

Audit et sécurité web

Pierre-Marie JUNGES, Florent NOSARI

Université de Lorraine

11 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
- Tests d'intrusion

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 DVWA (en local)
- Méthodes (boite blanche/grise/noire)
→ boite blanche
- Demandes techniques et administratives
→ code source
- Définition des échéances
→ 11 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
- 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

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



w3af



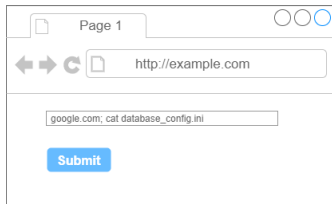
Raisonnement
humaine



OWASP Zap

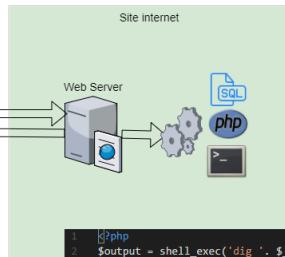
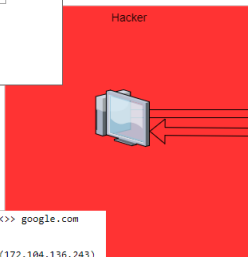
Injection (OS)

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
```



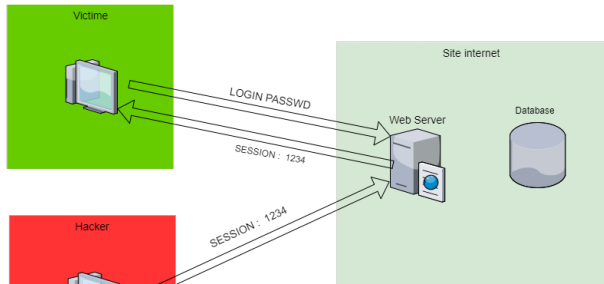
2. Execution du code

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

3. Affichage du résultat

Violation de gestion d'authentification et de session

1. La victime se connecte

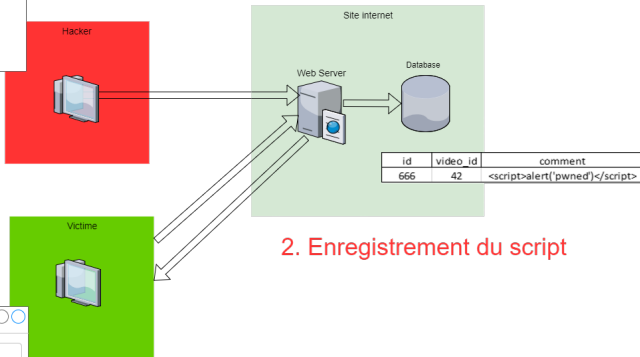
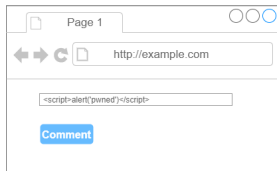


2. Le serveur donne un ID de session à l'utilisateur

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

Cross-Site Scripting (XSS)

1. Injection du script



2. Enregistrement du script

3. Execution du script





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 ?

- 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 ?

Images :

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