations


STAR TREK

First Generation

- Challenges were easier
- Some competitions really poor
- We were obnoxious, always drinking, yet still won
- We had it easy

Before smoking's dangers were well-known, it was common to find greats like Stan Mikita puffing away before and even during games.

Lee Balterman/Sports Illustrated

It's amazing that Guy Lafleur could smoke a pack of cigarettes a day and still excel in an aerobically demanding sport like hockey.

Bruce Bennett/Getty Images


STAR TREK 365
THE NEXT GENERATION®
BY PAULA M. BLOCK AND TERRY J. ERDMANN
INTRODUCTION BY RONALD D. MOORE

The Next Generation

- Better educated
- More resources online
- Generally a lot stronger
- Challenges are **way** harder

Conclusion

Y’en a pas de tool secret…

Failure is simply the opportunity to begin again, this time more intelligently. There is no disgrace in honest failure; there is disgrace in fearing to fail.

— Henry Ford


LNX EU

Questions?

Merci!

- @obilodeau
- NorthSec
- My online bookmarks
- My programming and infosec scratchpad
- MontréHack monthly workshops
- RingZero Team Online CTF
- The Northern Coalition Slack

OWASP
Open Web Application
Security Project