Audit et sécurité web

Pierre-Marie JUNGES, Florent NOSARI

Université de Lorraine

9 décembre 2017

Introduction

- Sécuriser une application web \rightarrow enjeu important
- Application indéfiniment invulnérable \rightarrow impossible
- ullet Vérifier régulièrement le niveau de sécurité o audit
 - \rightarrow Audit de sécurité d'une application web

Plan

- 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

Termes et definitions

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 recommendations, corrections

Auditeur

Personne participante à la réalisation d'un audit

Audité

Commanditaire de l'audit

Mise en place

Contact audité-auditeur :

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

Mise en place

Contact audité-auditeur :

- Objectif
 - → vérifier des vulnérabilités de l'OWASP TOP 10
- Porté
 - \rightarrow application web (en local)
- Méthodes (boite blanche/grise/noire)
 - \rightarrow boite blanche
- Demandes techniques et administratives
 - \rightarrow code source
- Définition des échéances
 - \rightarrow 9 décembre 2017
- Composition de l'équipe
- Confirmation légale

OWASP?

OWASP

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

Top $10 \rightarrow 80-90\%$ des attaques/menaces (2017)

Vulnérabilités à vérifier

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

Activités d'audit

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

Méthodes d'audit choisies

"Audit applicatif" recommandé par l'ANSSI :

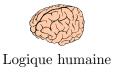
- Revue de code source
- Relevés de configuration
- Tests d'intrusion (fuzzing)

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

Outils utilisés







Elaboration du rapport d'audit

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
- ullet Auditeur o restituer ou detruire les traces de l'audit
- Audit de validation?

Conclusion

Audit de sécurité d'une application :

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

Bientot remplacé par du Bug bounty?

Références