

Sécurité Web et audit

Pierre-Marie JUNGES, Florent NOSARI

Université de Lorraine

7 décembre 2017

- Audit de Sécurité
- +
- Sécurité Web
- =
- Audit de sécurité d'une application web

1 Initier l'audit

- Termes et définitions
- Principes à respecter
- Mise en place

2 Execution de l'audit

- Différentes pratiques
- Tests d'intrusion

- Vue à un instant T de la sécurité d'un système
- Pratique encadré légalement (accord avec l'audité)
- Comparaison à un référentiel (loi, politique interne, références)
- Action ponctuelle

Principes à respecter

- Intégrité
- Précision
- Professionnalisme
- Confidentialité
- Impartialité
- Approche factuelle

Contact avec l'audité (réunion) :

- Objectif
- Porté
- Méthodes (boite blanche/grise/noire)
- Composition de l'équipe
- Demandes techniques et administratives
- Définition des échéances
- Confirmation légale

Contact avec l'audité (réunion) :

- Objectif **Garantir une application sans failles de l'OWASP Top 10**
- Porté **Application web**
- Méthodes **Boite blanche**
- Composition de l'équipe
- Demandes techniques et administratives **code source**
- Définition des échéances **7 décembre 2017**
- Confirmation légale

Différentes pratiques existent :

- Audit organisationnel
- Tests d'intrusion (fuzzing)
- Revue de code source
- Relevés de configuration
- Analyse d'architecture

Différentes pratiques existent :

- Audit organisationnel
- Tests d'intrusion (fuzzing)
- Revue de code source
- Relevés de configuration
- Analyse d'architecture



FIGURE 1 – Metasploit



FIGURE 2 – OWASP Zap