Audit et sécurité web

Pierre-Marie JUNGES, Florent NOSARI

Université de Lorraine

10 décembre 2017

Introduction

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

→ Audit de sécurité d'une application web

Plan

1. Initier l'audit
   - Mise en place
   - Activités d'audit
2. Execution de l'audit
   - Outils utilisés
   - Tests d'intrusion
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
  → 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)
4. Violation de contrôle d'accès

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

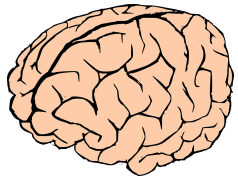
"Audit applicatif" recommandé par l'ANSSI :

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

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

Outils utilisés

w3af

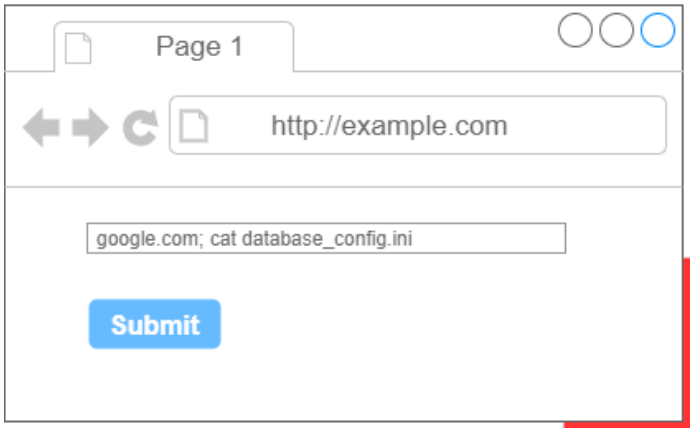


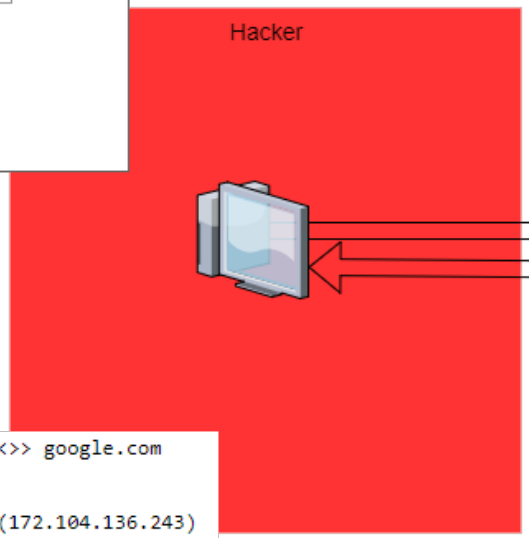
Logique humaine

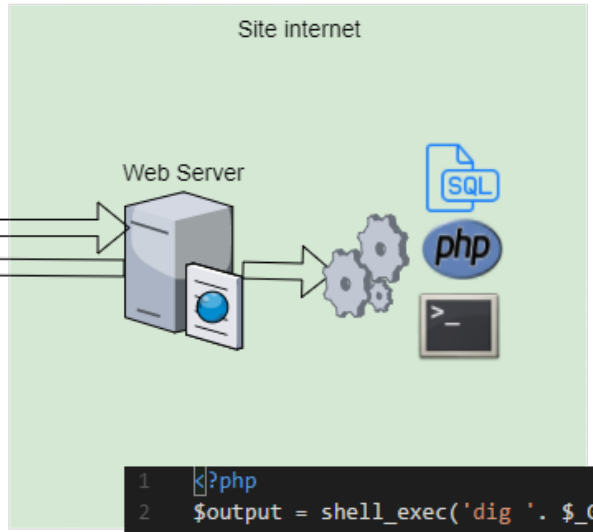
OWASP Zap

Injection (OS)

1. Injection du code








```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com
...
;; Query time: 27 msec
;; SERVER: 172.104.136.243#53(172.104.136.243)
;; WHEN: Sat Nov 11 18:42:09 STD 2017
;; MSG SIZE  rcvd: 191

db_user = admin
db_password = admin
db_host = db-host.com
db_port = 3306
```

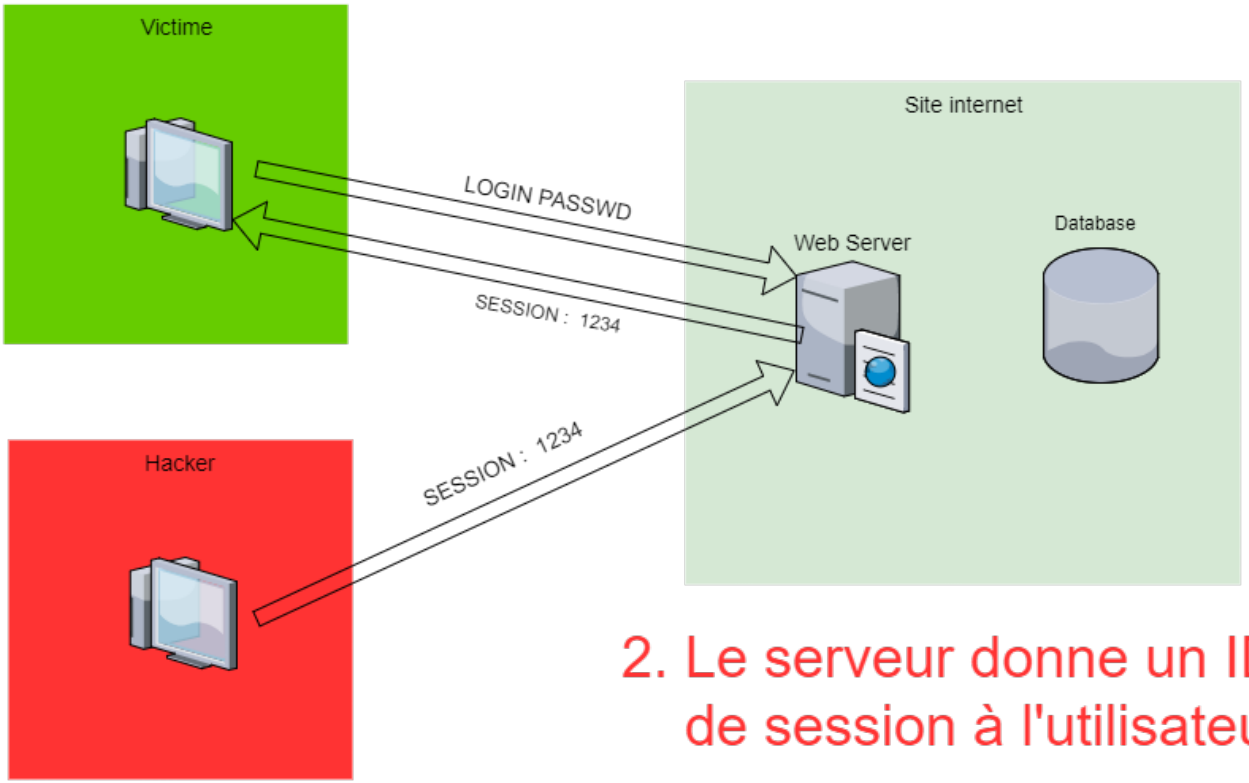
```
1  <?php
2  $output = shell_exec('dig '. $_GET['host'
3  echo "<pre>$output</pre>";
4  ?>
```

2. Execution du code

3. Affichage du résultat

Violation de gestion d'authentification et de session

1. La victime se connecte



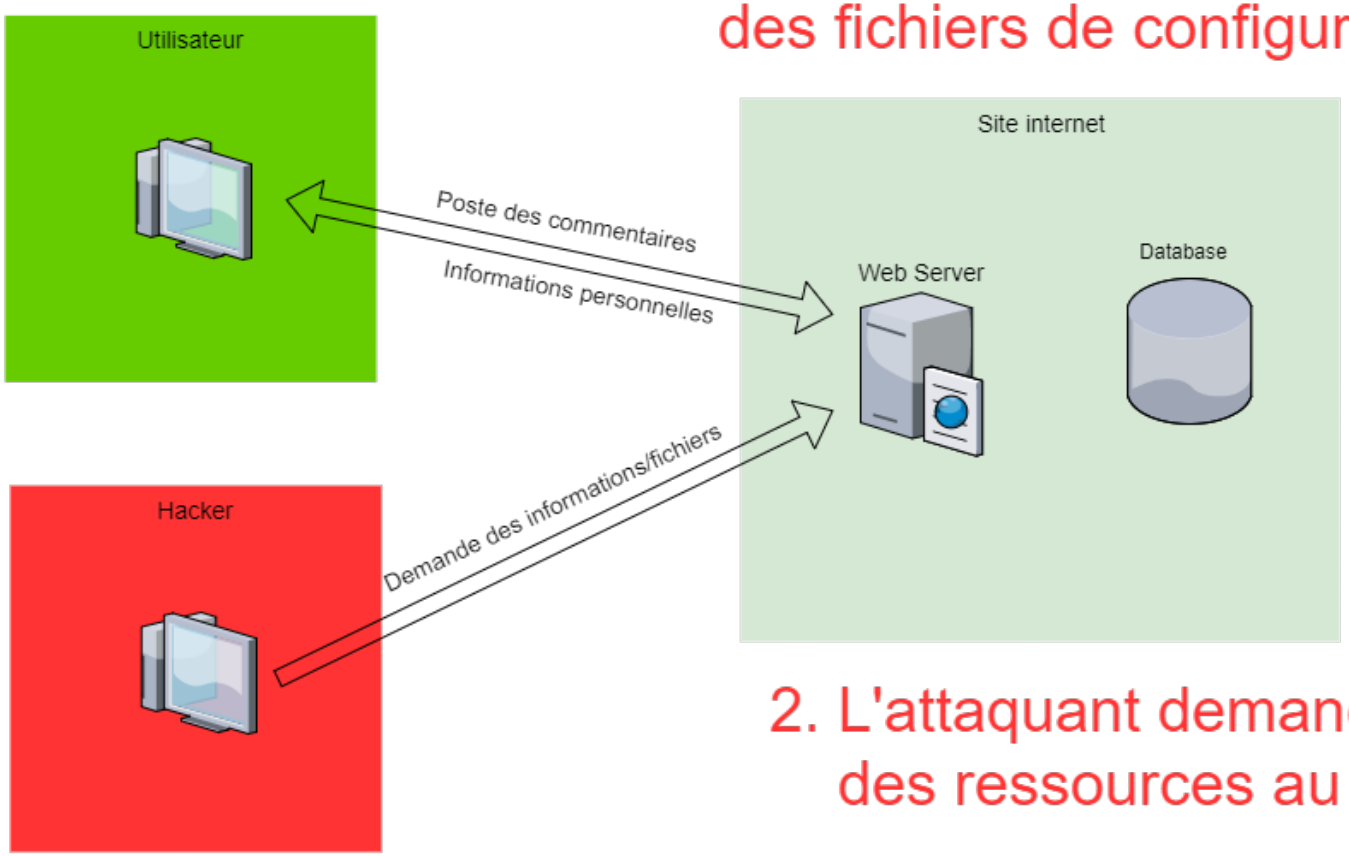
2. Le serveur donne un ID de session à l'utilisateur

3. L'attaquant récupère le numéro de session de la victime et se fait passer pour elle

Violation de contrôle d'accès

1.a Un utilisateur
met du contenu

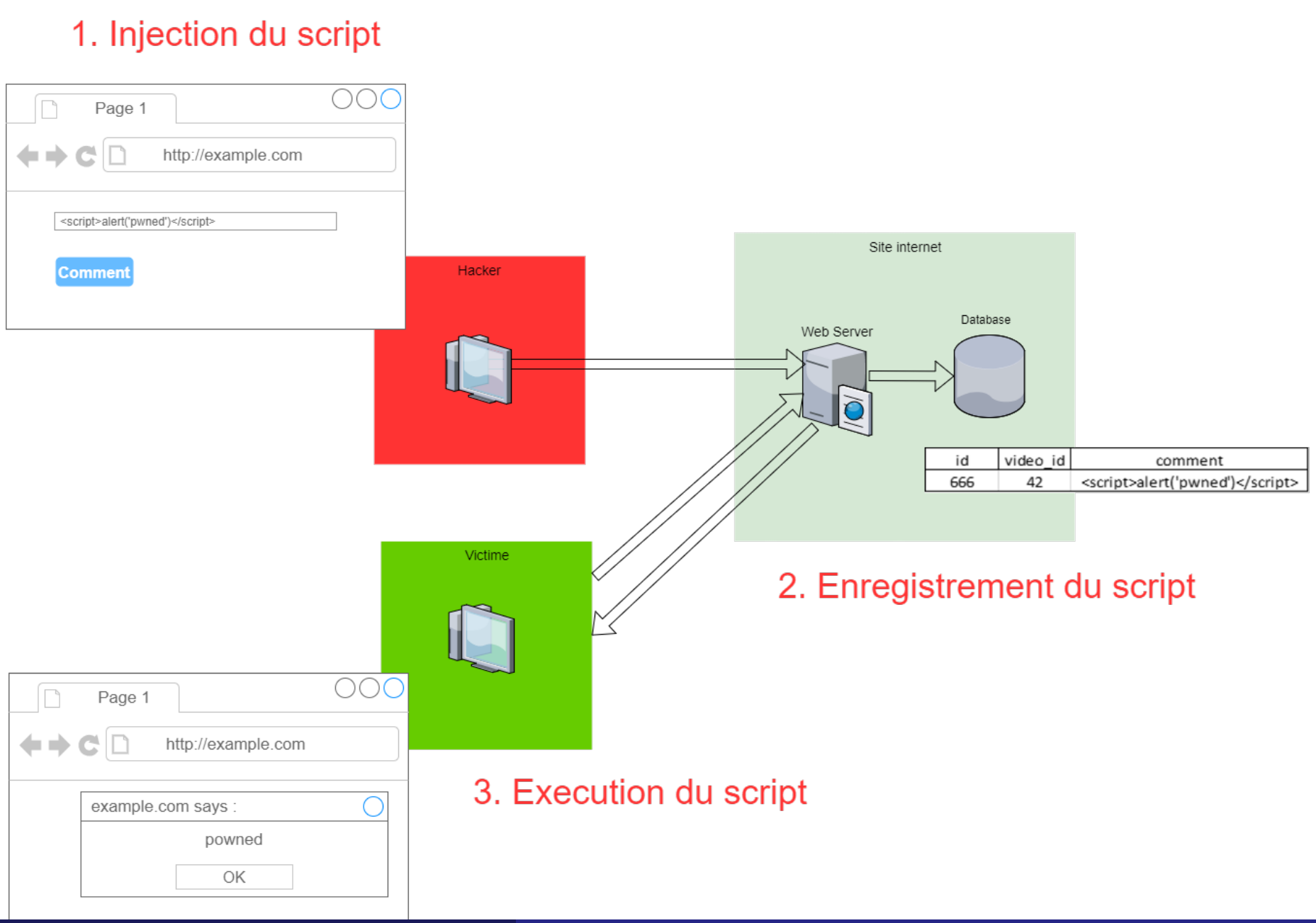
1.b Le développeur créé
des fichiers de configuration



2. L'attaquant demande
des ressources au serveur

3. Le serveur ne vérifie pas les droits
et donne les ressources à l'attaquant

Cross-Site Scripting (XSS)



Elaboration du rapport d'audit

Audit terminé ⇒ 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 detruire les traces de l'audit
- Audit de validation ?

Conclusion

Audit de sécurité d'une application :

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

Bientot remplacé par du Bug bounty ?

Références

Images :
pixabay.com/en/brain-human-brain-knowledge-anatomy-155190/
scanforsecurity.com/wp-content/uploads/2016/11/w3af_scanner.png