



**HACKFEST**  
**INFINITY**

**TRAININGS** 1-2-3RD  
**CONFERENCES** 4-5TH  
**NOVEMBER** 2016

**HACKFEST 2016**

---

**INFINITY EDITION**

---

# PLAN DE LA PRÉSENTATION

- ▶ Qu'est-ce que le Hackfest?
- ▶ Résumé de la 8<sup>ème</sup> 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 trafic 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

← → ↻ testphp.vulnweb.com/artists.php?artist=1

 acunetix  acu art

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

**artist: r4w8173**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent

# CTF-EXEMPLE D'INJECTION SQL

- ▶ Essayer de modifier les paramètres de la requête

The screenshot shows a web browser window with the address bar containing the URL: `testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, 2, 3`. The page header features the Acunetix logo and the text "acuart". Below the header, there is a navigation menu with links for "home", "categories", "artists", "disclaimer", "your cart", "guestbook", and "AJAX Demo". The main content area displays "artist: 2" in a large font, with a small orange box containing the number "3" to its left. Below this, there are two links: "view pictures of the artist" and "comment on this artist". On the left side of the page, there is a search bar labeled "search art" with a "go" button, and a list of navigation links: "Browse categories", "Browse artists", "Your cart", "Signup", and "Your profile".

# CTF-EXEMPLE D'INJECTION SQL

- ▶ Abuser la requête pour récupérer des données

testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users

acunetix acu art

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

Browse categories  
Browse artists  
Your cart  
Signup  
Your profile

artist: test

1234-5678-2300-9000

[view pictures of the artist](#)

[comment on this artist](#)

# RÉSUMÉ DE LA 8<sup>ÈME</sup> EDITION









---

# JOUR 1



# VULNÉRABILITÉ D'HTTP/2 AUX ATTAQUES DDOS





# LE BITCOIN, PAS AUSSI ANONYME QU'ON LE CROIT



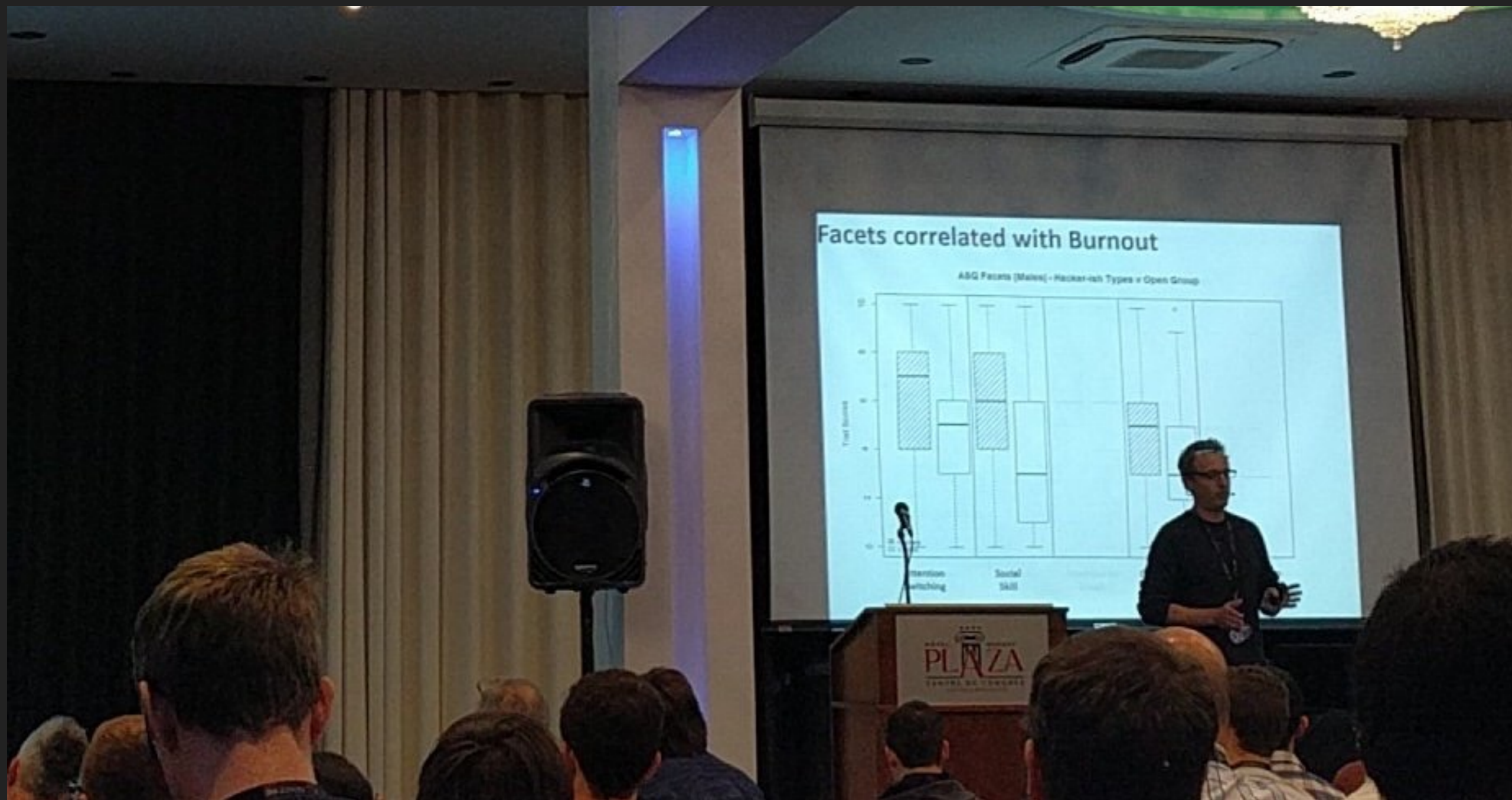


# BONNES PRATIQUES POUR LA CONFIGURATION DES SERVEURS





# LA PSYCHOLOGIE DU HACKER PERSONA





# BURP SMART BUSTER





# COMMENT LES PRISONS SE PROTÈGENT DES DRONES?





# WEB HACKING

101 How to Make Money  
Hacking Ethically

Analysis of 30+ vulnerability reports that paid!



Peter Yaworski

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 => Meilleures relations => Augmente la rémunération



---

# ATELIER – PETER YAWORSKI

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



CTF

---

**HACKFEST**

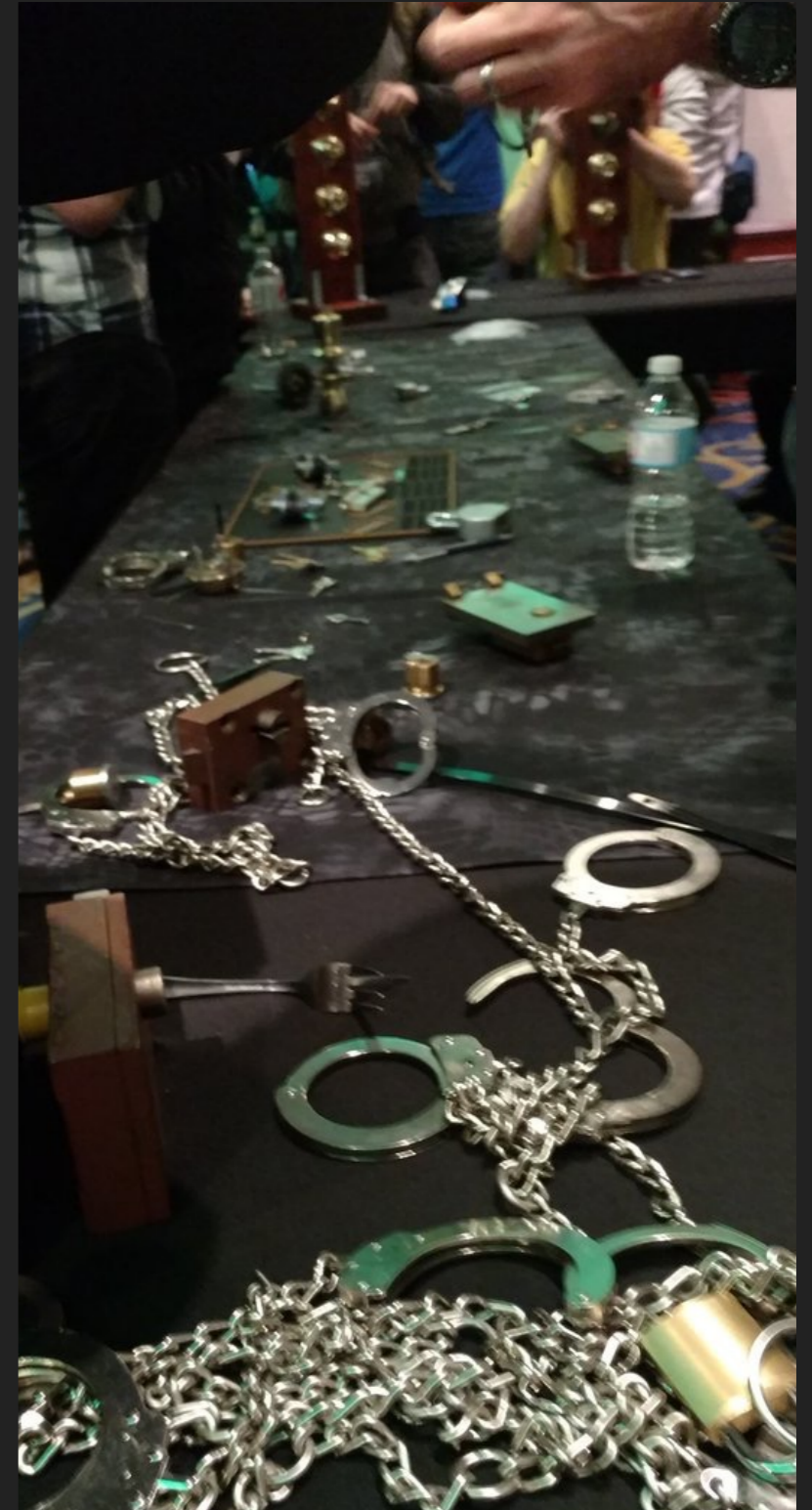


# CTF





# 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

Interesting fact about making an "Online Game".

```
graph TD; A[Receive Unfiltered Data] --> B((Receive Client N Data)); B --> C((Flush Client N New Data)); C --> D((Update Game)); D --> E((Update Database)); E --> B; F[Game Server Logic] --- B; F --- C; F --- D; F --- E;
```

The diagram illustrates the data flow in an online game server. It starts with 'Receive Unfiltered Data' (a blue box) pointing to 'Receive Client N Data' (a red circle). This leads to 'Flush Client N New Data' (a red circle), which then points to 'Update Game' (a red circle). From 'Update Game', the flow goes to 'Update Database' (a red circle), which then loops back to 'Receive Client N Data'. In the center of the cycle is 'Game Server Logic'. To the right of the diagram is a cartoon illustration of a character sitting on a stack of books, reading a book titled 'Reverse Engineering' under a lamp.

Loading : Level

**HACKFEST**



# 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!



---

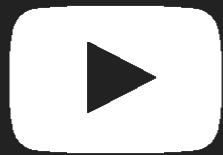
# HACKFEST SUR LE WEB

WWW

<http://www.hackfest.ca/>



[@hackfest\\_ca](https://twitter.com/hackfest_ca)



[hackfestca](https://www.youtube.com/channel/UC...)

QUESTIONS?

