



# Sécurité

# Sécurité ?

2

- ▶ Règle #1 : Never trust user inputs !
  - ▶ la force d'une chaine est égale à son maillon le plus faible
  - ▶ Hack = détourner de son usage normal

## ► Article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **deux ans d'emprisonnement et de 30 000 euros d'amende**.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de **trois ans d'emprisonnement et de 45 000 euros d'amende**.

## ► Article 323-2

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de **cinq ans d'emprisonnement et de 75 000 euros d'amende**.

# Législation

4

- ▶ **Article 323-3**

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de **75 000 euros d'amende**.

- ▶ **Article 323-3-1**

Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

► **Article 323-4**

La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou **pour l'infraction la plus sévèrement réprimée**.



► **Article 323-5**

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° **L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille**, suivant les modalités de l'article 131-26;

2° **L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle** ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° **La confiscation de la chose qui a servi ou était destinée à commettre l'infraction** ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° **La fermeture, pour une durée de cinq ans au plus, des établissements** ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° **L'exclusion, pour une durée de cinq ans au plus, des marchés publics** ;

6° **L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques** autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

# Législation

7

## ► **Article 323-6**

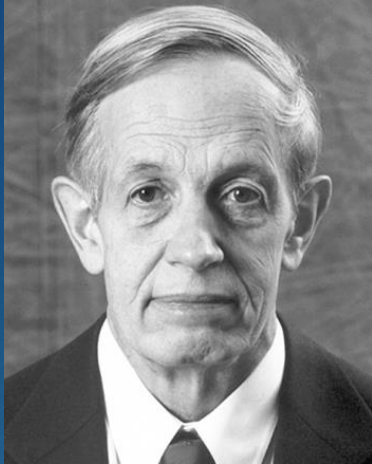
Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39. L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

## ► **Article 323-7**

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

# Histoire

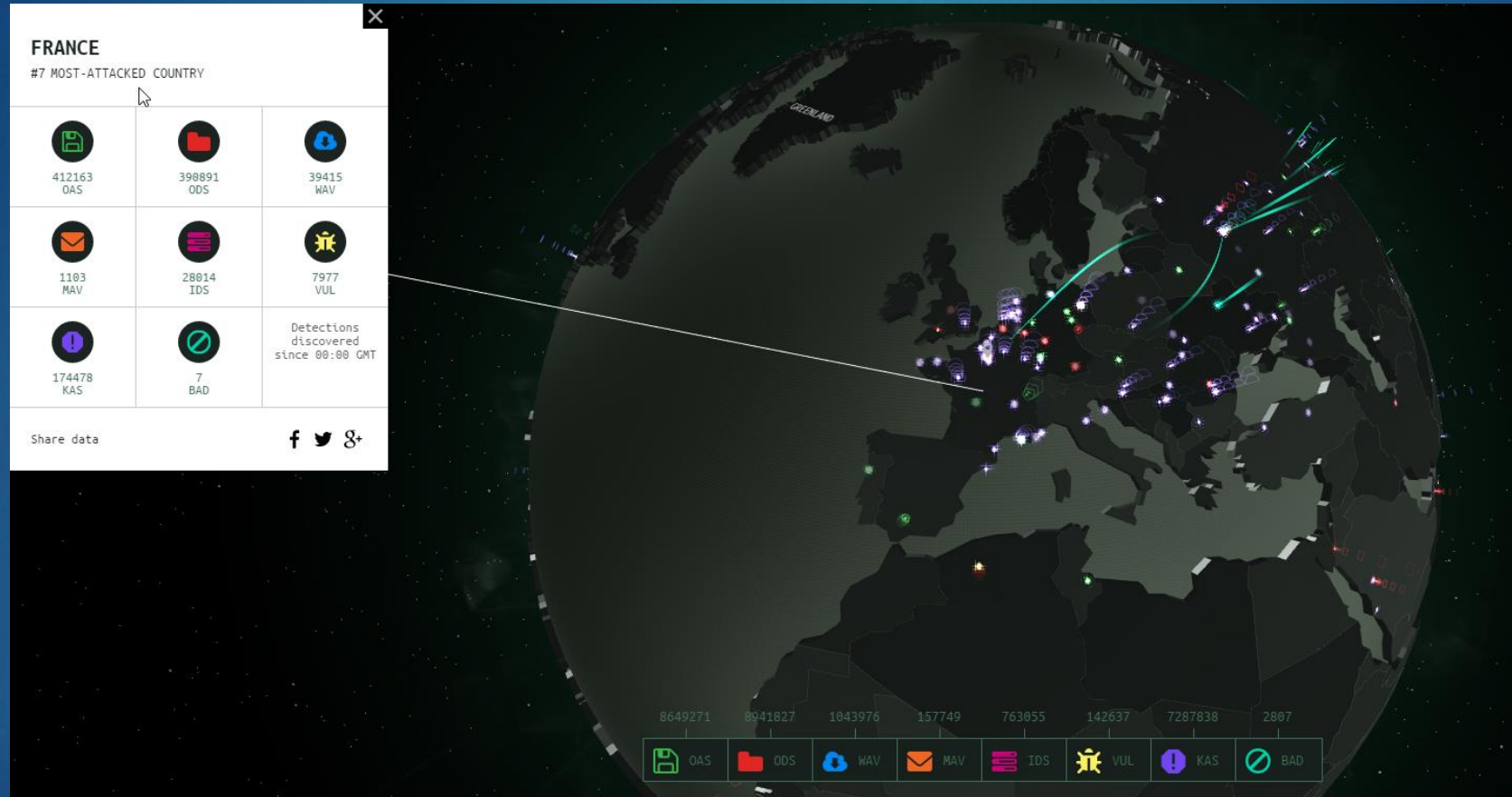
8





# Histoire

9



# Let me introduce you

10



# XSS

11

- ▶ cross-site scripting
- ▶ Redirection de l'utilisateur (hameçonnage)
- ▶ Vol d'informations, par exemple sessions et cookies.
- ▶ Actions sur le site faillible, à l'insu de la victime et sous son identité (envoi de messages, suppression de données...)
- ▶ Rendre la lecture d'une page difficile (boucle infinie d'alertes par exemple).

# Injection SQL

12

- ▶ Échapper les caractères
- ▶ Préparer les requêtes



# LFI

13

- ▶ Par URL
- ▶ Par upload

# CSP


14

Bloquer l'exécution de script depuis son site

# XFrame

15

## ► clickjacking



Click on the link to get rich now:  
[CLICK ME!](#)  
You'll be rich for the whole life!

# Htaccess / httpasswd

16

- ▶ *La maladie* du LIMIT



# Directory listing

17

- ▶ - Indexes
- ▶ Placer un fichier index dans chaque dossier

# Sitemap / robots.txt

18



Certains développeurs placent des URL sensibles dedans

# Limite du MD5 / SHA1

19

- ▶ John the ripper
- ▶ Salez vos passwords

# Vérifications

20

- ▶ Toujours faire une vérification côté serveur
- ▶ Masquer les erreurs de code
- ▶ Ne pas afficher les erreurs de connexion



# Configuration Apache

21

- ▶ Indexes
- ▶ Multiviews
- ▶ Préciser un dossier sans fichiers sensibles

# HTTPS

22

- ▶ Trafic (Wireshark)
- ▶ VOTRE VIE PRIVÉE !

# DNS Spoofing / Cache poisoning

23

- ▶ DNSSEC
- ▶ Cloudflare

# Web Application Firewall

24

- ▶ Naxsi (nginx)

- ▶ Cloudflare

- ▶ ...



# Social engineering

25

- ▶ PNL (programmation neuro linguistique)
- ▶ Phishing

# Pare-feu

26

- ▶ UFW
- ▶ Iptables

# Bruteforce

27

- ▶ Rainbow tables
- ▶ Fail2Ban
- ▶ Simplicité des passwords

# Accès physique

28

- ▶ Script « pain aux chocolat »
- ▶ Lockpicking
- ▶ Vol de matériel
- ▶ Rubber ducky



À vous de jouer !