

Distribution trouée DVWA

Florian Barbarin, Abdelkader Beldjilali, Alexis Letombe

3 mai 2017



1 Introduction

2 Présentation de vulnérabilités

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- Injection SQL et Blind Injection SQL
- Résultat de l'injection
- Attaques XSS : Cross Site Scripting
- Attaques Reflected XSS (non persistante) - 1
- Attaques Reflected XSS (non persistante) - 2
- Attaques Stored XSS (persistante)

3 Conclusion

1 Introduction

2 Présentation de vulnérabilités

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- Injection SQL et Blind Injection SQL
- Résultat de l'injection
- Attaques XSS : Cross Site Scripting
- Attaques Reflected XSS (non persistante) - 1
- Attaques Reflected XSS (non persistante) - 2
- Attaques Stored XSS (persistante)

3 Conclusion

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

1 Introduction

2 Présentation de vulnérabilités

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- Injection SQL et Blind Injection SQL
- Résultat de l'injection
- Attaques XSS : Cross Site Scripting
- Attaques Reflected XSS (non persistante) - 1
- Attaques Reflected XSS (non persistante) - 2
- Attaques Stored XSS (persistante)

3 Conclusion

Brute Force

Caractéristiques de la vulnérabilité

- Intervient lors de la connexion d'un utilisateur
- Permet la découverte du mot de passe d'un utilisateur
- Deux moyens de procéder : avec ou sans dictionnaire

Caractéristiques de la vulnérabilité

- Essais à la main (sans dictionnaire)
- Appartition des login / mot de passe dans l'URL
- Essai multiples pour un login donné (si le nombre de tentatives n'est pas limité)

Command Injection

Caractéristiques de la vulnérabilité

- Utilisation d'un champ prévu pour exécuter un *Ping* sur l'adresse entrée
- Exécuter des commandes dans un champ non prévu à cet effet
- Possibilité d'exécuter plusieurs commandes à la suite

Caractéristiques de la vulnérabilité

- On enchaîne les commandes séparées par des ';'
- Naviguer dans les répertoires du système
- Premier point d'entrée pour une opération de plus grande ampleur

CSRF

Présentation de la vulnérabilité

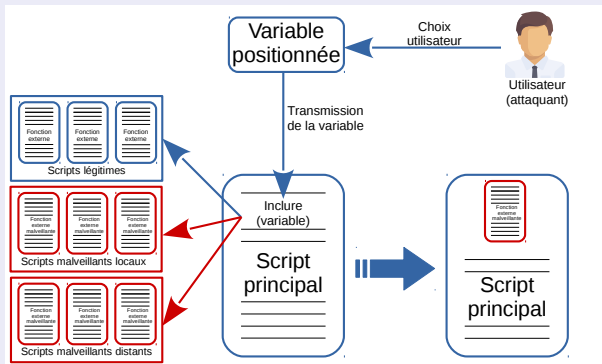
- CSRF : *Cross-Site Request Forgery*
- Permet de modifier le mot de passe de l'utilisateur
- Faire exécuter une action par un utilisateur à son insu

Caractéristiques de la vulnérabilité

- Aucune vérification de l'identité de la personne
- L'ingénierie sociale permet d'y arriver
- Un raccourcissement de l'URL qui permet l'exécution de l'action

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

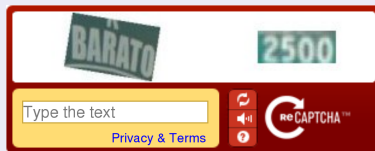
- Fonctionnalité très répandue dans les applications web (*cloud, mail*)
- Permet chargement sur le serveur de fichiers locaux
- Type de fichier doit être conforme à ce qu'attend l'application : contrôles nécessaires

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 automatiser 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 et Blind Injection SQL




Caractéristiques de la vulnérabilité

```
// Check database
$query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
```

Vulnérabilités courantes :

- DVWA-Low ne filtre pas les entrées utilisateurs,
- L'injection suivante ' **UNION select password, last_name from users#** permet de récupérer les mots de passe dans la base de données du site web.

Résultat de l'injection



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

ID: ' UNION select password, last_name from users#
First name: 5f4dcc3b5aa765d61d8327deb882cf99
Surname: admin

ID: ' UNION select password, last_name from users#
First name: e99a18c428cb38d5f260853678922e03
Surname: Brown

ID: ' UNION select password, last_name from users#
First name: 8d3533d75ae2c3966d7e0d4fcc69216b
Surname: Me

ID: ' UNION select password, last_name from users#
First name: 0d107d09f5bbe40cade3de5c71e9e9b7
Surname: Picasso

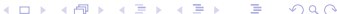
ID: ' UNION select password, last_name from users#
First name: 5f4dcc3b5aa765d61d8327deb882cf99
Surname: Smith

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavtuna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

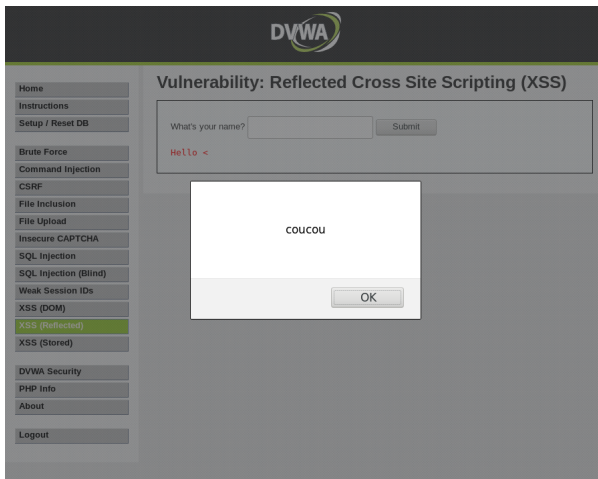


Florian Barbarin, Abdelkader Beldjilali, Alexis Letombe

Distribution trouée DVWA

3 mai 2017

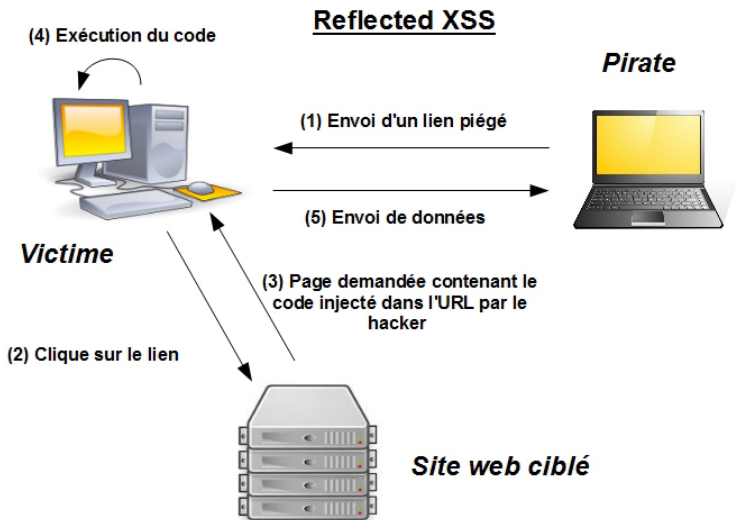
12 / 18



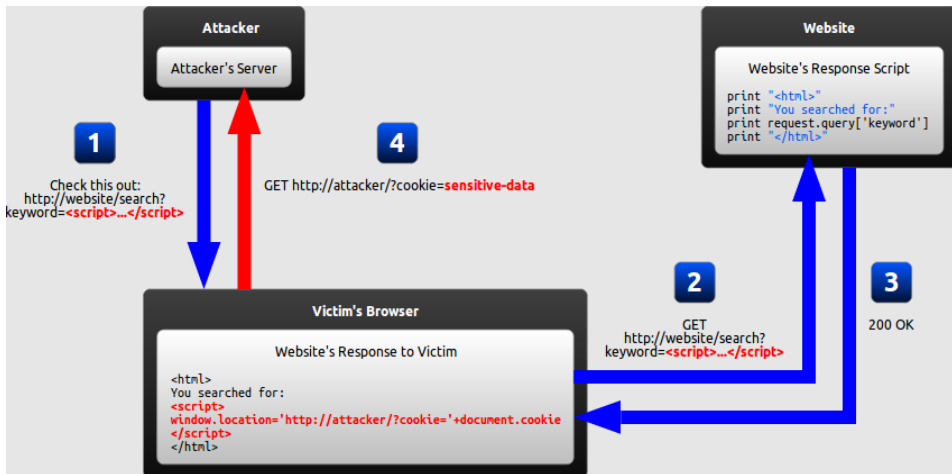
Test de vulnérabilité aux attaques XSS

```
<script>alert('coucou')</script>
```

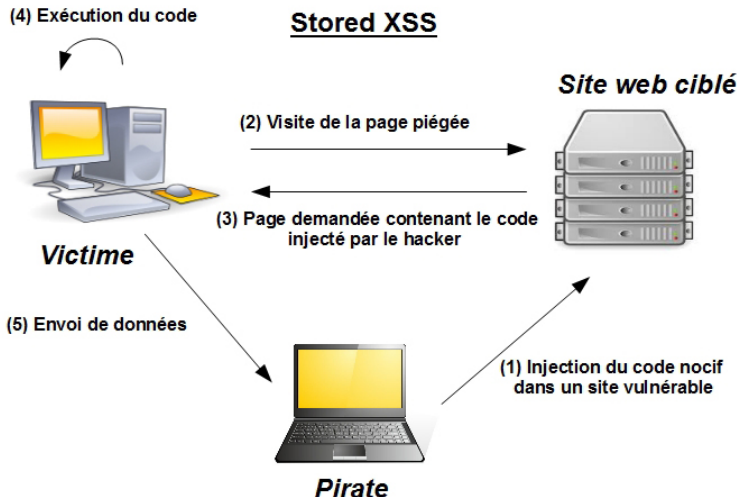
Attaques Reflected XSS (non persistante)



Attaques Reflected XSS (non persistante)



Attaques Stored XSS (persistante)



1 Introduction

2 Présentation de vulnérabilités

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- Injection SQL et Blind Injection SQL
- Résultat de l'injection
- Attaques XSS : Cross Site Scripting
- Attaques Reflected XSS (non persistante) - 1
- Attaques Reflected XSS (non persistante) - 2
- Attaques Stored XSS (persistante)

3 Conclusion

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