HACKFEST
UPSIDEDOWN
EDITION

HACKFEST 2019

UPSIDEDOWN EDITION

PLAN DE LA PRÉSENTATION

- Qu’est-ce que le Hackfest?
- Pourquoi participer?
- Résumé de la dernière édition
- Conclusion

HACKFEST? 

QU'EST-CE QUE LE HACKFEST?

- Le plus gros événement de sécurité informatique au Canada (~1300 pers.)
  - **Quand?** En novembre
  - **Où?** À Québec
  - **Combien?** 90$ en prévente, 120$ à la porte
  - **Quoi?** Réseautage, Conférences, Formations Ateliers, Villages, *CTF*
    - Bilingue, *mais surtout anglophone*

CONFÉRENCES

FORMATIONS ET ATELIERS

RÉSEAUTAGE


OWASP
Open Web Application
Project
OWASP


EGYDE
CYBERSÉCURIT
SORTIE
DES SERVICES INNOVANTS
EN CYBER URITÉ


Remot
Devolutions
Password Server
Wayk N
GESTIO
CONN
GES
MOT
ACCÈS
SO
A


SECURE ACCESS
IN A WORLD
WITHOUT
BOUNDARIES
MAKE
RISK
LESS
RISKY
RAPIDLY LINK
BUSINESS RISK
TO A
SECURITY
INCIDENT
RSA SEC
RSA


GARDIEN
TUEL
Sé é de l'information
PARTNER
Gardien Virtuel est partenaire
exclusif d'AlienVault au
Québec !
www.gardienvirtuel.ca/siem
Services conseils
• ISO 27001 / PCI / Conti
• Audits de sécurité
• Sécurité de sites Web


scalar
scalar

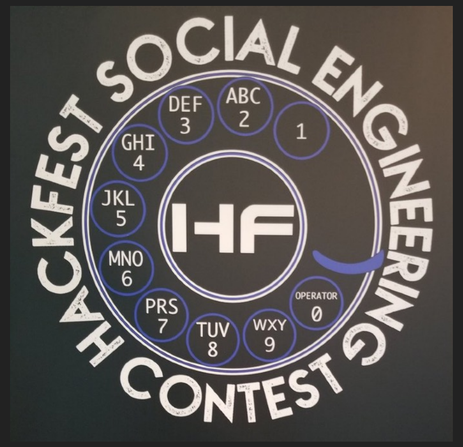
OBJETS CONNECTÉS

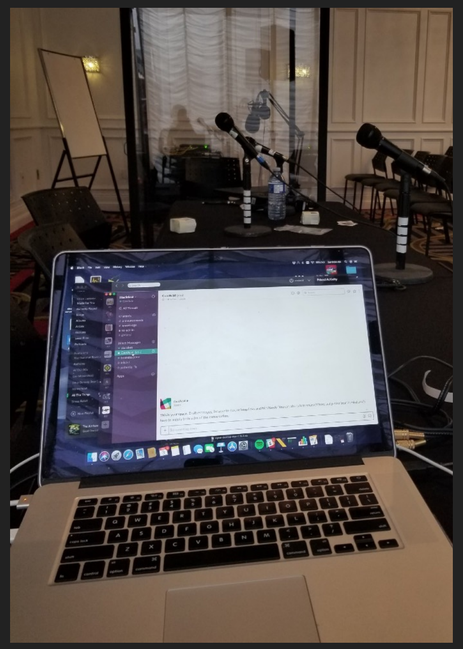
SOUDURE


SOLDERING
VILLAGE
HACKFEST DECADE
NOVEMBER 2ND
2-3 NOVEMBRE 2018 // QUÉBEC, CANADA
Throwing Star LAN Tap
GREAT SCOTT GADGETS
J1
J3
J4
C1 220pF
C2 220pF

CROCHETAGE

INGÉNIERIE SOCIALE



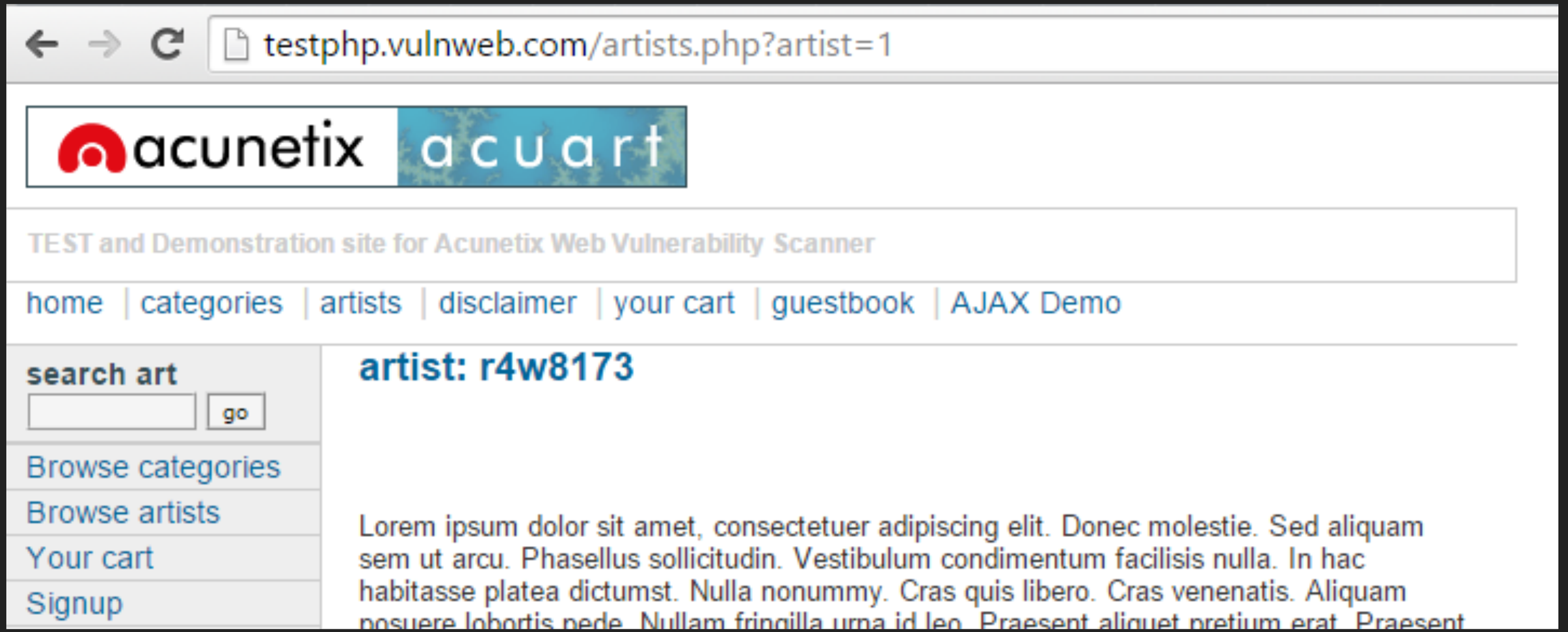


CTF?

- *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

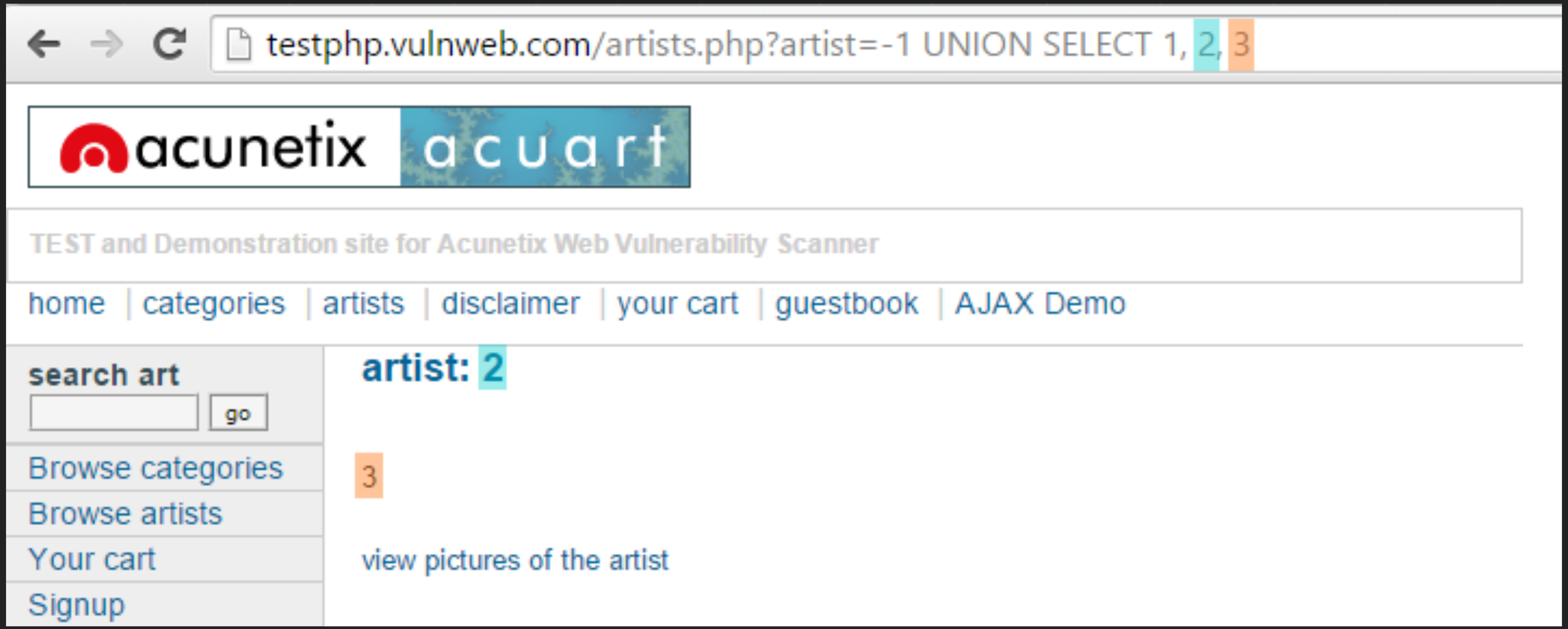
CTF-EXEMPLE D'INJECTION SQL

- Trouver une requête acceptant les entrées de l'utilisateur



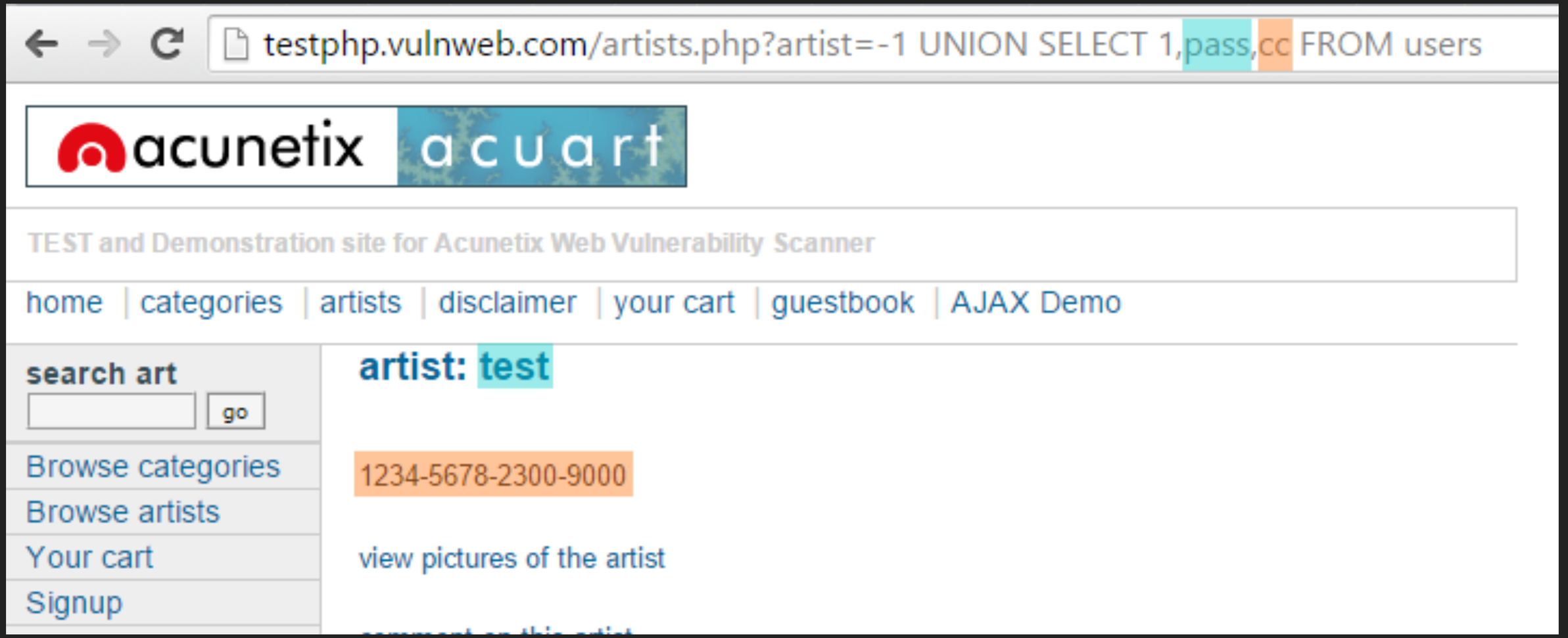
CTF-EXEMPLE D'INJECTION SQL

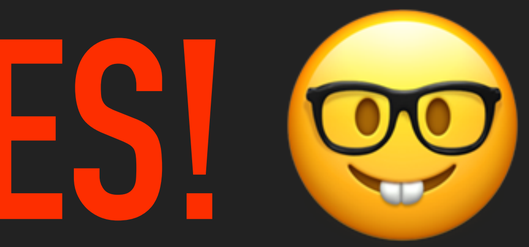
- Essayer de modifier les paramètres de la requête



CTF-EXEMPLE D'INJECTION SQL

- Abuser la requête pour récupérer des données



PLUS D'EXEMPLES! 

POURQUOI? 

RESPONSABILITÉS D'UN DÉVELOPPEUR

- En tant que développeur, vous avez un rôle primordial à jouer dans la mise en oeuvre de la **sécurité dans les applications**
- Votre code effectue divers traitements sur les données et peut constituer la porte d'entrée vers une utilisation non-autorisée
- Vous devez exploiter le principe de **programmation défensive** pour corriger les failles potentielles au fur et à mesure de la rédaction du code
- Ainsi, connaître les techniques de contournement devient un atout pour mieux se sécuriser: ***Hacker Mindset***
- **Être conscient des enjeux inhérents à la sécurité vous rends plus complet**

RÉSUMÉ DE LA DERNIÈRE ÉDITION

PARTICIPATION DES ÉTUDIANTS DU PROGRAMME AU HACKFEST DE QUÉBEC!

Énigmatiks
CÉGEP DE SHAWINIGAN

Fièrement propulsé par
ICO
SOLUTIONS

JOUR 1

JOUR 1

- F2P - Free to pawn
  Portée abusive des publicités dans les applications mobiles
- You shall not pass, even if you look like a hobbit
  Défis de la sécurité physique
- Mind the gap - managing insecurity in enterprise IoT
  Gestion des objets connectés sur un réseau à grande échelle.
- Conclusions from Tracking Server attacks at scale
  Résultats d'une recherche du comportement des attaquants sur des *honeypots*
- *Why Johnny still can't pentest*
  Comparaison de plusieurs outils d'analyse de vulnérabilités *open source*

JOUR 2

JOUR 2

- Journée d’atelier
  - Deserialization: RCE for modern web applications
    Atelier d’expérimentation des mécanismes vulnérables en *désérialization* de Java et .Net
  - User Interaction Revisited: Beyond alert(1);
    Mise en place d’une preuve de concept d'exploitation d’une chaîne de vulnérabilités sur Wordpress menant à la prise de contrôle de l’hôte.

CTF

- Beginner
- Hackfest
- 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!

IMPACT DU HACKFEST AU COLLÈGE SHAWINIGAN

- Site du département
  https://shawinigan.info/hackfest-2019/
- Journal du réseau collégial du Québec
  http://lescegeps.com/pedagogie/approches_pedagogiques/des_conferences_formatrices_en_securite_informatique_au_college_shawinigan
- Mise en place d'activités locales en sécurité informatique durant les semaines de relâche

HACKFEST SUR LE WEB

http://www.hackfest.ca/

@hackfest_ca

hackfestca

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

- Ressources connexes
  - securite.fm
  - quebecsec.ca
  - ihack.computer

RESSOURCES POUR DÉMARRER

- https://ressources.shawisec.ca/
  - https://www.hackerone.com/start-hacking
  - https://www.offensive-security.com/metasploit-unleashed/
  - 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

QUESTIONS?