



HACKFEST 2017

---

9 LIVES EDITION

---

# PLAN DE LA PRÉSENTATION

- ▶ Qu'est-ce que le Hackfest?
- ▶ Résumé de la 9ème édition
- ▶ Conclusion

# HACKFEST?

---

# QU'EST-CE QUE LE HACKFEST?

- ▶ Le plus gros événement sur le piratage et la sécurité informatique au Canada (~900 participants)
- ▶ **Quand?** En novembre
- ▶ **Où?** À Québec
- ▶ **Combien?** 90\$ en prévente, 120\$ à la porte
- ▶ **Quoi?** Conférences, Ateliers, CTF, Crochetage, Ingénierie sociale
- ▶ Bilingue, *mais surtout anglophone*

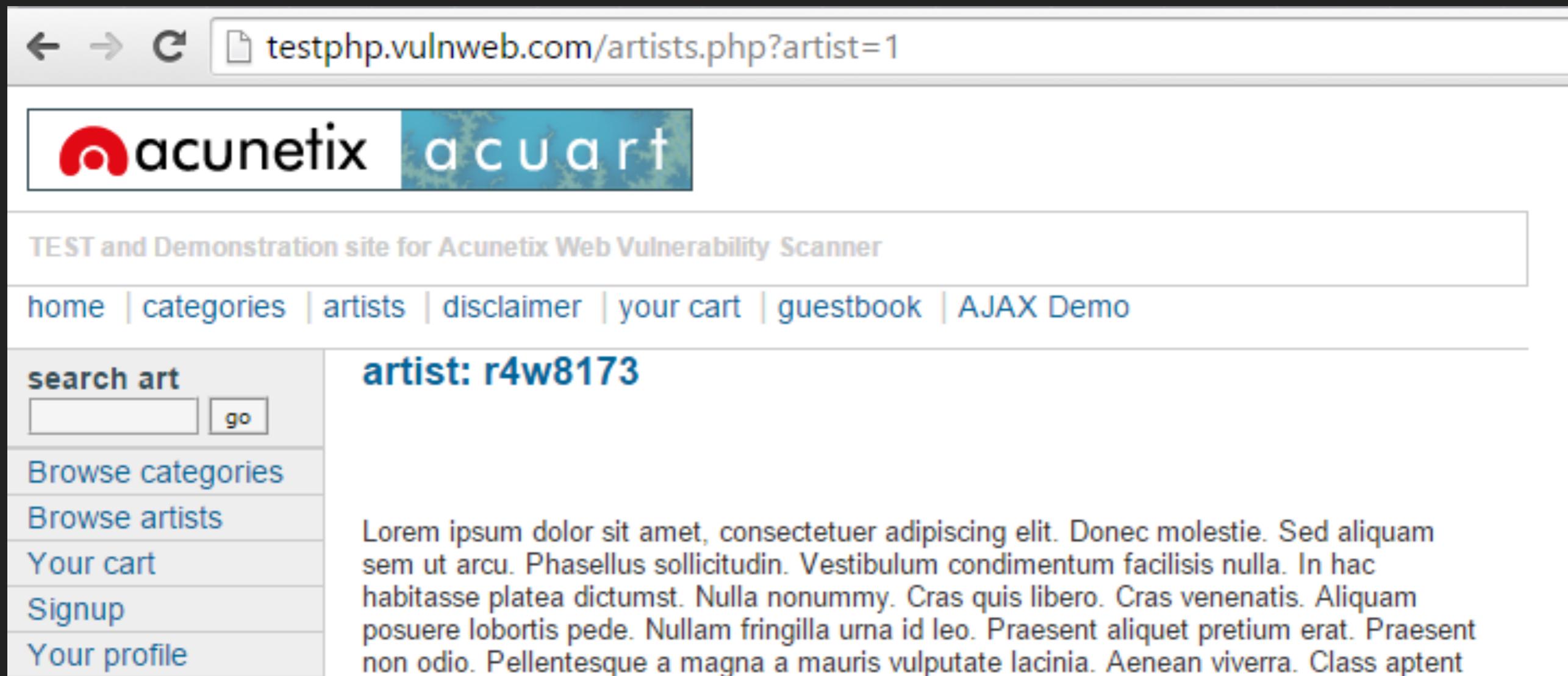
---

# CTF?

- ▶ *Capture the Flag*
- ▶ Jeu d'habileté qui simule un environnement présentant des vulnérabilités pouvant être exploitées 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

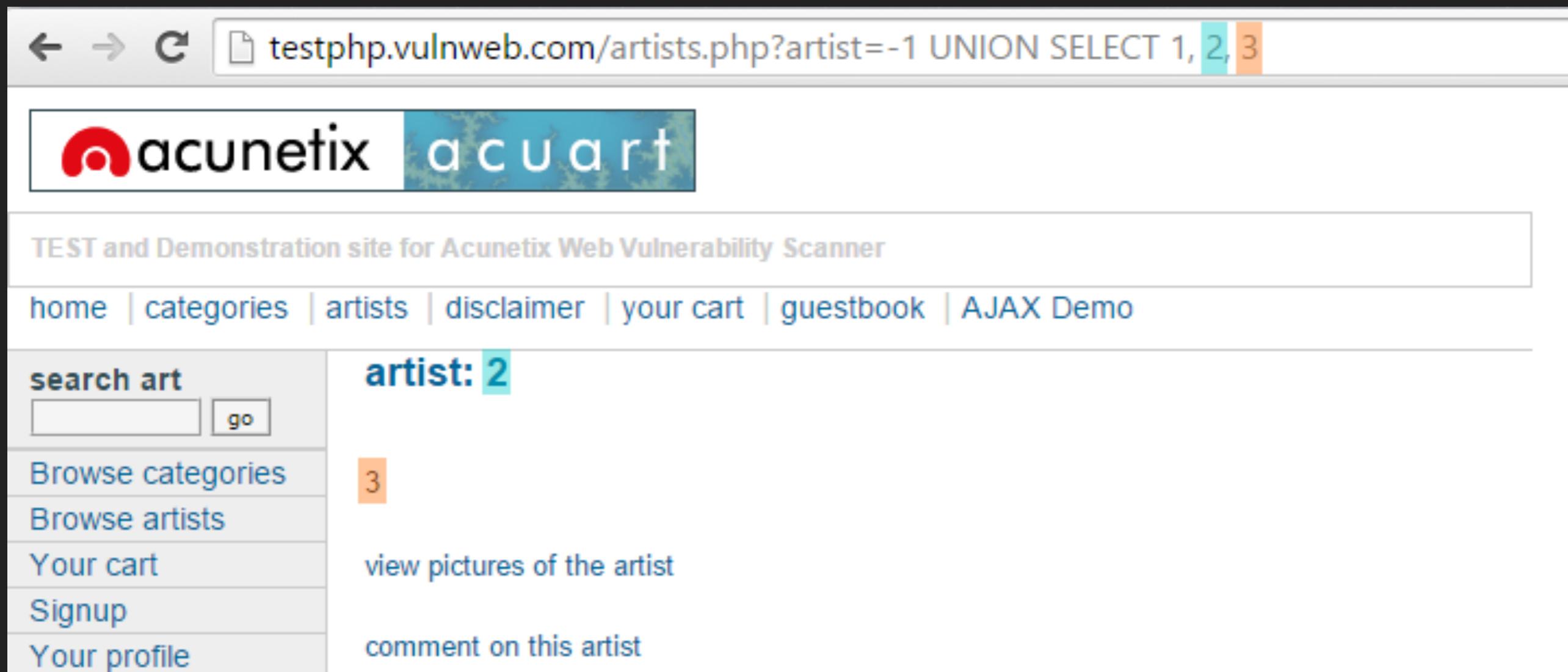
- ▶ Trouver une requête acceptant les entrées de l'utilisateur



The screenshot shows a web browser with the URL `testphp.vulnweb.com/artists.php?artist=1` in the address bar. The page is titled "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays the text "artist: r4w8173" followed by a large block of placeholder text: "Lorem ipsum dolor sit amet, consectetuer 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". On the left, there is a sidebar with a "search art" form containing a text input and a "go" button, and a list of links: "Browse categories", "Browse artists", "Your cart", "Signup", and "Your profile".

# CTF-EXEMPLE D'INJECTION SQL

- ▶ **Essayer de modifier les paramètres de la requête**

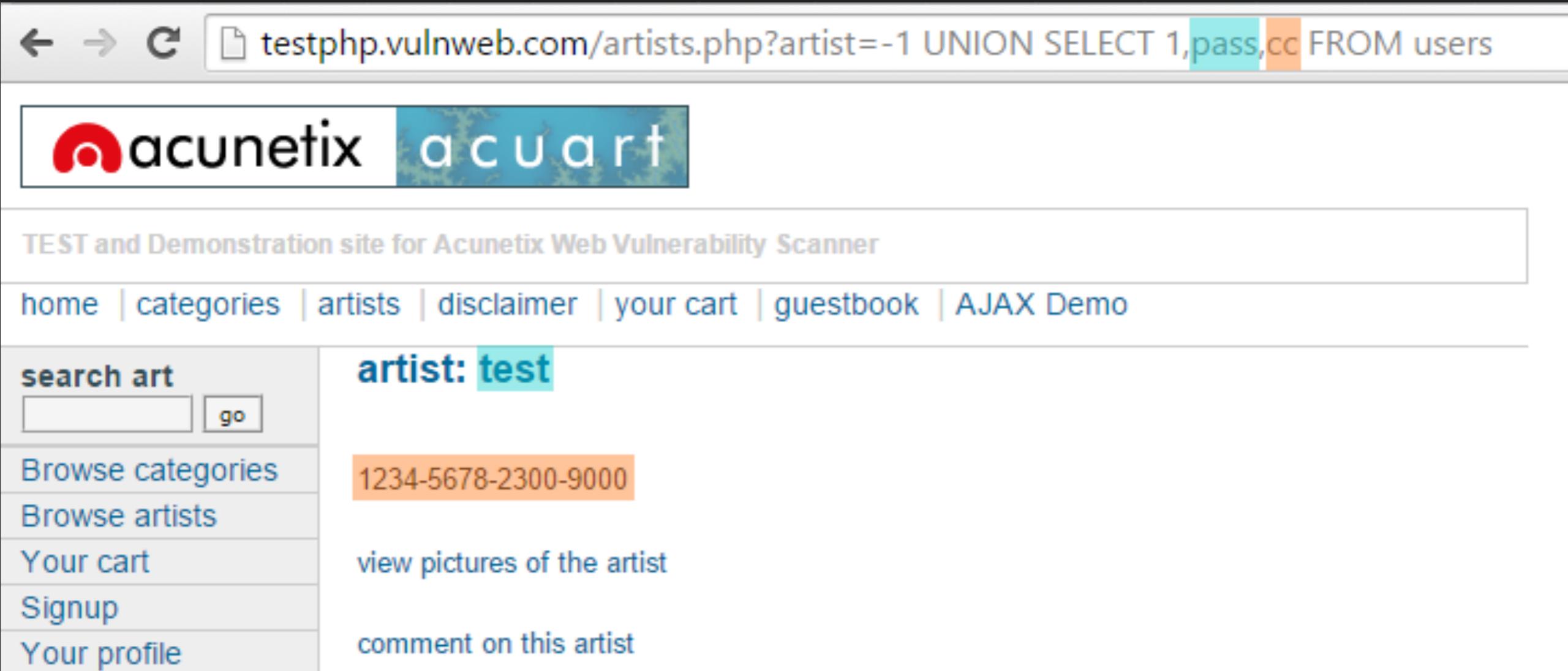


The screenshot shows a web browser with the following details:

- Address Bar:** testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, 2, 3
- Page Title:** TEST and Demonstration site for Acunetix Web Vulnerability Scanner
- Header:** acunetix acuart
- Navigation:** home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
- Left Sidebar (search art):**
  - Search input field
  - Go button
  - Browse categories
  - Browse artists
  - Your cart
  - Signup
  - Your profile
- Main Content:**
  - Artist: 2
  - 3
  - [view pictures of the artist](#)
  - [comment on this artist](#)

# CTF-EXEMPLE D'INJECTION SQL

- Abuser la requête pour récupérer des données



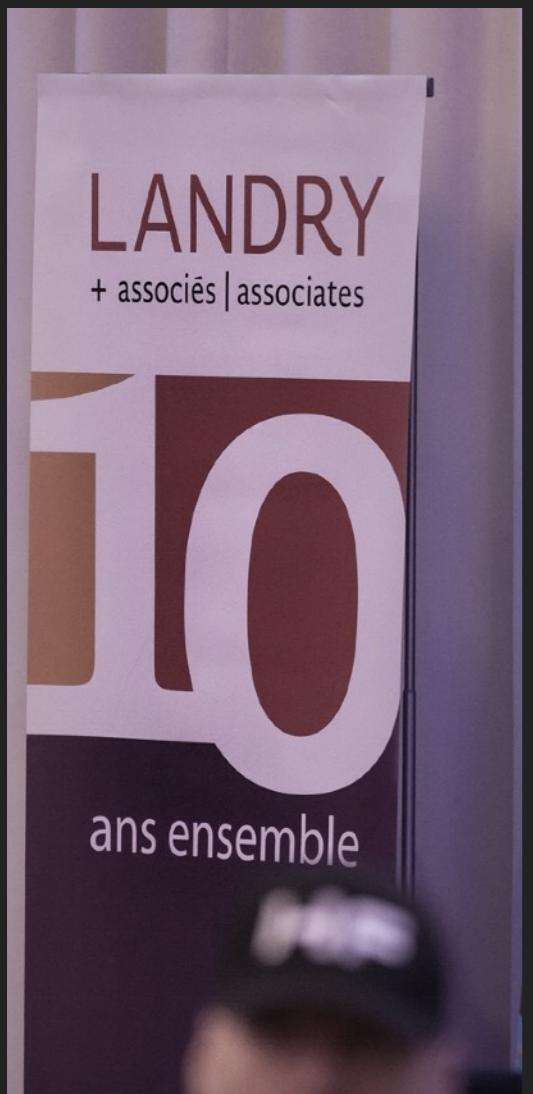
The screenshot shows a web browser with the following details:

- Address Bar:** testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users
- Page Header:** acunetix acuart
- Page Title:** TEST and Demonstration site for Acunetix Web Vulnerability Scanner
- Page Navigation:** home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
- Left Sidebar (search art):**
  - Search input field
  - Go button
  - Browse categories
  - Browse artists
  - Your cart
  - Signup
  - Your profile
- Main Content:**
  - Artist search input: artist: test
  - Result: 1234-5678-2300-9000
  - Links: view pictures of the artist, comment on this artist

# RÉSUMÉ DE LA 9ÈME EDITION

# POUR LA PREMIÈRE FOIS, DES ÉTUDIANTS DU COLLÈGE PARTICIPENT!





# FORMATIONS





# JOUR 1

# SUPERHÉROS TOUS! COMMENT L'EMPATHIE PEUT AIDER L'INCLUSION DU PERSONNEL AVEC ASD/ADHD



# FINGERPRINTING ANDROID MALWARE PACKAGING PROCESS THROUGH STATIC ANALYSIS TO IDENTIFY THEIR CREATOR

**Fingerprinting Android malware packaging  
process through static analysis to identify  
their creator**



**François Gagnon**

[francois.gagnon@ccirc-ccric.ca](mailto:francois.gagnon@ccirc-ccric.ca)

[www.cegep-ste-foy.qc.ca/cybersecurite](http://www.cegep-ste-foy.qc.ca/cybersecurite)

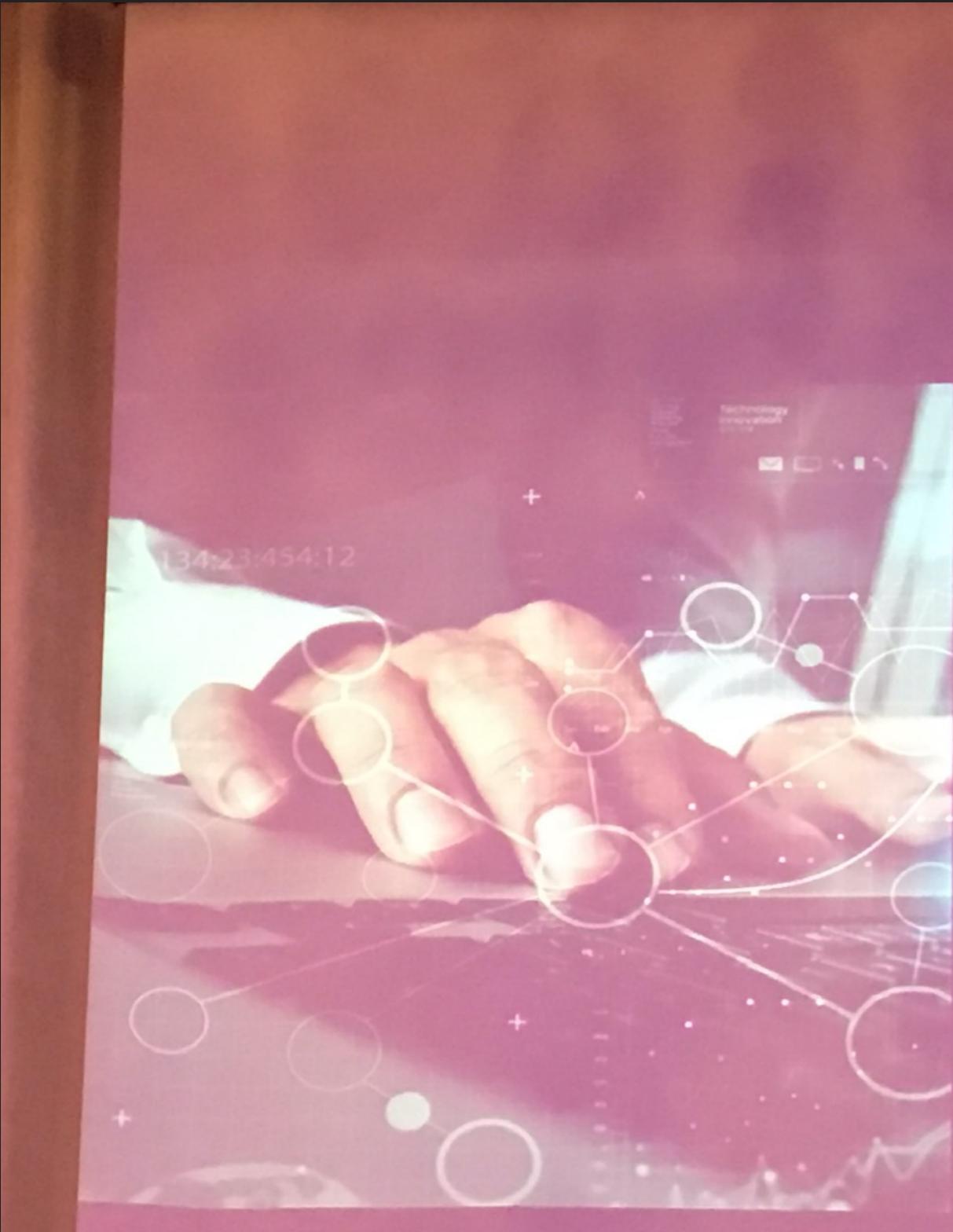


**Frédéric Massicotte**

Canadian Cyber Incident Response Centre (CCIRC)  
Public Safety Canada

Hackfest 2017

# CREATING A PROFESSIONAL-QUALITY EMBEDDED DEVICE ON A BUDGET



**MAKE A THING –  
CREATING A  
PROFESSIONAL-  
QUALITY  
EMBEDDED DEVICE  
ON A BUDGET**

Michael Vieau, CISSP, CEH  
Kevin Bong, GSE, PMP, QSA,  
CISSP, GCIH, GCFA  
November 3, 2017

**SIKICH.**

# HOW TO PWN AN ENTERPRISE IN 2017 (OR 2016, OR 2015...)



# BEATING THE DISINFORMATION DRIFT: FACTS ABOUT THE ALPHABAY MARKET

## Beating the Disinformation Drift Facts about the AlphaBay Market

Masarah Paquet-Clouston  
GoSecure Research



# PRACTICAL ANALYSIS OF AWARENESS



# BANKING ON INSECURITY: WHY ATTACKERS CAN TAKE THE MONEY AND RUN





CTF

---

HACKFEST

---

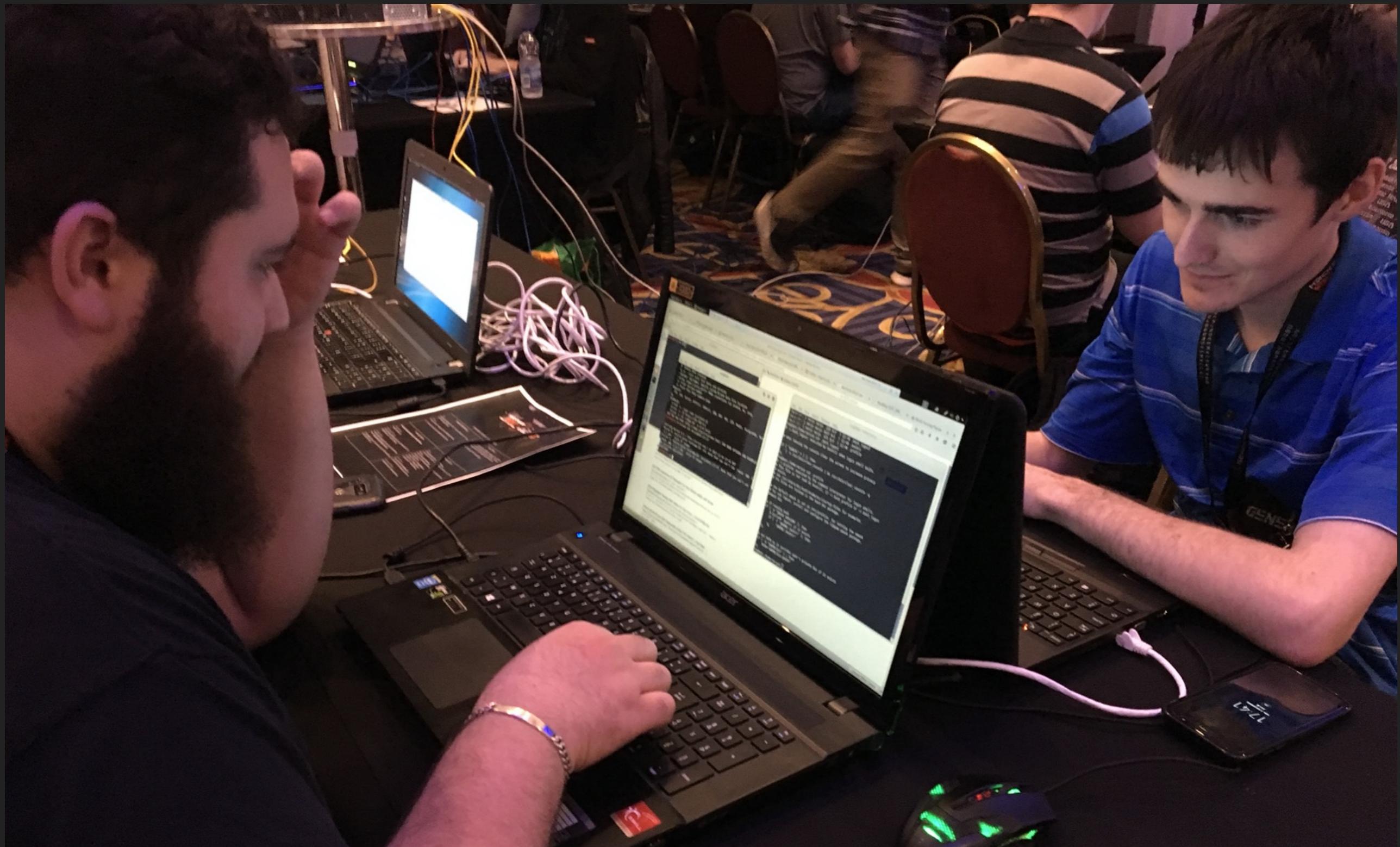
CTF



CTF



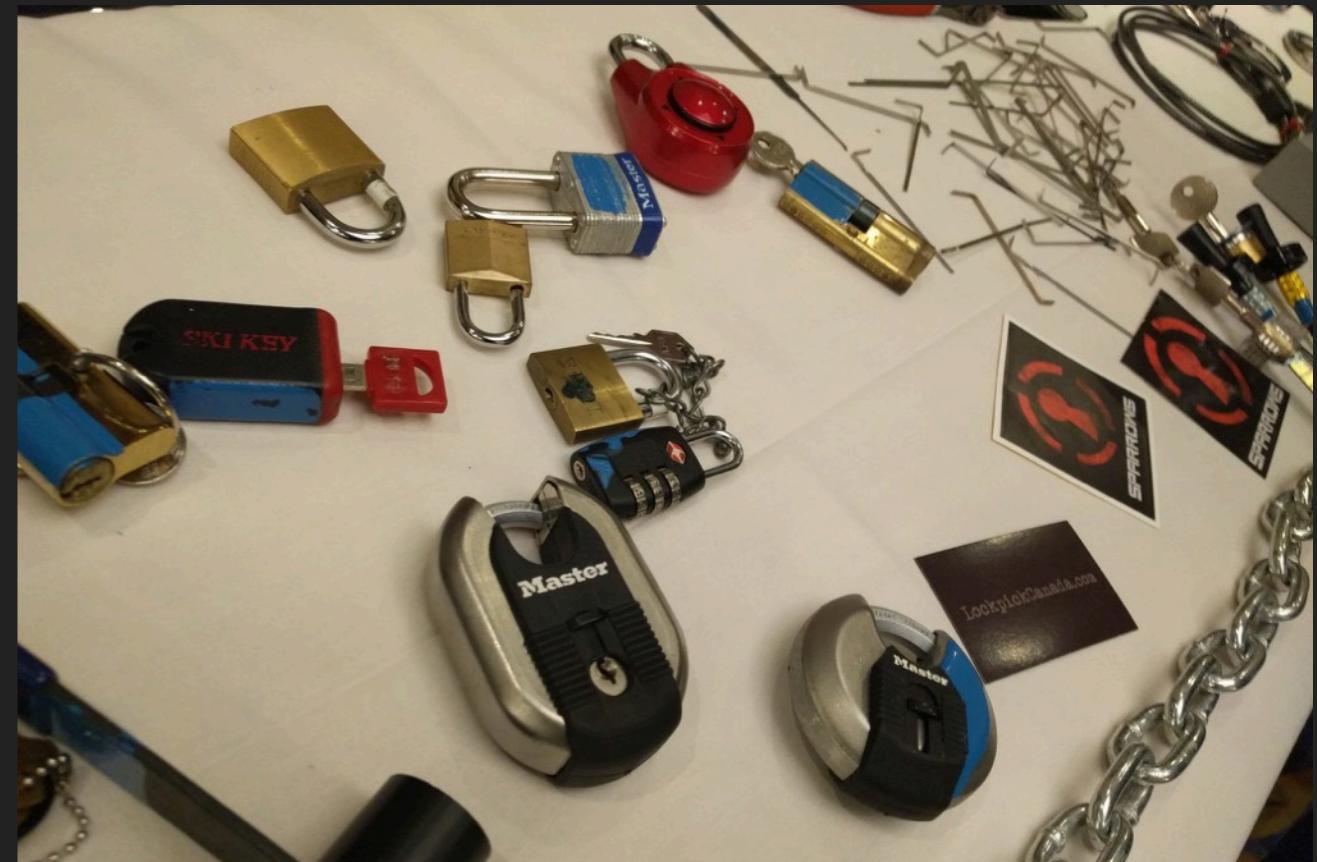
# CTF



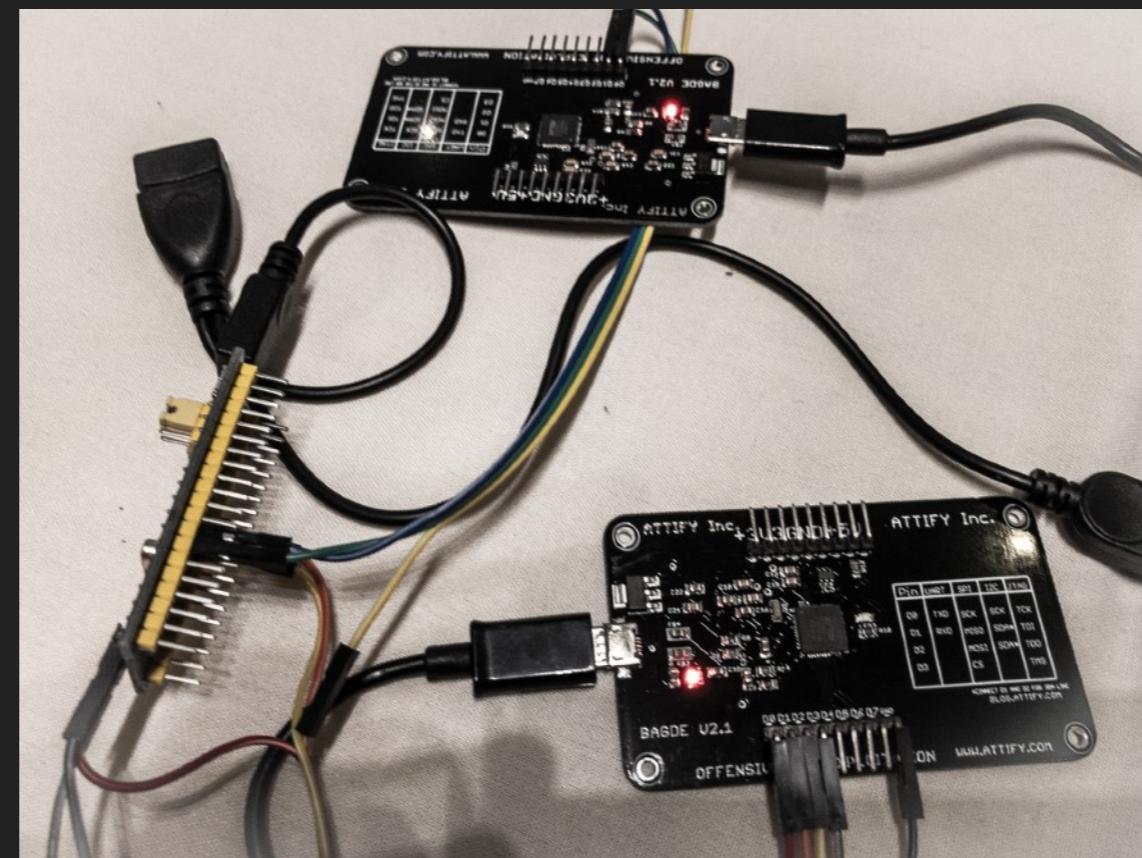
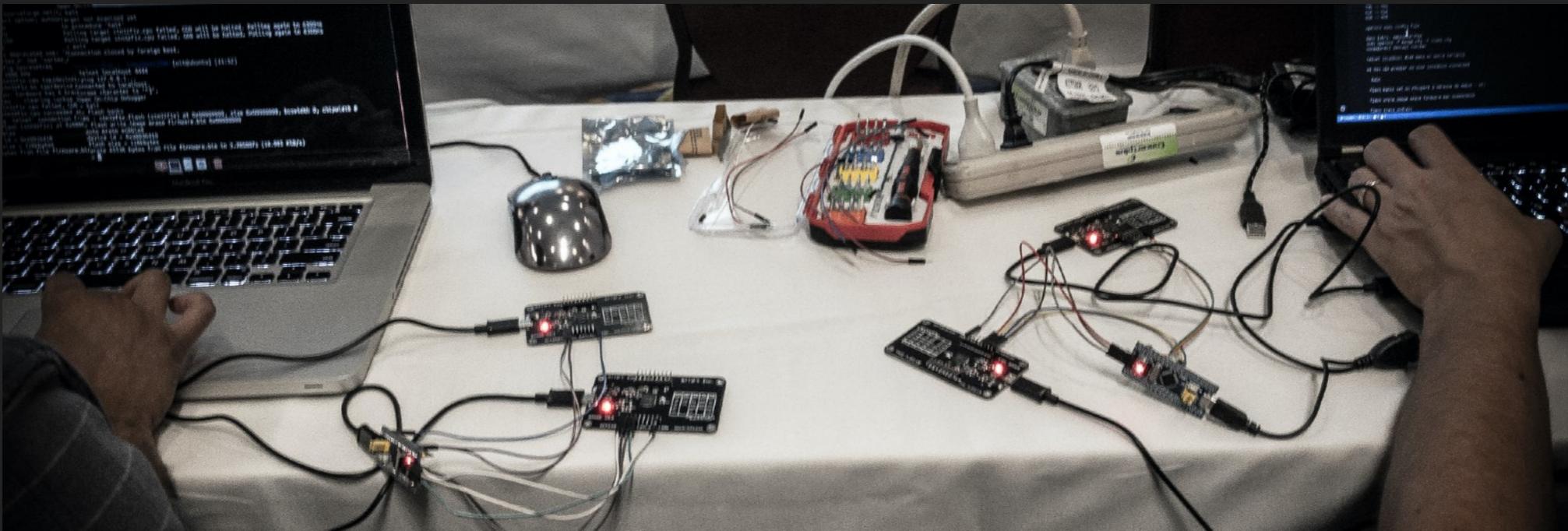
# CTF - 270 PARTICIPANTS



# CTF - CROCHETAGE



# CTF - ÉLECTRONIQUE



# CTF - INGÉNIERIE SOCIALE





---

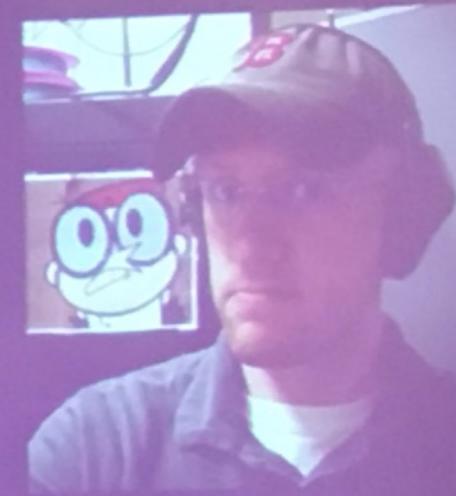
# JOUR 2

# ATTACK DRIVEN DEVELOPMENT: GETTING STARTED IN APPLICATION SECURITY

hackFest.CA

## Attack Driven Development

Getting Started in Application Security



Presented by:  
Keith Hoodlet



@andMYhacks



<https://github.com/andMYhacks>



keith@attackdriven.io

Nov. 3rd & 4th, 2017

# GENETIC ALGORITHMS FOR BRUTE FORCING



# DISSECTING A METAMORPHIC FILE-INFECTING RANSOMWARE

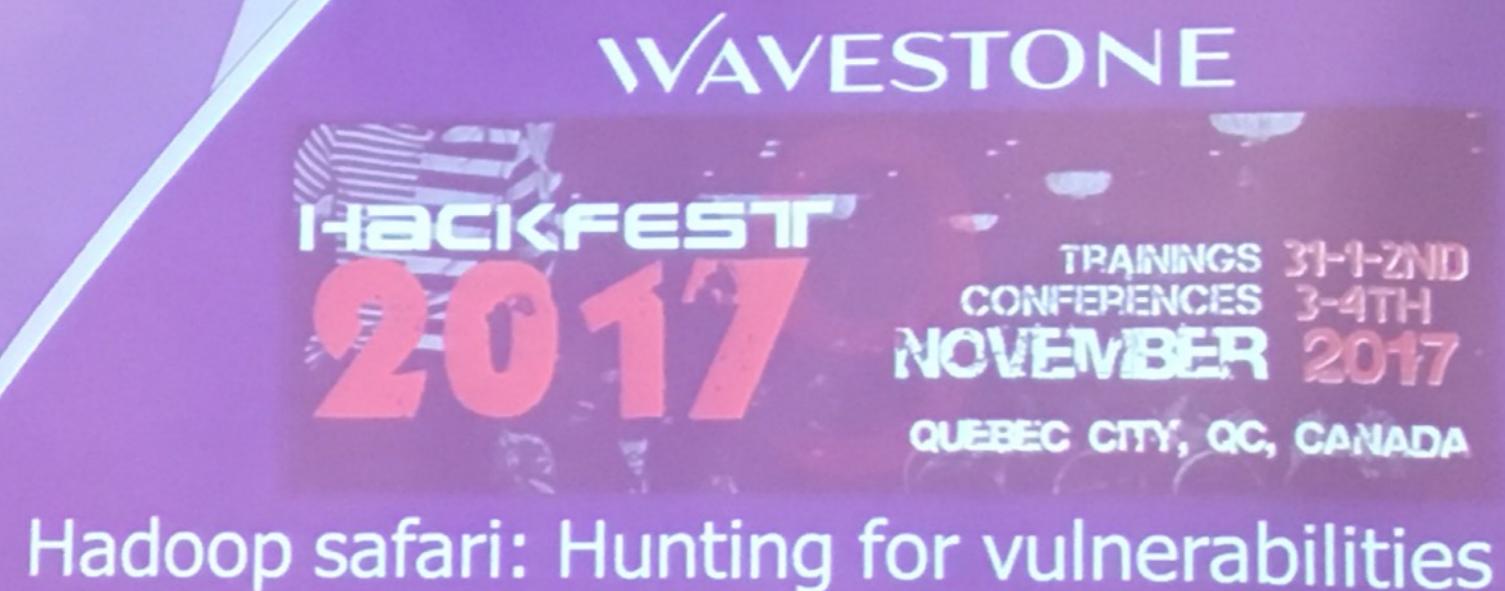


---

# STATIC-ANALYSIS TOOLS: NOW YOU'RE PLAYING WITH POWER!



# HADOOP SAFARI : HUNTING FOR VULNERABILITIES



Hackfest 2017 – November, 4th

Thomas DEBIZE  
[thomas.debize@wavestone.com](mailto:thomas.debize@wavestone.com)

# LESSONS LEARNED HUNTING IOT MALWARE

Lessons Learned Hunting IoT Malware

Olivier Bilodeau, <[obilodeau@gosecure.ca](mailto:obilodeau@gosecure.ca)>

GoSECURE

# LES VÉHICULES AUTONOMES, LEUR TÉLÉMÉTRIE ET L'IMPACT SUR LA SÉCURITÉ

Les véhicules autonomes, leur télémétrie  
et l'impact sur la sécurité

Marc-André Bélanger, CFE, CEPT, CISSP, CPO  
Hackfest 2017

# BUGCROWD PARTY ET MINI-CTF OWASP



---

# <DUALCORE>

- ▶ <http://dualcoremusic.com/nerdcore/>



# PODCAST - LA FRENCH CONNECTION

► <http://securite.fm/>



---

# MINI-CTF OWASP

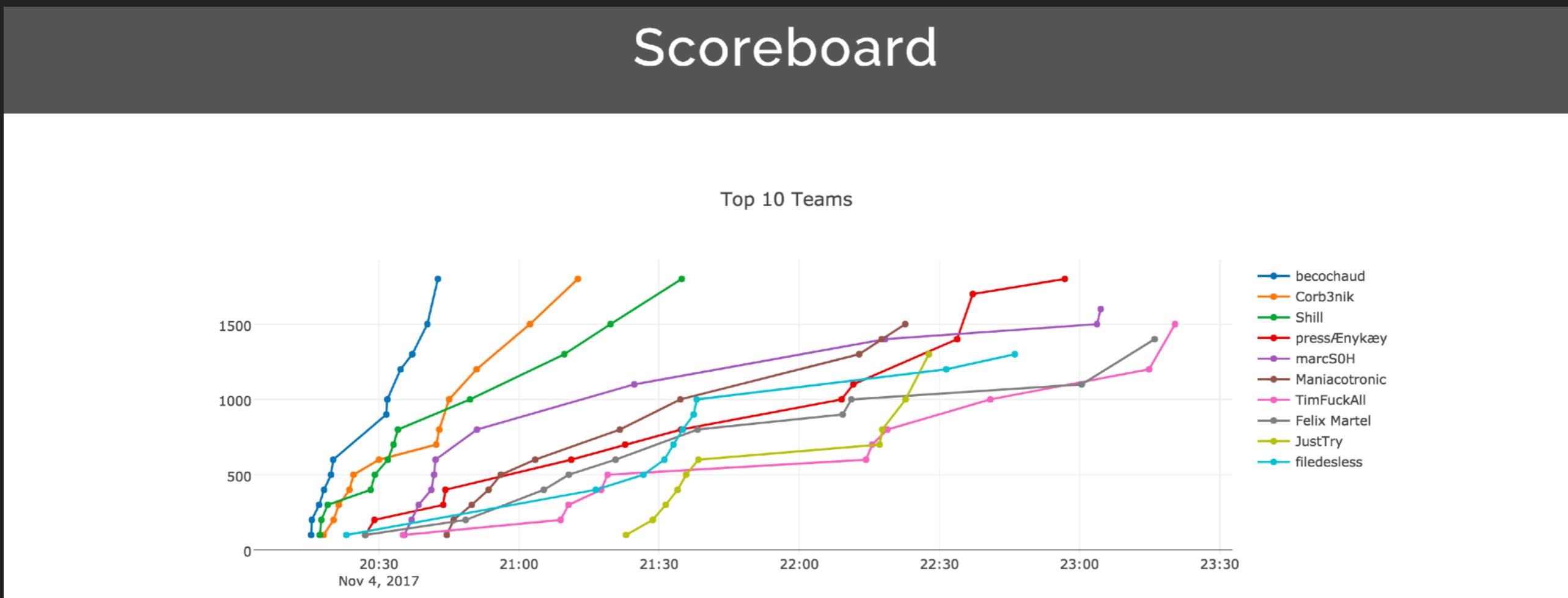


# MINI-CTF OWASP : 12ÈME / 57

Mini-CTF OWASP    Teams    Scoreboard    Challenges    Team    Profile    Logout

## Challenges

Qualification					
Privilege Escalation 2 100	Upload 1 100	Privilege Escalation 1 100	SQL Injection 1 100	Encoding 1 100	RCE 1 100
Local File Inclusion 1 100	Direct Object Reference 1 100	XXE 1 200	Exploit 1 200	Upload 2 300	SQL Injection 2 300



# 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/user/hackfestca)



<https://www.flickr.com/photos/hackfest2k9>

---

# RESSOURCES POUR DÉMARRER

- ▶ <https://www.hackerone.com/start-hacking>
- ▶ <https://www.offensive-security.com/metasploit-unleashed/>
- ▶ [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)
- ▶ <https://leanpub.com/web-hacking-101>
- ▶ <https://leanpub.com/ltr101-breaking-into-infosec>
- ▶ <https://www.amazon.ca/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470>

---

# IMPACT DU HACKFEST AU COLLÈGE SHAWINIGAN

- ▶ Site du département

<https://shawinigan.info/le-departement-participe-au-hackfest-2017-a-quebec/>

- ▶ Journal du réseau collégial du Québec

[http://lescegeps.com/pedagogie/approches\\_pedagogiques/des\\_conferences\\_formatrices\\_en\\_securite\\_informatique\\_a\\_u\\_college\\_shawinigan](http://lescegeps.com/pedagogie/approches_pedagogiques/des_conferences_formatrices_en_securite_informatique_a_u_college_shawinigan)

- ▶ Mise en place d'un club de sécurité informatique au département à l'**hiver 2018**

QUESTIONS? 😊