# Veille Cyber Attaques Back-End

KATZ Sarah
JAWORSKI Cédric
SAURO Mathéo

Back

Next

# Table of contents



Back

Next

# 01
# Introduction

Back

Next

Back

Next

# 02 Injection SQL

Back

Next

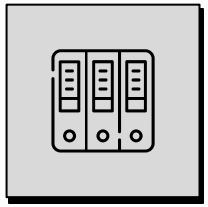
# Exemple Injection SQL

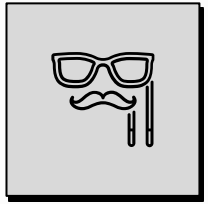
## Requete

*Ex:* SELECT user FROM users
WHERE user = [username] AND password = [mdp hashé];

## Mauvaise interpretation

*Avec username = [Admin'; --]...*
*[...]* WHERE user = 'Admin'; -- AND password = [n'importe quoi]





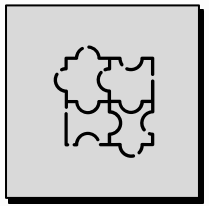
## Acces non-autorise

L'expression ignore le mot de passe, donnant accès au compte sans le connaître

Back

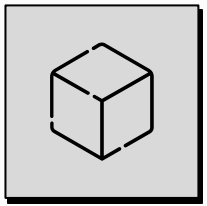
Next

# Contrer les injections SQL



## Requetes preparees

Les requêtes préparées ne sont pas affectées



## Utiliser un ORM

En général, les ORMs gèrent la sécurité et les requêtes

## Utiliser un Framework

Une solution bien plus complète et sécurisée qu'utiliser un ORM à part

Back

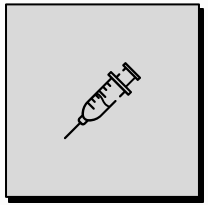
Next

# 03 Attaque XSS

Back

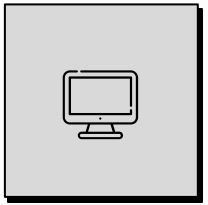
Next

# Attaque XSS



Injection

Inputs



Code

Back

Next

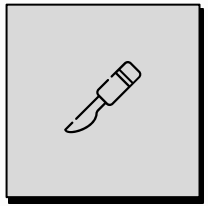
# Assainir un input

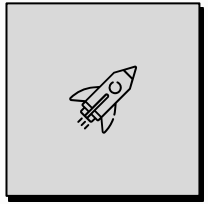
## Se mefier

de toute données en provenance d'un utilisateur, même dans nos propres champs

## Filtrer

les symboles et caractères réservés du langage de votre back-end





## Preferer

L'utilisation d'un framework, ceux-ci gèrent souvent  par eux même la protection xss

Back

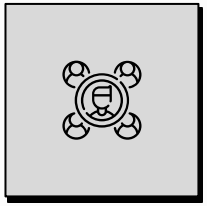
Next

# 04 Attaque CSRF

Back

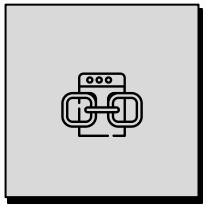
Next

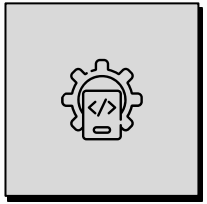
# Attaque CSRF



Ingénierie Sociale

Faux Lien



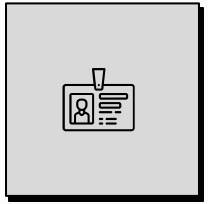


Modification
De données

Back

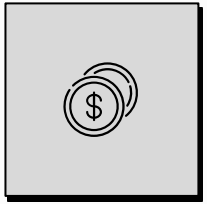
Next

# Se proteger



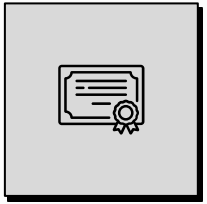
## Indicateur SameSite

Restreindre l'envoi de cookies dans les requêtes inter-sites



## Token CSRF

Ajouter un jeton unique à chaque requête de formulaire ou API



## Cookie JWT

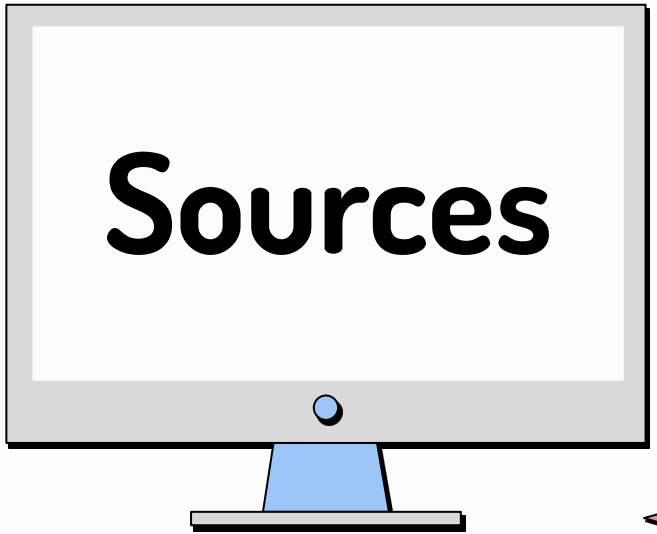
Stocker des informations d'authentification côté client

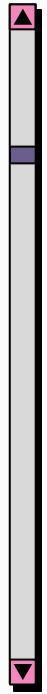
Back

Next

# Sources


- https://cyber.gouv.fr/
- https://cyber.gouv.fr/publications/securiser-un-site-web
- https://owasp.org/



Back

Next

# Merci !

Vous avez des questions?
onestpaslà@cestnoel.com
+01 23 456 789
essayeEncore.com

Back

Next