Hunch LEARN





HACKFEST 2016

INFINITY EDITION

QUI SUIS-JE?

- James Hoffman
- Développeur
 - Mobile

Le meilleur moment pour planter un arbre était il y a 20 ans. Le Deuxième meilleur moment est maintenant.

PLAN DE LA PRÉSENTATION

- Qu'est-ce que le Hackfest?
- Résumé de la 8^{ème} 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

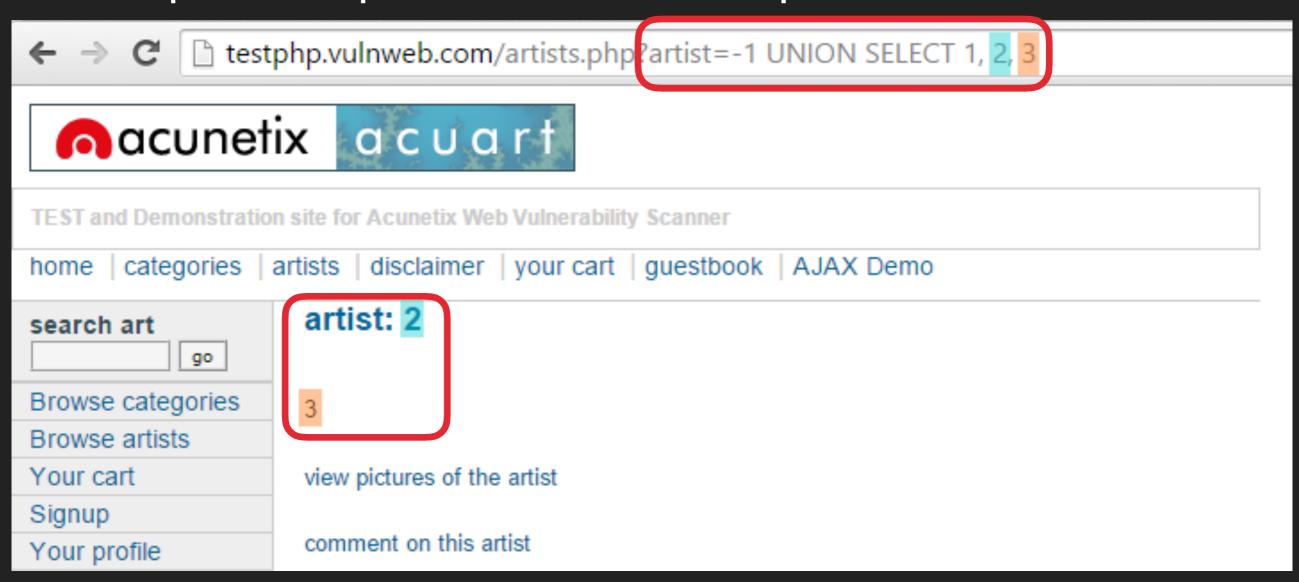
CTF-EXEMPLE D'INJECTION SQL

Trouver une requête acceptant les entrées de l'utilisateur



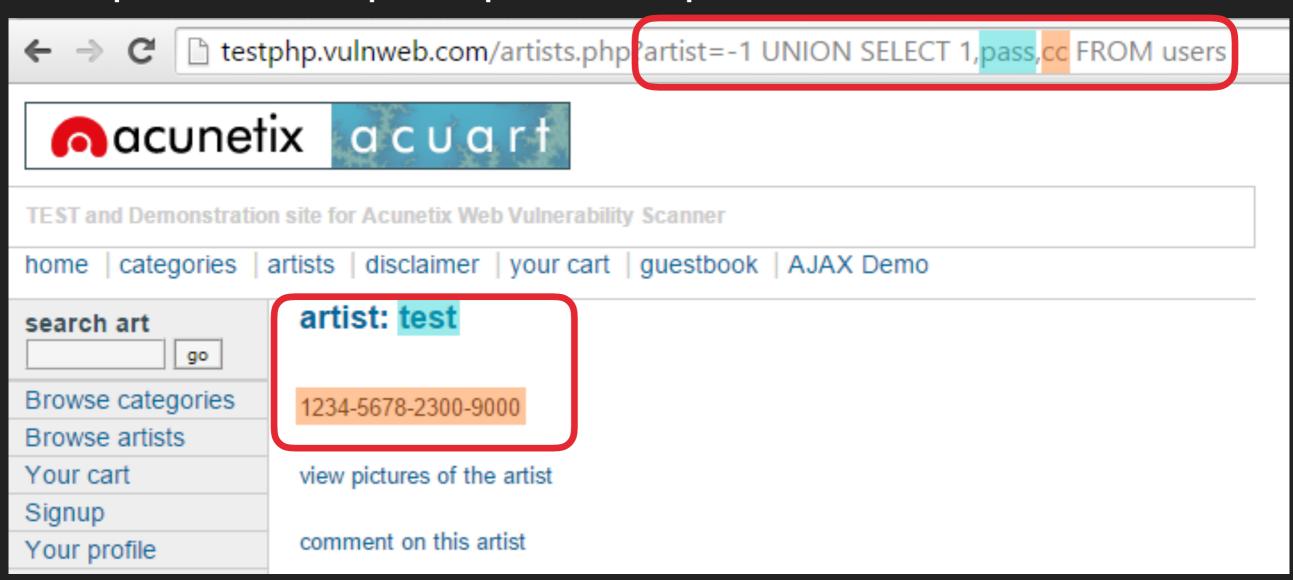
CTF-EXEMPLE D'INJECTION SQL

Manipuler les paramètres de la requête



CTF-EXEMPLE D'INJECTION SQL

Exploiter la requête pour récupérer des données

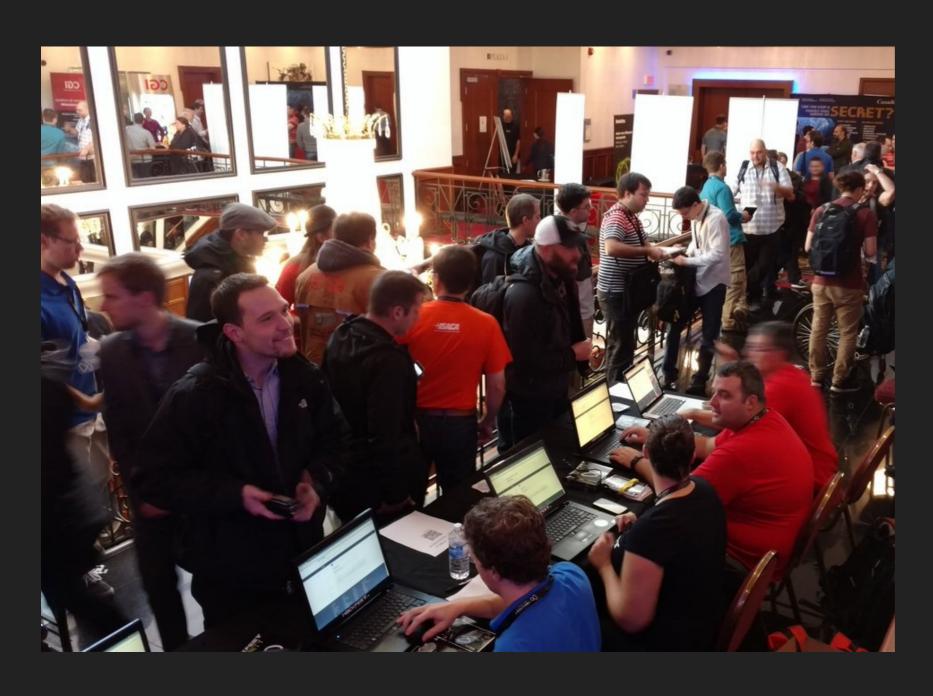


RÉSUMÉ DE LA 8IÈME EDITION



JOUR 1

ACCUEIL





CONFÉRENCES VARIÉES, POUR TOUT LES NIVEAUX

- Vulnérabilité d'HTTP/2 aux attaques DDoS
- Le bitcoin, pas aussi anonyme qu'on le croit
- Bonnes pratiques pour la configuration des serveurs
- Burp Smart Buster
- La psychologie du hacker persona
- Gérer la concurrence dans les applications web
- Vulnérabilités de la sérialisation Java
- Hacker les jeux vidéo pour le plaisir
- Préparer l'équipe de défense comme les pilotes de chasse
- Sécuriser les apps iOS

COMMENT LES PRISONS SE PROTÈGENT DES DRONES?







ATELIER

PETER YAWORSKI

ATELIER - PETER YAWORSKI

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

ATELIER - PETER YAWORSKI

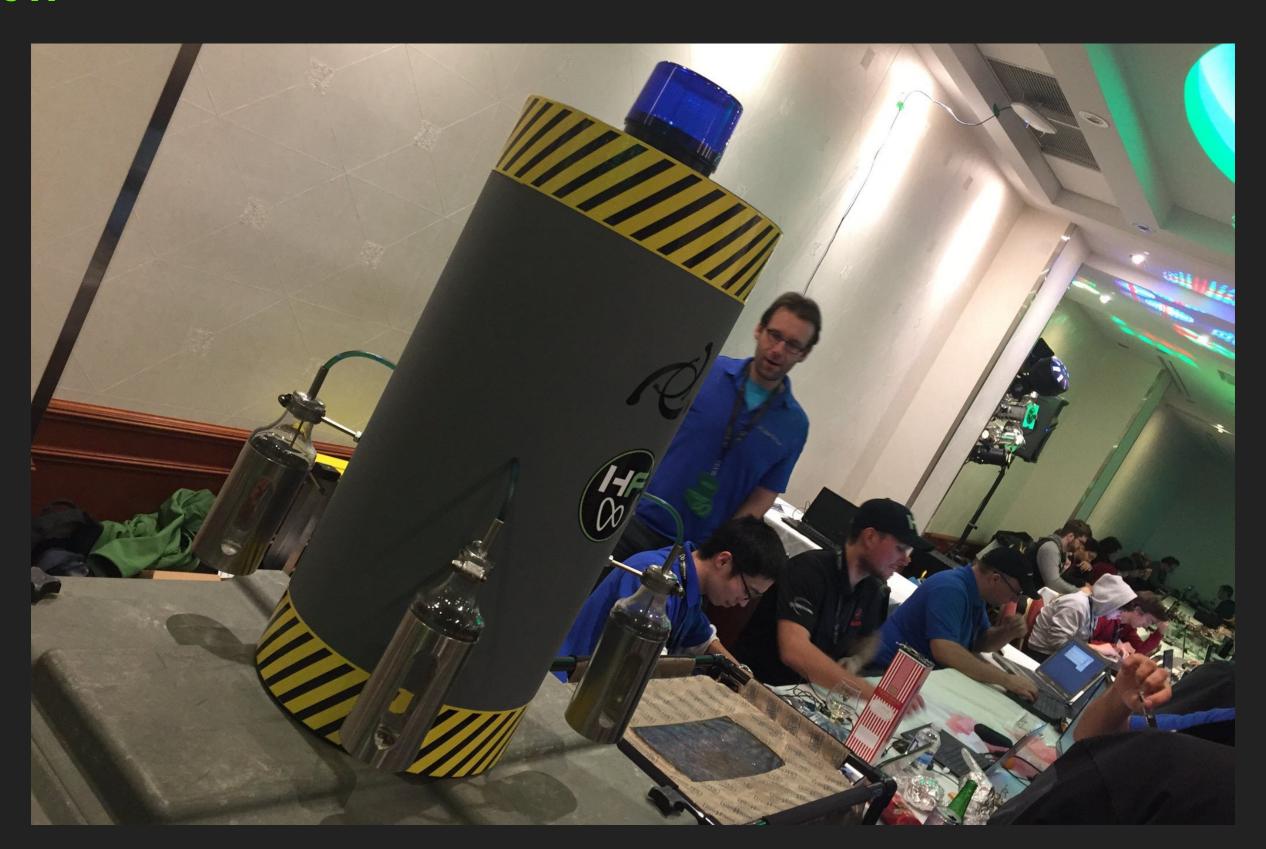
- Ce n'est pas de l'argent facile
- Persévérez!
- Il faut fournir une preuve de concept avec un rapport de bogue
- Votre réputation est vitale sur les plateformes de bug bounty
- De bons contacts et la capacité d'observation sont aussi importants que les connaissances brutes
- Sortez des sentiers battus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

ATELIER - PETER YAWORSKI

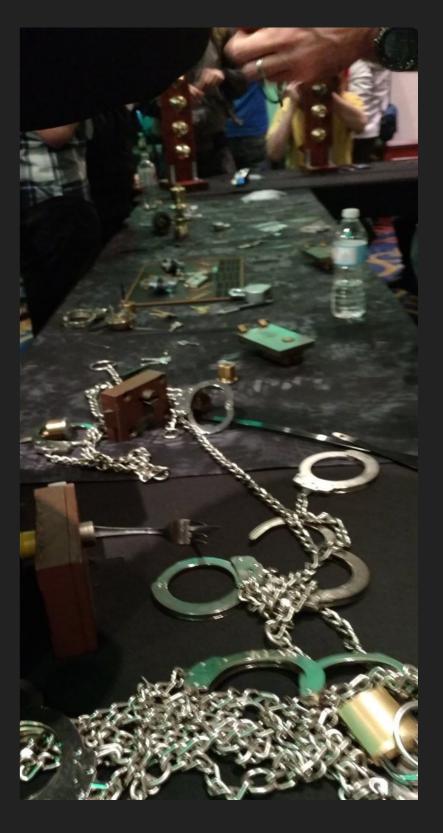
- Quelques outils pour démarrer
 - burp
 - fiddler proxy
 - nmap
 - gitrob
 - sublist3r
 - reconengineer
 - wappalyser
 - xsshunter
 - dex2jar

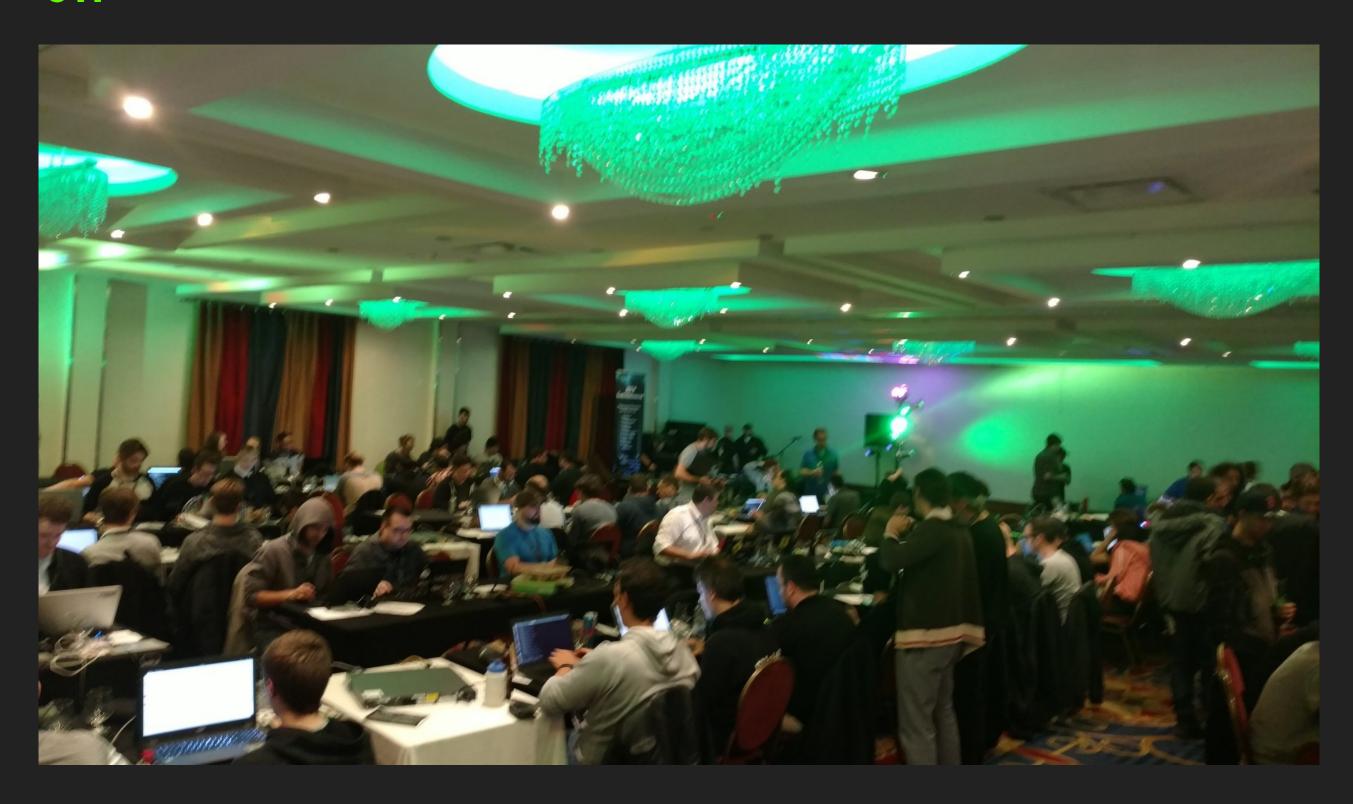


HACKFEST











JOUR 2

MANIPULATION DES ORGANISATIONS DE CROISIÈRES



L'ÉCONOMIE DU DARK WEB

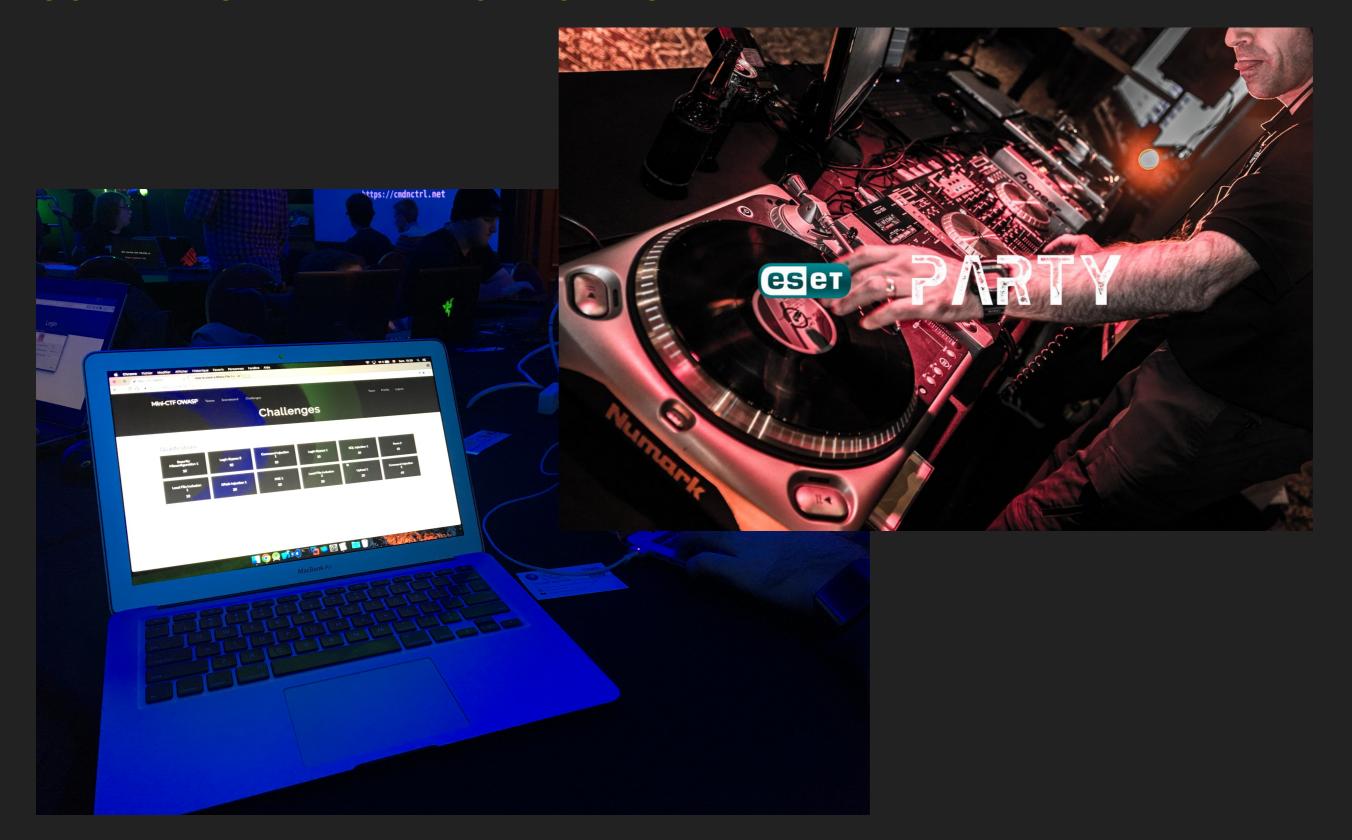


PODCAST - LA FRENCH CONNECTION

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?