

# T6 - PROJET LIBRE

SOLUTION SAAS DE DÉTECTION ET D'ANALYSE  
DE VULNÉRABILITÉ POUR APPLICATION WEB

JULES BOZOUKLIAN

[**EPITECH.**]  
LE FUTUR DE L'INFORMATIQUE  
LE MEILLEUR DE L'INNOVATION



**43%**

*des cyberattaques visent les petites entreprises*

*source : [ansii](#)*



**60%**

*des entreprises touchées par des cyberattaques déposent leur bilan*

*source : [ipi-ecoles.com](#)*

L'objectif du projet est de fournir une solution SaaS de détection et d'analyse de vulnérabilité dans les applications web.

Les PME étant les entreprises les plus visés par des cyber attaques en France, l'objectif du projet est de fournir une solution simple d'utilisation et à la fois extrêmement efficace.

Le projet est destiné à être utilisé par des développeurs qui n'ont pas les connaissances nécessaires en matière de sécurité afin de faire face aux cyber attaques qui visent leurs applications.

Le choix d'une solution SaaS nous permettra de fournir une solution clé en main pour les clients.

La solution se présentera sous la forme d'un tableau de bord permettant de lancer des audits de type "black-box", c'est-à-dire sans aucune information sur la cible. Une fois l'audit terminé un rapport sera généré.

Un accès à une page de veille sécuritaire et un système d'alerte paramétrable sera aussi disponible.



**Node**

**Go**

**Web**

**React**

**UI / UX**

**PDCA**

**Détection**

**Cybersécurité**

**Exploitation**

**Veille**

**Alerte**

**ANSII**

**OWASP**

**Cloud**

**Docker**

**SaaS**

# PLANING

Début : 08 juin 2020

Fin: 26 juillet 2020

14 jours de projet (7 semaines)

Kick-off: 11 juin 2020

Groupe: 4 personnes

4 \* 14 = 56 jours / hommes

## MAJEUR

Gestion du projet / Equipe : Amel (12 jours)

Architecture du projet : Equipe (1 jour)

Dashboard (Front End) : Greg + Jules (1,5 jour)

Gestion Utilisateur (Back End) : Greg + Jules (1,5 jour)

Detection Vulnérabilité (Back End) : Jules (5 jours)

Analyse /vulnérabilité (Back End) : Jules + Greg (5 jours)

Veille / Alerte ANSII (Back End) : Greg (5 jours)

Analyse solution cloud : Maxime (1 jours)

Déploiement cloud : Maxime (12 jours)

Site vitrine : Amel (2 jours)

## MINEUR

Design (Logo, ...)

Mise en place outils (Gitlab / CI - CD / Sonar / ...)

Finition

Code review

Préparation KeyNote

Sprint 1

Sprint 2

Sprint 3



# FONCTIONNALITES

## Détection:

Langages  
CMS  
Framework  
OS  
Serveur  
Web application firewall (WAF)  
OSINT

## Audit:

Apache status  
Php info  
Robot txt  
CORS  
XST  
Open redirect  
Configurations

## Rapport:

Détail et recommandation

## Veille:

Flux ANSSI (CERT Fr)  
Alerte

## Attaques:

Injection SQL  
XSS  
Local File Inclusion  
Injection de commande  
Injection HTML  
Injection PHP  
Injection côté serveur  
Injection XPATH  
Injection LDAP  
XML External Entity

## Bruteforce:

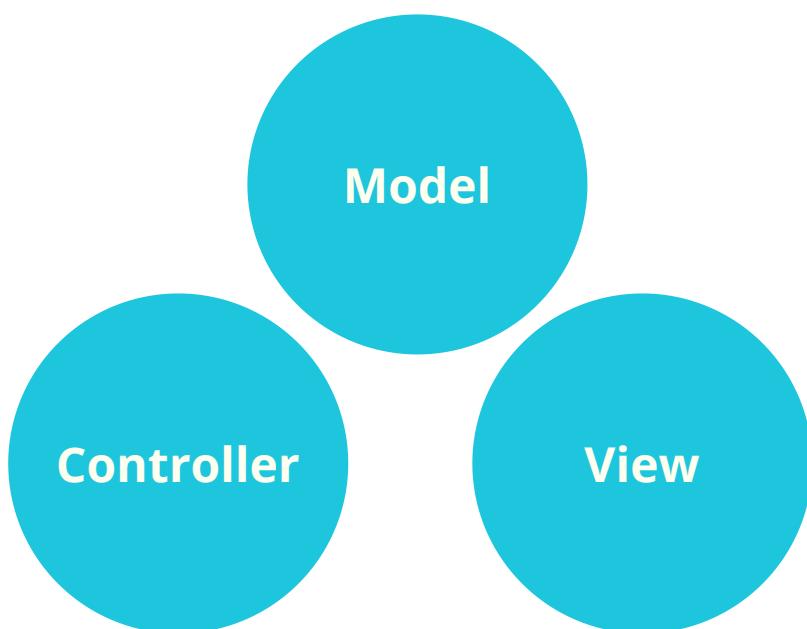
Panel administrateur  
Backdoor commun  
Dossier de backup  
Fichier de backup  
Répertoire commun  
Fichier commun  
Paramètre caché

## Informations sensible:

IP privé  
Erreurs  
Emails



# ARCHITECTURES



# ROUE DE DEMING



# OUTILS & TECHNOLOGIES

## Outils d'organisation et gestion de projet :

Teams  
Trello  
Gantt

## Technologies:

ReactJs pour le front-end  
NodeJs / Go pour le back-end  
Mongodb  
Jest pour tests unitaires  
CI / CD gitlab  
Docker



**250**

un des objectifs du projet et  
d'avoir au minimum 250 tests  
de sécurité différents

**100 %**

de détection des potentiels  
failles de sécurité

**7**

semaines de projet