HACKFEST 2016

INFINITY EDITION

PLAN DE LA PRÉSENTATION

- Qu'est-ce que le Hackfest?
- Résumé de la 8ème édition
- Conclusion

HACKFEST?

QU'EST-CE QUE LE HACKFEST?

- Le plus gros événement sur le piratage et la sécurité informatique au Canada
  - **Quand?** En novembre
  - **Où?** À Québec
  - **Combien?** 90$ en pré-vente, 120$ à la porte
  - **Quoi?** Conférences, Ateliers, *CTF*, Crochetage, Ingénierie sociale
    - Bilingue, *mais surtout anglophone*

CTF?

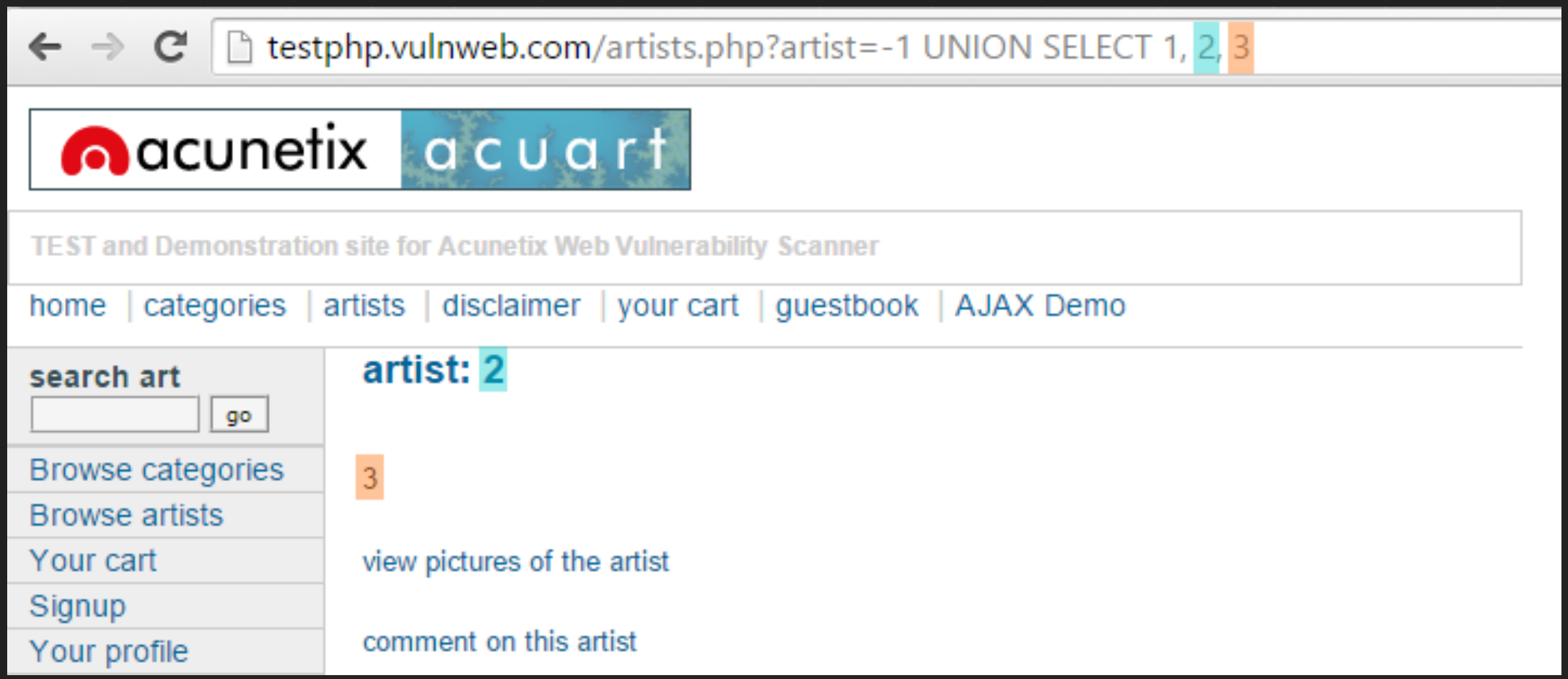
- *Capture the Flag*
- Jeu d'habileté qui simule un environnement présentant des vulnérabilités pouvant être exploités par les participants
- Il existe différents types d'épreuves demandant des aptitudes différentes
  - Rétro-ingénierie
  - Analyse du traffic réseau
  - Programmation
  - Encryption
  - Attaque/Défense
  - Électronique
- Un fois un défi résolu, un *flag* est remis et peut être validé pour obtenir des points

CTF-EXEMPLE D'INJECTION SQL

- Trouver une requête acceptant les entrées de l'utilisateur

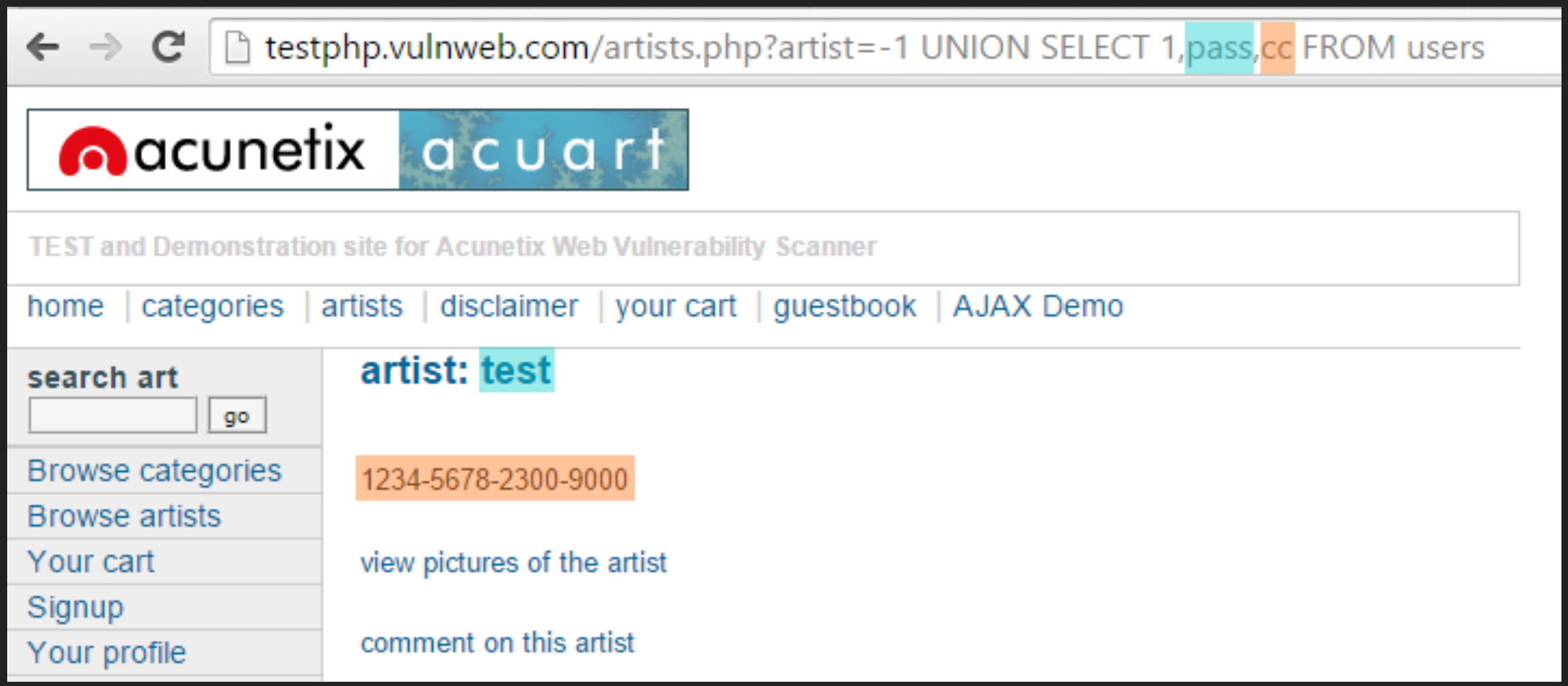
CTF-EXEMPLE D'INJECTION SQL

- Essayer de modifier les paramètres de la requête



CTF-EXEMPLE D'INJECTION SQL

- Abuser la requête pour récupérer des données



RÉSUMÉ DE LA 8IÈME EDITION


SECRET?


LANDRY
+ associés | associates
NE RIEN
LAISSER
AU HASARD®
BROWNING
landryconsulting.com


0100 0101 0000 0000 0000 0000 0010 1000
0000 0100 0010 1101 0100 0000 0000 0000
1000 0100 0000 0110 1111 1110 1001 0100
0000 1010 0110 0100 0001 0101 1000 1000
1010 1100 0001 1100 0000 0101 1001 0111

JOUR 1

VULNÉRABILITÉ D'HTTP/2 AUX ATTAQUES DDOS

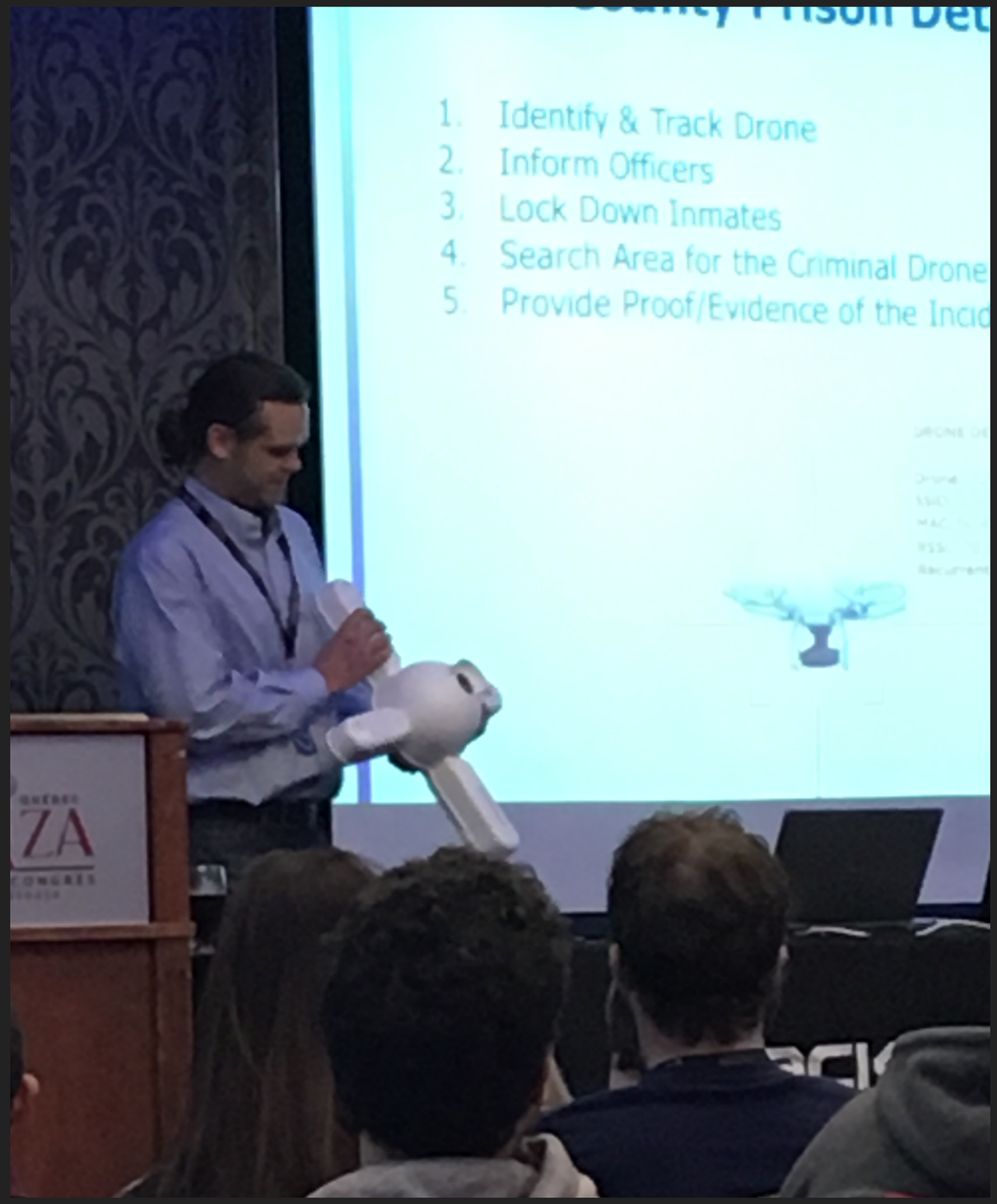
LE BITCOIN, PAS AUSSI ANONYME QU'ON LE CROIT

BONNES PRATIQUES POUR LA CONFIGURATION DES SERVEURS

LA PSYCHOLOGIE DU HACKER PERSONA

BURP SMART BUSTER

COMMENT LES PRISONS SE PROTÈGENT DES DRONES?



ATELIER

PETER YAWORSKI

ATELIER – PETER YAWORSKI

- @yaworsk
- Surpasser le statut de débutant en *bug bounty*(chasseur de bogues)
- Web Hacking 101
- Plateformes de *bug bounty*
  - hackerone
  - bugcrowd

ATELIER – PETER YAWORSKI

- Ce n'est pas de l'argent *facile*
- Persévérez!
- Il faut fournir une preuve de concept avec un rapport de bogue
- Votre réputation est vitale sur les plateformes de *bug bounty*
- De bons contacts et la capacité d'observation sont aussi importants que les connaissances brutes
- Sortez des sentiers battus
- Bons rapports => Meilleurs relations => Augmente la rémunération

ATELIER – PETER YAWORSKI

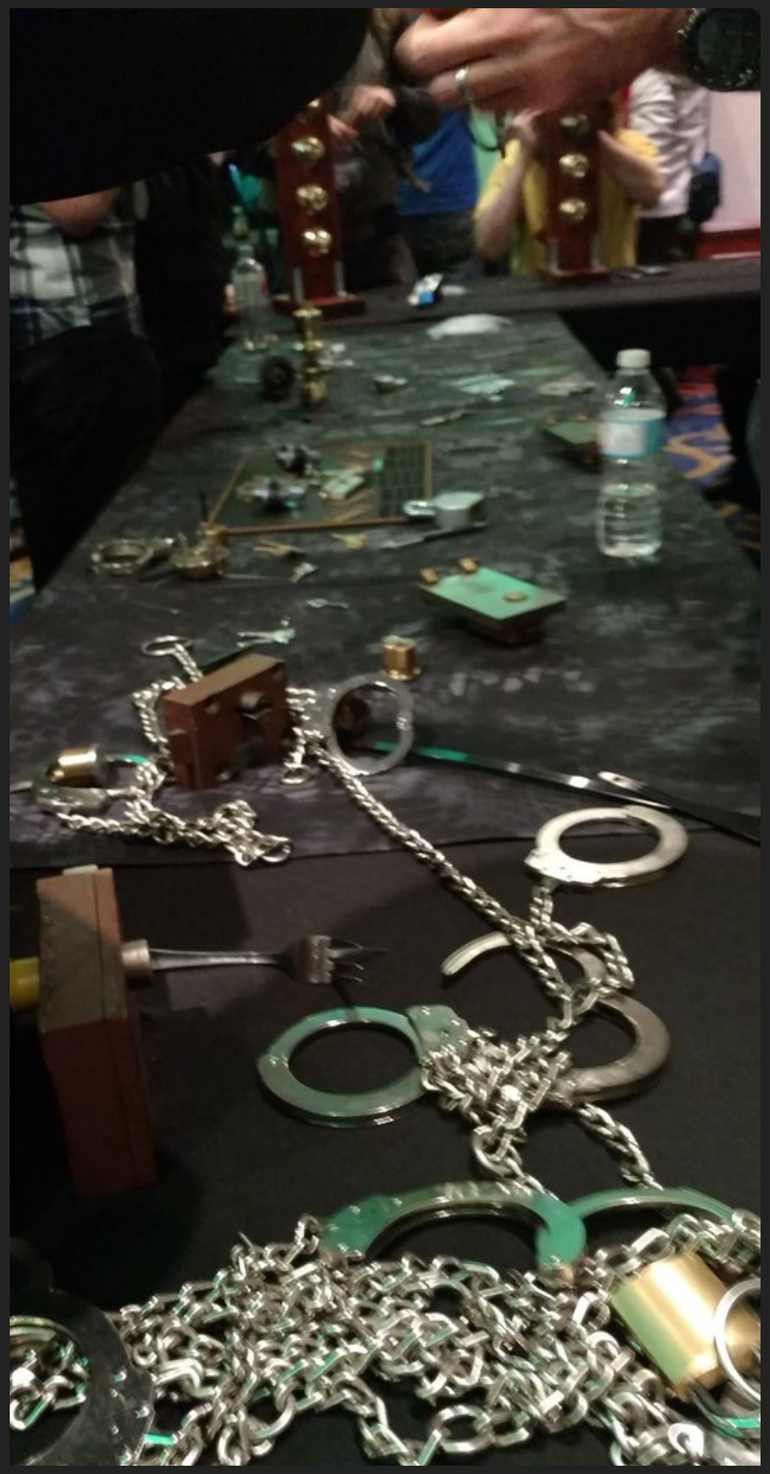
- Quelques outils pour démarrer
  - burp
  - fiddler proxy
  - nmap
  - gitrob
  - sublist3r
  - reconengineer
  - wappalyser
  - xsshunter
  - dex2jar

CTF

HACKFEST

CTF

CTF



CTF

JOUR 2

PROBLÈMES DE CONCURRENCE DANS LES APPLICATIONS WEB

VULNÉRABILITÉS DE LA SÉRIALISATION JAVA

MANIPULATION DES ORGANISATIONS DE CROISIÈRES

L'ÉCONOMIE DU DARK WEB

ABUSER LES JEUX VIDÉO POUR LE PLAISIR

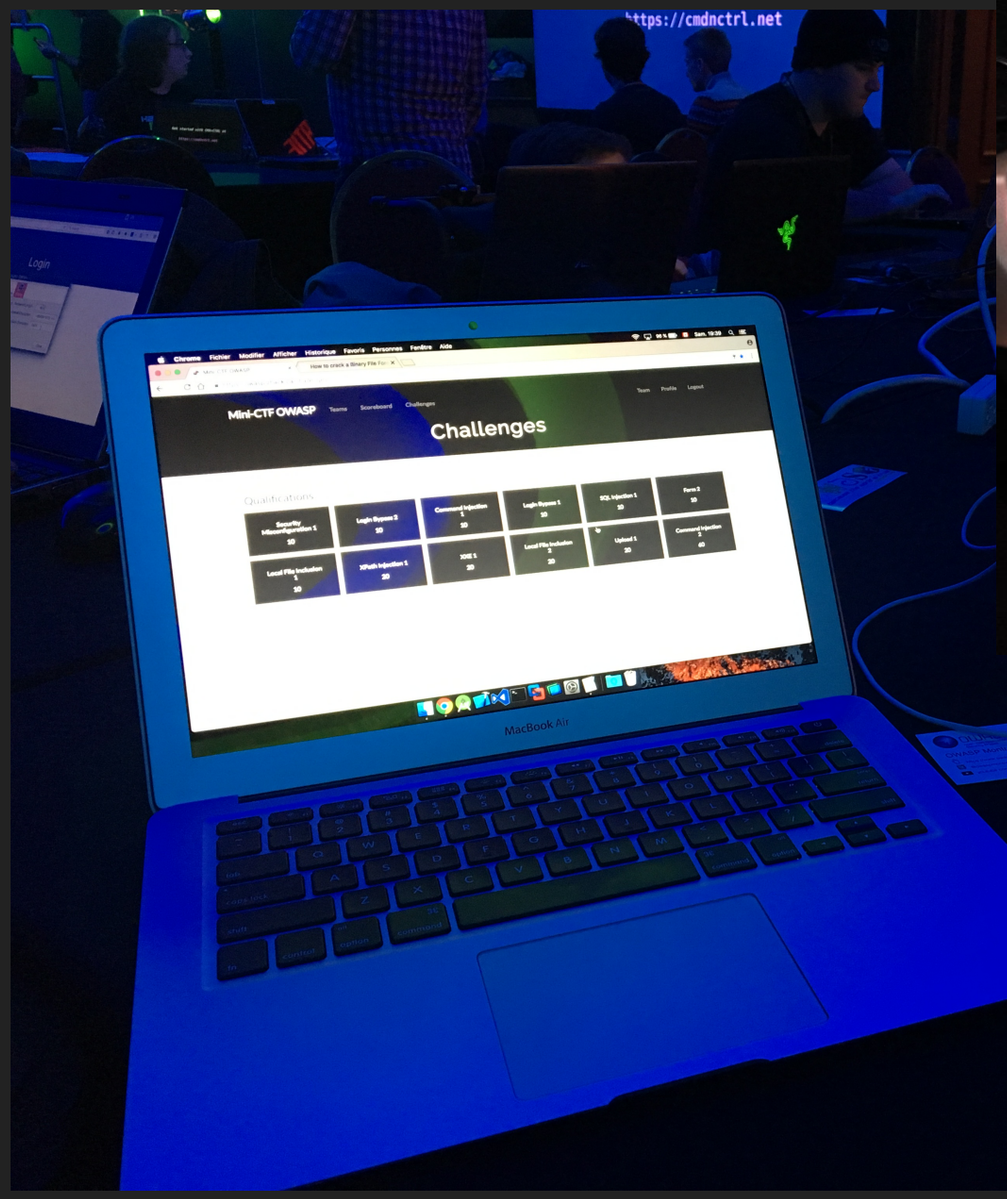
PRÉPARER L'ÉQUIPE DE DÉFENSE COMME LES PILOTES DE CHASSE

SÉCURISER LES APPS IOS

PODCAST – LA FRENCH CONNECTION

- http://securite.fm/

SOIRÉE ESET ET MINI-CTF OWASP



CONCLUSION

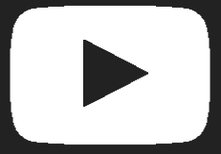
CONCLUSION

- Le Hackfest est un événement unique au Canada
- La communauté *infosec* est très ouverte et accueillante
- Sans être un expert en sécurité, il est important d'être sensibilisé à ces enjeux
- C'est un événement très accessible pour en apprendre plus sur tout ce qui touche la sécurité informatique!

HACKFEST SUR LE WEB

http://www.hackfest.ca/

@hackfest_ca



hackfestca

QUESTIONS?