HACKFEST 2018

DECADE EDITION

PLAN DE LA PRÉSENTATION

- Qu’est-ce que le Hackfest?
- Pourquoi participer?
- Résumé de la 10ème édition
- Conclusion

HACKFEST? 

QU'EST-CE QUE LE HACKFEST?

- Le plus gros événement de sécurité informatique au Canada (~1000 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


Remote
Devolutions
Password Server
Wayk


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


GARDIEN
TUEL
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

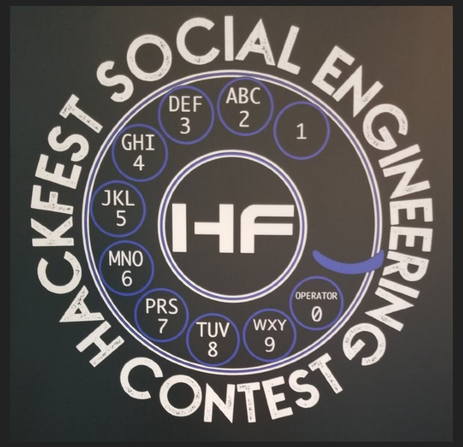
OBJETS CONNECTÉS

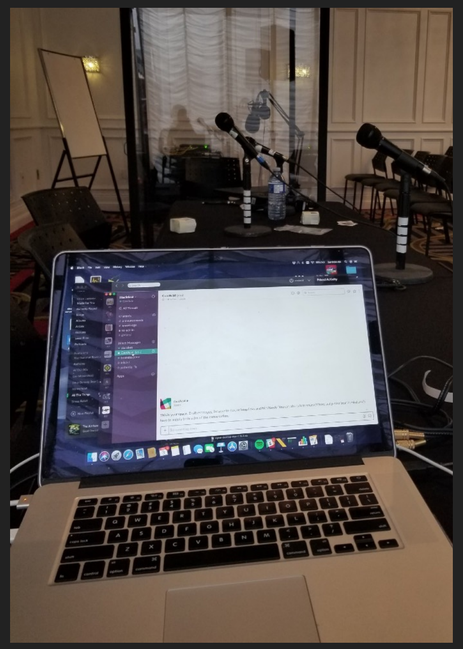
SOUDURE


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



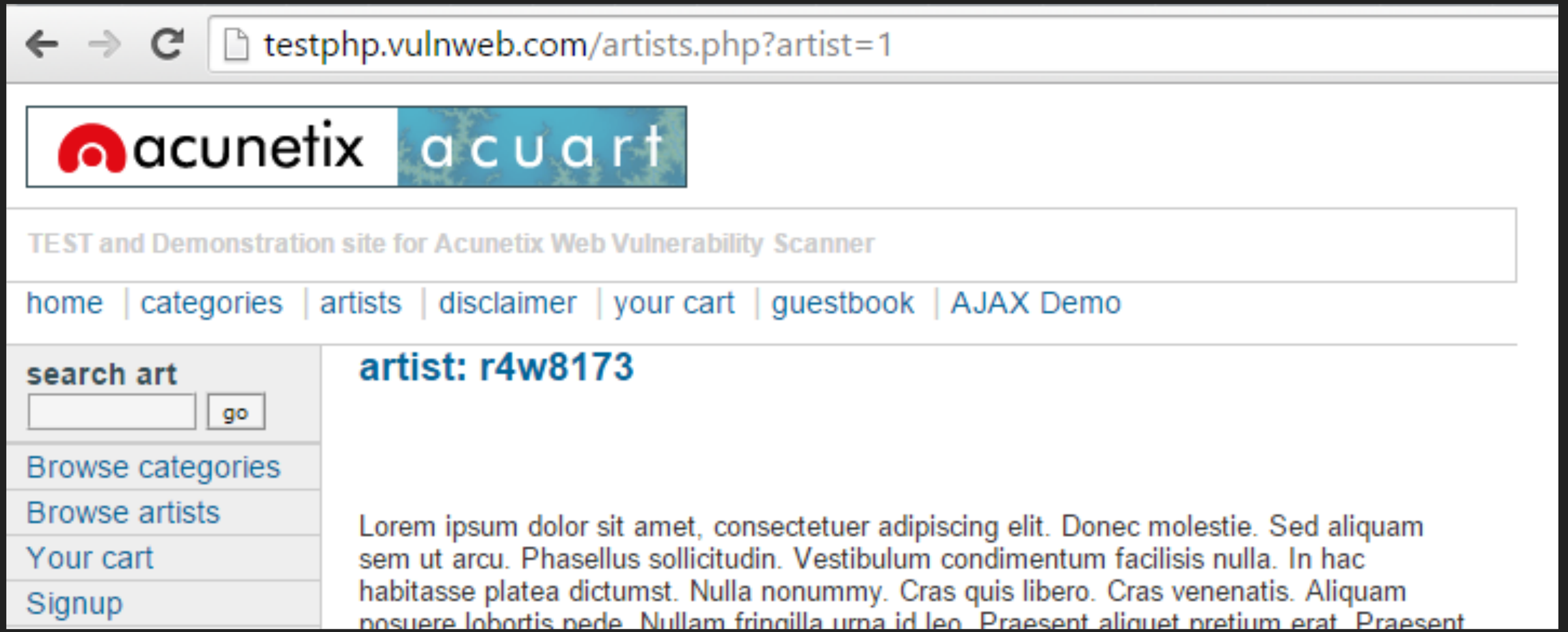


CTF?

- *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

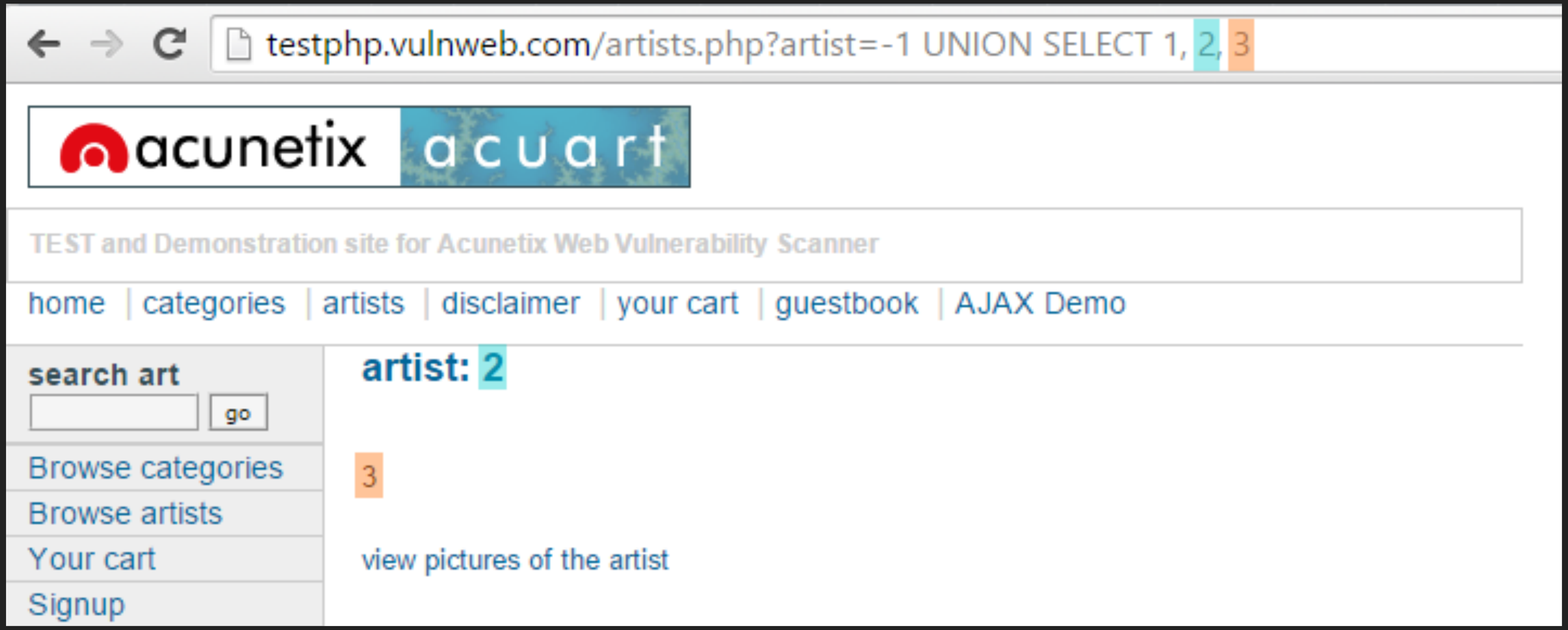
CTF-EXEMPLE D'INJECTION SQL

- Trouver une requête acceptant les entrées de l'utilisateur



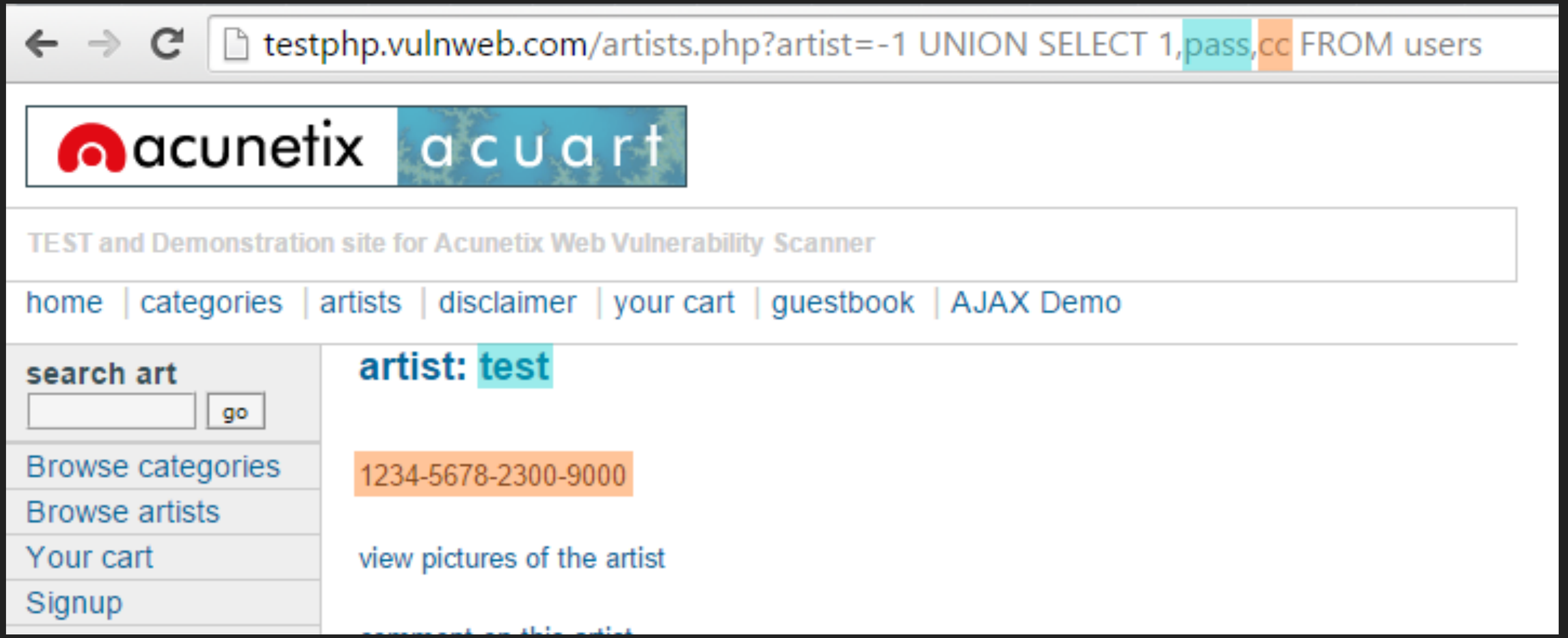
CTF-EXEMPLE D'INJECTION SQL

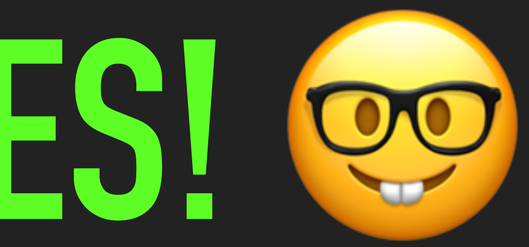
- Essayer de modifier les paramètres de la requête



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 10ÈME EDITION

PARTICIPATION DES ÉTUDIANTS DU PROGRAMME!

Enigmatiks
COLLÈGE SHAWINIGAN

Fièrement propulsé par
ICO
SOLUTIONS

JOUR 1

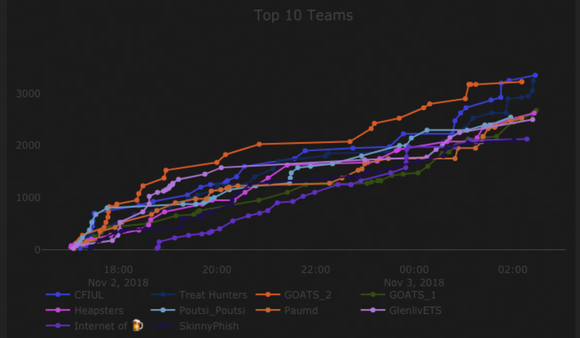
CTF HACKFEST

./challenges

- Nostalgia Track
  - Hackfest Infinity (by MaxWhite) (25) ✔
  - Hackfest Reloaded (by T3kn1cs) (25) ✔
  - Hackfest H4RdeR,B3ttEr, LoNGER, strONger (by T3kn1cs) (25) ✔
  - Hackfest The Return (by MaxWhite) (25) ✔
  - Hackfest Optimized (by MaxWhite) (25) ✔
  - Hackfest Revolution (by MaxWhite) (25) ✔
  - Hackfest Strikes Back (by MaxWhite) (25) ✔
  - Hackfest Lucky Edition (by MaxWhite) (25) ✔
  - H9ckfest Nine Lives (by dax) (100)
  - Hack the Gibson (by Viper) (200)
- SSRF in the Clouds (by MaxWhite)
  - Easy Corporate Server (50) ✔
  - That magical place in the Cloud (75)
  - Hidey Corporate Server (100)
  - What a scheme... (100)
  - Octy Corporate Server (100) ✔
  - Hexy Corporate Server (100) ✔
  - Open-Source curiosity (125)
  - Shorty Corporate Server (150)
  - Modern Directory Listing (250)
  - What lies beyond... (275)
- Imperial ClusterOps (by LED)
  - Package Manager (50)
  - It's not serverless (50)
  - Someone is watching... (100)
  - Imperial Central Intelligence (150)
  - Message in Cloud City (150)
  - Cloud City's hidden gem (200)
  - Darth Vader (250)
  - Package Manager's manager (275)
- 3cma gone wild (by Antony)
  - Secure communication (50)
  - Cover your tracks (50)
  - Patience is key. (50)
  - Client Side Security (100)
  - SQLi's are easy (100)
- CloudHopper (by Justgeoff)
  - Single Page Static Content (Obviously!) (50)
  - It's all fun and games untill someone loses their ... (50)
  - Message in a bottle (50)
  - Still single but not really static (150)
- PhenixCorp
  - Phenix Login (SPA Failed Nostalgia) (50)
- Threat Hunting (by t3kn1cs)
  - 2 - Execute (75)
  - 5 - Hacking Back (100)
  - 1 - Find the IOC (150)
  - 3 - Decode (150)
  - 4 - Deobfuscate (200)
- /dev/random
  - Easy-Peasy (by MaxWhite) (75)
- La puce Chinoise (By Lei)
  - Serial Port Sniffing (100)
  - Undesirable access (100)
  - Fake node access ;) (200)
  - Extreme Temperature (350)
  - Sensor simulation (350)
- Blue Team (by t3kn1cs)
  - Stolen Flag (150) ✔
  - Malicious Document (150)
  - ReverseThis (150)
  - White paper (150) ✔
- Anonymous (Hash)
  - Mr Potato Hash Me Please! (300)

36	r00tmont.new	750
37	AcoDevTech	724
38	No Ragr3TS	675
39	HackAlpacas	650
40	Blueteam Ninjas	600
41	CDHE	595
42	LesPtitGarsDeShawiAlpha	575
43	LesPtitGarsDeShawiBeta	550
44	UpasdeS	550
45	nmapteam	550
46	UnicornPowered	500

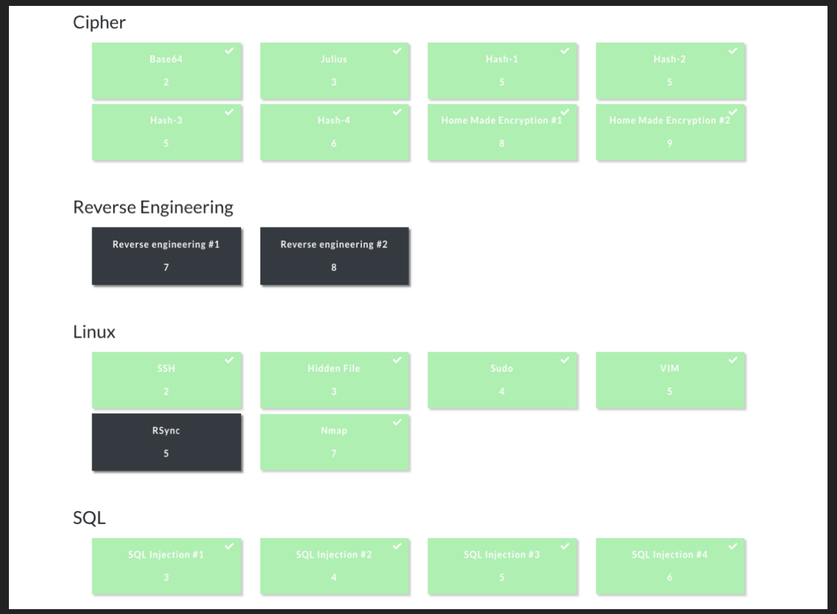
./scoreboard

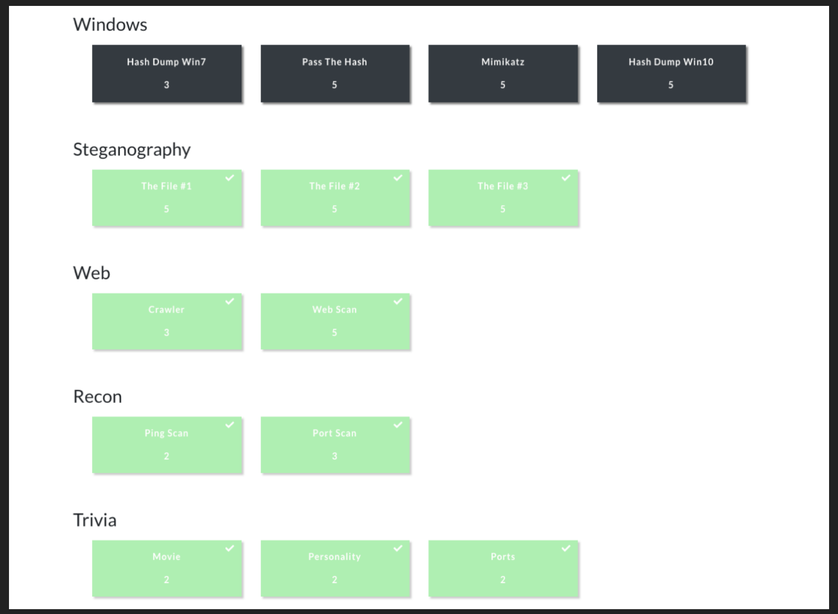


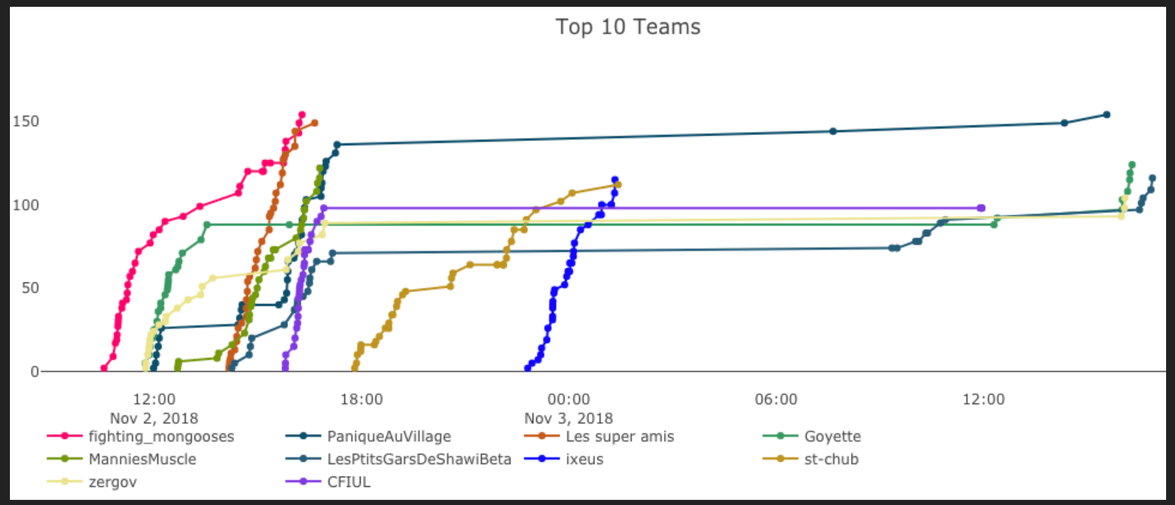
lace	team	score
1	CFIUL	3350
2	Treat Hunters	3250
3	GOATS_2	3225
4	GOATS_1	2675
5	Heapsters	2625
6	Poutsi_Poutsi	2545
7	Paumd	2525
8	GlenlivETS	2500
9	Internet of 🍺	2125
10	SkinnyPhish	2100
11	Internet Explorer	2025
12	buy high sell low	2024

JOUR 2

CTF NON COMPÉTITIF

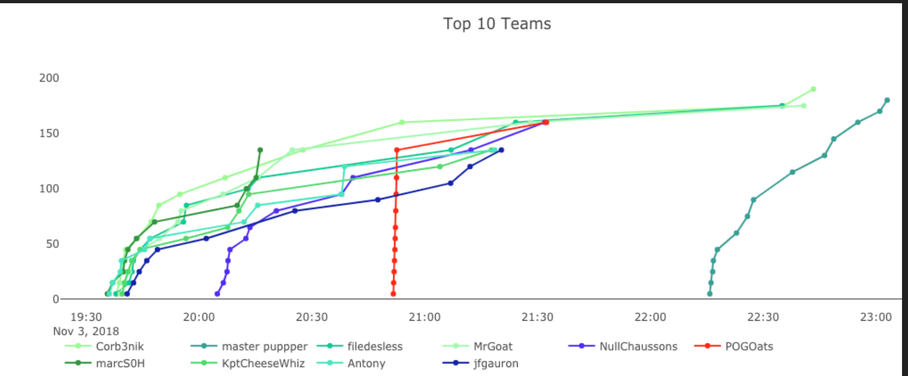






DÉFI ÉVASION

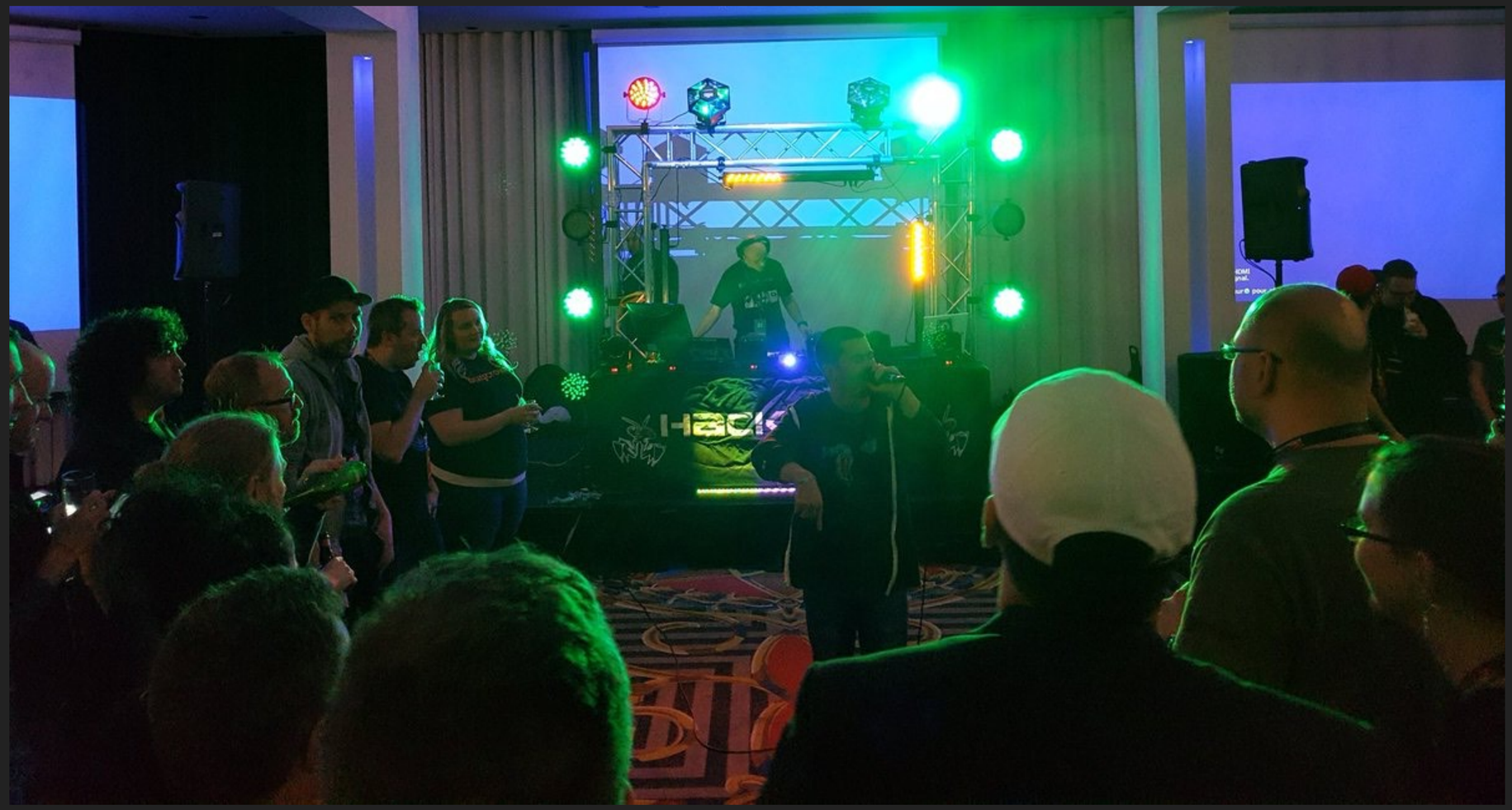
MINI-CTF OWASP



Place	Team	Score
1	Corb3nik	190
2	master puppper	180
3	filedesless	175
6	POGOats	160
7	marcS0H	135
8	KptCheeseWhiz	135
9	Antony	135
10	jfgauron	135
11	fighting_mongooses	135
12	Sideni	135
13	LesPtitsGarsDeShawi	135
14	BlahBlah	125
15	gnomz	125
16	team1	125
17	The_Nancys	125
18	a_bot	120
19	L'Enigmatik	120

<DUALCORE>

- http://dualcoremusic.com/nerdcore/



PODCAST – LA FRENCH CONNECTION

- http://securite.fm/

MINI-CTF OWASP

MINI-CTF OWASP : 12ÈME / 57

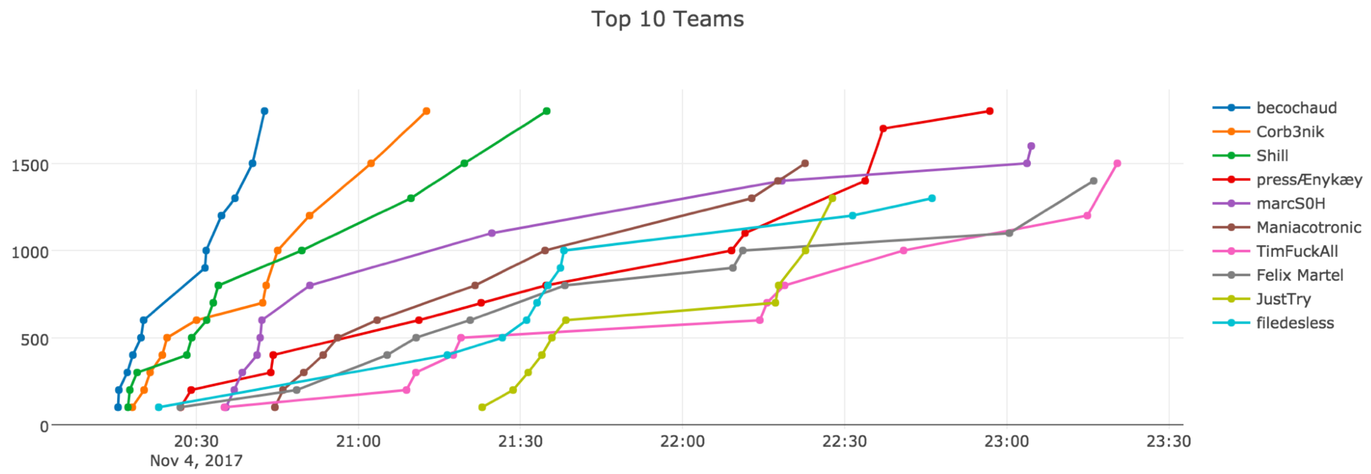
Mini-CTF OWASP Teams Scoreboard Challenges Team Profile Logout

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

Scoreboard



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-2018/
- 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

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://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?