Distribution trouée DVWA

Florian Barbarin, Abdelkader Beldjilali, Alexis Letombe

2 mai 2017

Introduction

Sécurité des applications web

- Technologies web de plus en plus présentes, à la fois dans la vie privée et au sein des entreprises
- Nombreux avantages : efficacité, centralisation des données, accès facilité à l'information, etc...
- Un grand nombre de menaces pèsent sur ces applications (cf. OWASP) : atteinte à la disponibilité, l'intégrité et/ou la confidentialité

Présentation de l'application DVWA

- Application web écrite en PHP/HTML
- Permet la formation à la sécurité des applications web
- 10 thèmes abordés

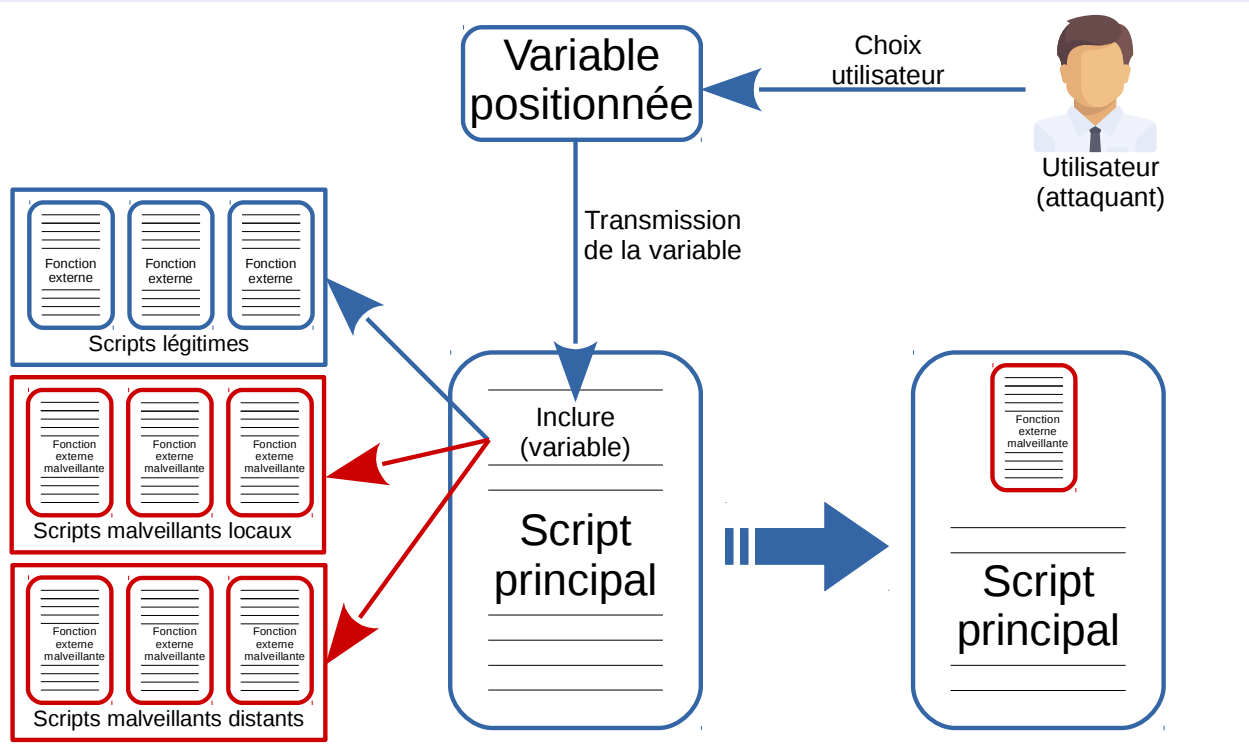
Brute Force

Command Injection

CSRF

File Inclusion

Présentation de la vulnérabilité



Caractéristiques de la vulnérabilité

- Moyen d'exécuter du code
- Code local ou code distant
- Souplesse *vs* sécurité

File Upload

Présentation de la vulnérabilité

- Fonctionnalité très répandue dans les applications web (*cloud*, *mail*)
- Permet chargement sur le serveur de fichiers locaux
- Type de fichier doit être conforme à ce qu'attend l'application : contrôles nécessaires

Caractéristiques de la vulnérabilité

- Moyen de charger sur le serveur du code malicieux
- Possibilité d'écraser/modifier des fichiers déjà présents sur le serveur (défacement)
- Mauvaise implémentation du contrôle des fichiers : ouverture du serveur à **tout** type d'attaques (scripts avec commandes systèmes, etc...)

Insecure CAPTCHA

Présentation de la vulnérabilité

- CAPTCHA : *Completely Automated Public Turing test to tell Computers and Human Apart*
- Permet de décider si une action est réalisée, ou non, par un humain
- Éviter automatisation de certaines tâches : nécessite non-contournement du contrôle

Caractéristiques de la vulnérabilité

Vulnérabilités courantes :

- Transmission de la solution (via URL, nom image, champ HTML caché, etc...)
- Mauvaise vérification de la réussite au test : contournement possible du contrôle
- Résolution automatique du test : contrôle doit être suffisamment difficile

Injection SQL

Injection SQL aveugle

Attaques Reflected XSS (non persistante

Stored XSS (persistante)

Conclusion

Sécurité des applications web

- Seulement quelques vulnérabilités présentées
- Nombreuses autres vulnérabilités existent
- Sensibilité des informations échangées dans les applications web : nécessaire sécurisation

Principes généraux de la sécurité des applications web

- Bon filtrage des saisies utilisateurs
- Bonne configuration du serveur web