



Mon appli est secure !
Enfin je crois ...

Jean-Louis Boudart

Nicolas Poirier

Au début

- Un “super” projet avec comme objectif de gérer des millions d'utilisateurs en concurrence.
- Vous avez les mains libres pour le choix des technos “Hipster”
- Vos managers vous demandent de développer une application web remplie de “Whaoouuu Feature”
- “Cela va révolutionner l'entreprise on compte sur vous !!”

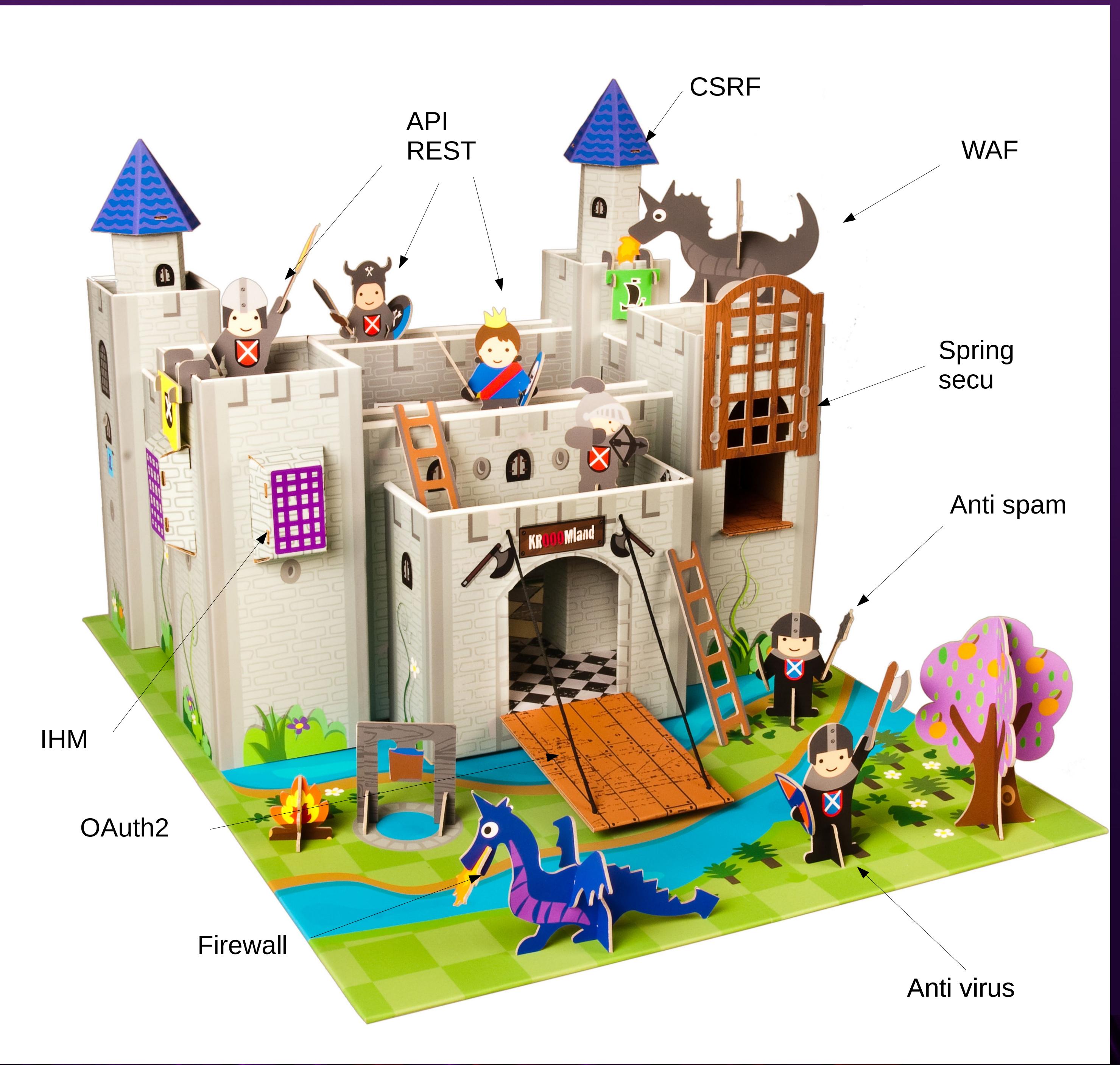
... ensuite on vous a montré une maquette



Et après de long mois ...

- L'application part enfin en production

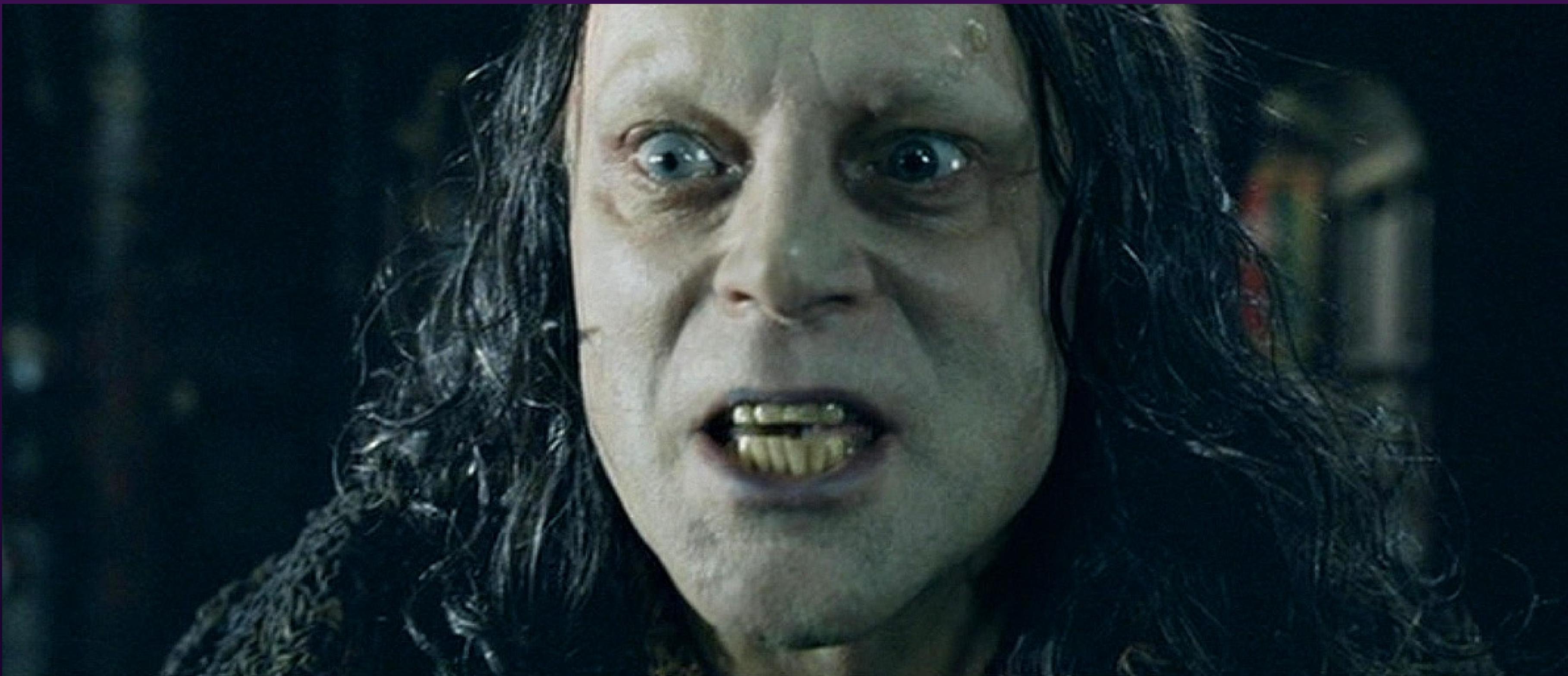




La sécurité est venue ...



et le pen testeur arriva ...



Les problèmes commencent ...

- Le pentesteur va rusher votre application



Avec tout ça on imagine ...



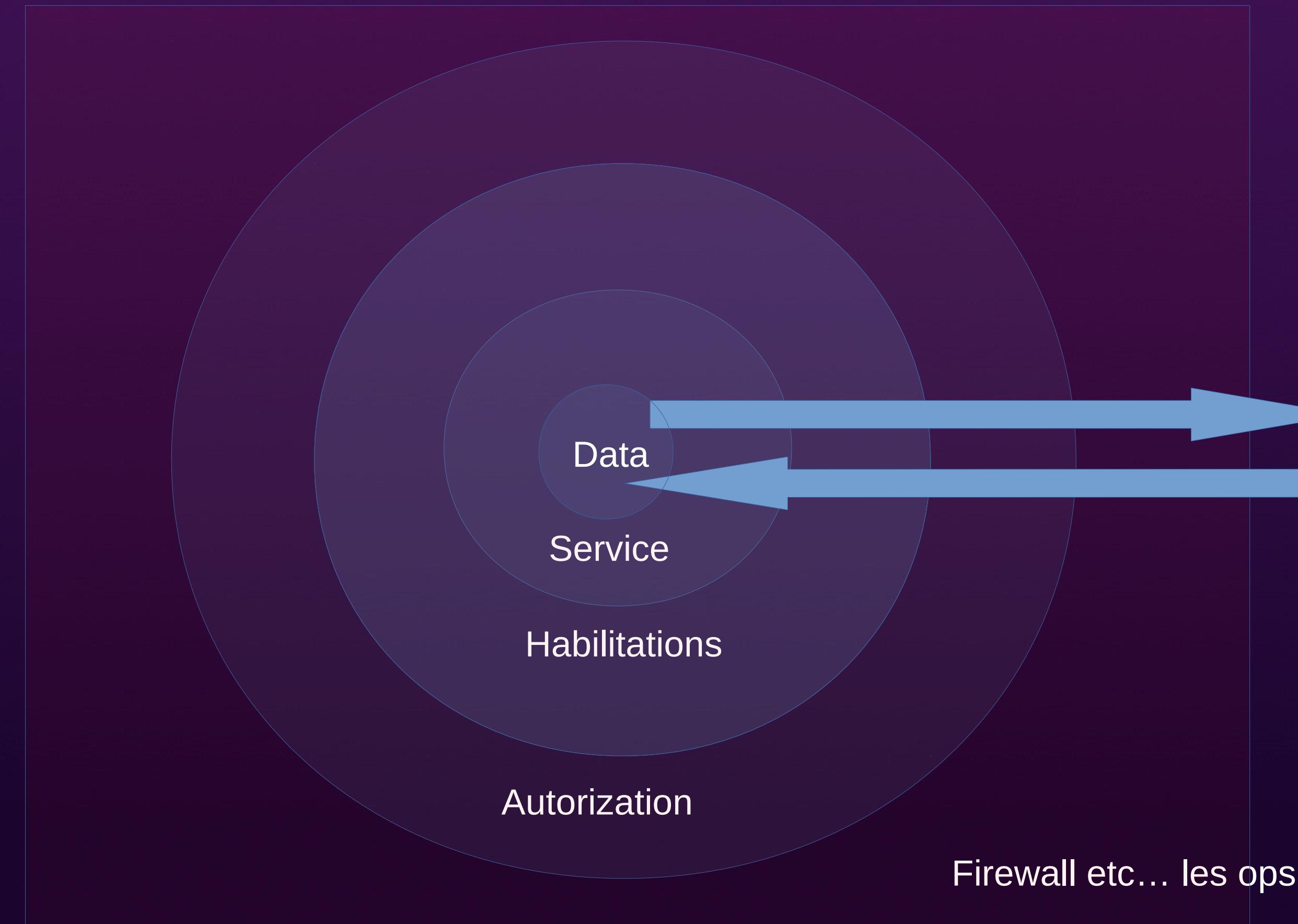
Le conseil: It's just a bug



Mais comment ca marche une application ?



Comment protéger les ressources ?



Solutions

- Lire tous les livres de l'OWASP
- Lire toutes les publications qui parlent de sécurité
- Comprendre toutes les normes et protocoles
- Etc....



Plus simple

Contrôler et Valider !

Let's try !

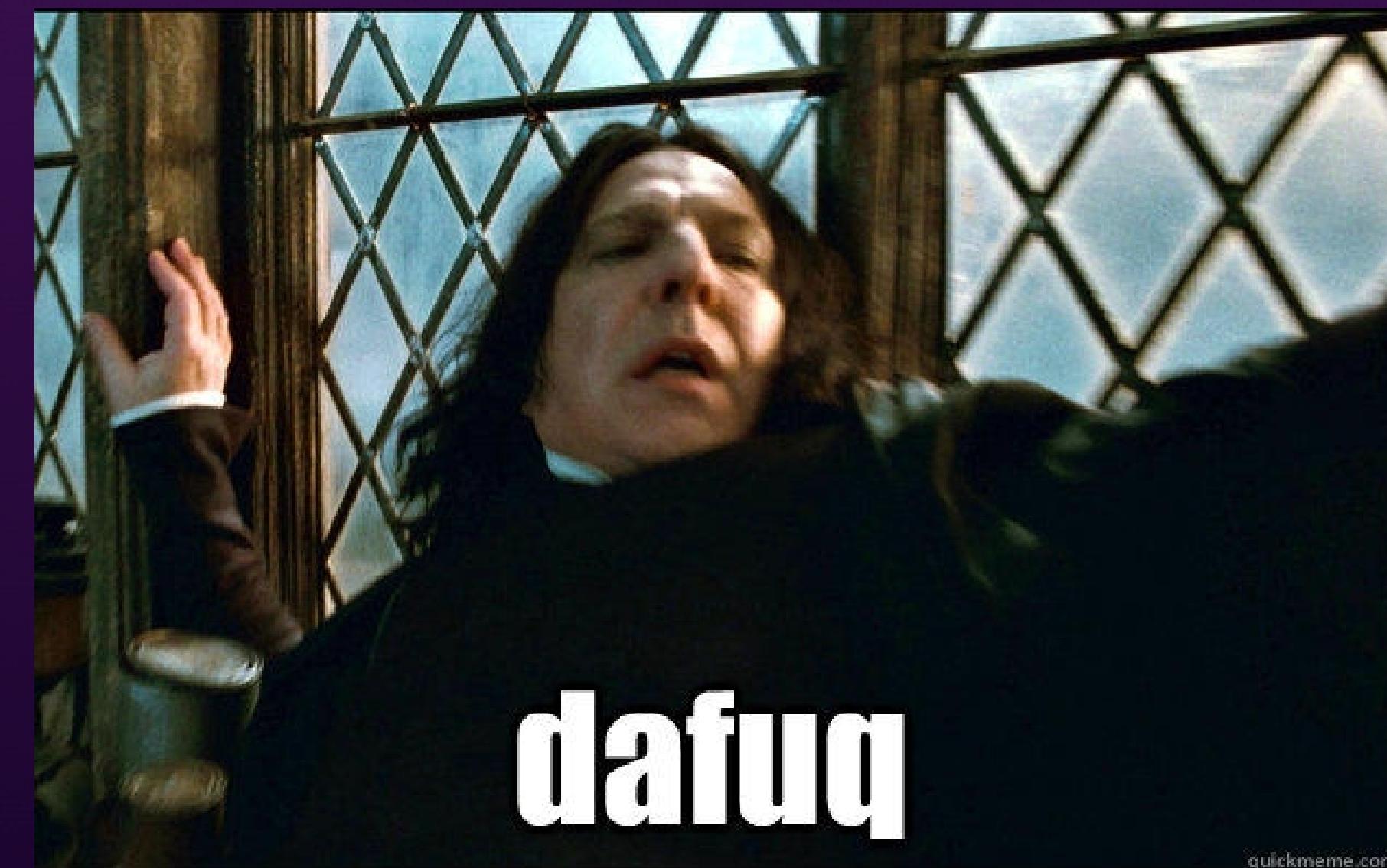
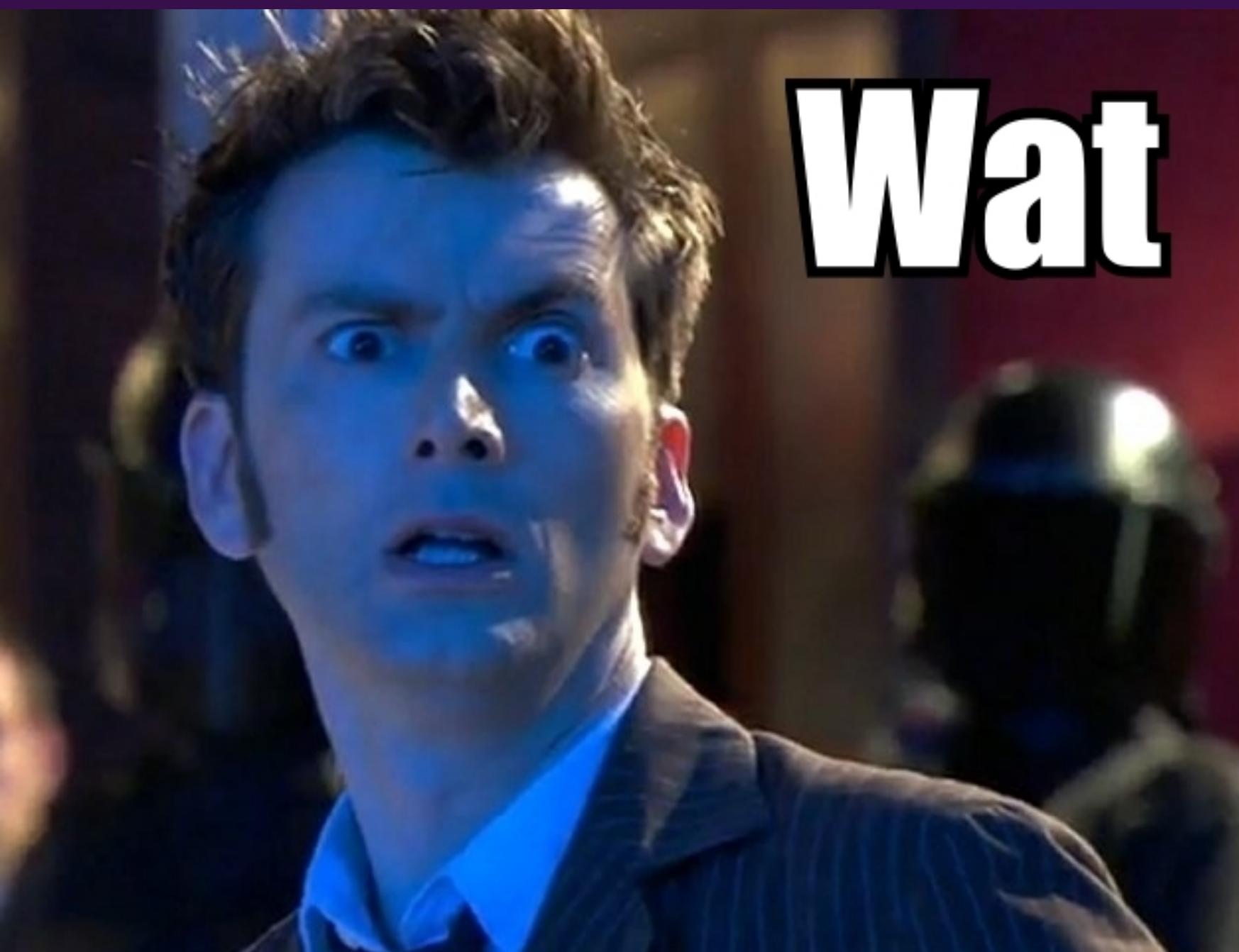
- “Est-ce que mon application est secure ?”
- Du code !!!

Highway to urHell !

- Petit agent qui va détecter vos points d'entrée !
- Back to code



Réaction ?



Highway To urHell

- Projet Open Source

https://www.owasp.org/index.php/OWASP_H2H_Tool_Project

- Objectif non avoué est de lister 100 % des ressources

- Java : Spring, JSF, JEE, JAX-RS, JMS, Struts ...
 - NodeJS : Express 3&4, sailsjs, strongloop en cours...

- Source Issues Feedbacks

<https://github.com/highway-to-urhell/highway-to-urhell>

Conclusion

- Pour nous faire de la sécurité applicative c'est :

Lister les ressources
Contrôler les actions
Valider les données

Questions ?