

Audit et sécurité web

Pierre-Marie JUNGES, Florent NOSARI

Université de Lorraine

10 décembre 2017

- Sécuriser une application web → enjeu important
- Application indéfiniment invulnérable → impossible
- Vérifier régulièrement le niveau de sécurité → audit

→ Audit de sécurité d'une application web

- 1 Initier l'audit
 - Mise en place
 - Activités d'audit
- 2 Execution de l'audit
 - Outils utilisés
- 3 Conclure un audit
 - Elaboration du rapport d'audit
 - Conclusion à l'audit

Audit de sécurité

- Vue à un instant T de la sécurité d'un système
- Pratique encadré (lois, réglementations, normes ISO 19011/27001)
- Objectif d'identifier et d'évaluer de potentiels vulnérabilités
- Établir des recommandations, corrections

Auditeur

Personne participante à la réalisation d'un audit

Audité

Commanditaire de l'audit

Contact audité-auditeur :

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

Contact audité-auditeur :

- Objectif
→ vérifier des vulnérabilités de l'OWASP TOP 10
- Porté
→ application web (en local)
- Méthodes (boite blanche/grise/noire)
→ boite blanche
- Demandes techniques et administratives
→ code source
- Définition des échéances
→ 10 décembre 2017
- Composition de l'équipe
- Confirmation légale

OWASP ?

OWASP

- Organisation internationale
- Spécialisée en sécurité des applications Web
- Fournie des informations sur des failles de sécurité

Top 10 → 80-90% des attaques/menaces (2017)

Vulnérabilités à vérifier

- ① Injection
- ② Violation de gestion d'authentification et de session
- ③ Cross-Site Scripting (XSS)

Suivant les objectifs définis, on choisit une/des méthode(s) d'audit

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

”Audit applicatif” recommandé par l’ANSSI :

- Revue de code source
- Relevés de configuration
- Tests d'intrusion (fuzzing)

L’ANSSI recommande de ne jamais faire uniquement les tests d'intrusion



Metasploit



OWASP Zap



Logique humaine

Audit terminé \Rightarrow échéance terminée ou activités prévues réalisées

Rapport d'audit, rédigé par l'auditeur

- Compréhensible par des non experts
- La liste des vulnérabilités trouvées
- La liste des mesures correctives proposées
- Déroulement des tests d'intrusion et méthodologie employés
- Mention des imprévues

Comment lister les vulnérabilités ?

Conclusion à l'audit

- Réunion audité-auditeur
- Audité → certifier l'état de sécurité de son système
- Auditeur → restituer ou détruire les traces de l'audit
- Audit de validation ?

Audit de sécurité d'une application :

- Nécessite du temps
- Sécurité → période de temps limitée
- Audité → bien choisir l'auditeur

Bientôt remplacé par du Bug bounty ?

Références