

TP sécurité - L3 - TP1

Le but de ce TP est de s'initier aux problèmes de sécurité dans le web. Pour cela, nous allons utiliser l'outil DVWA.

Une instance de l'outil est disponible à l'adresse suivante: <http://172.20.128.66/>

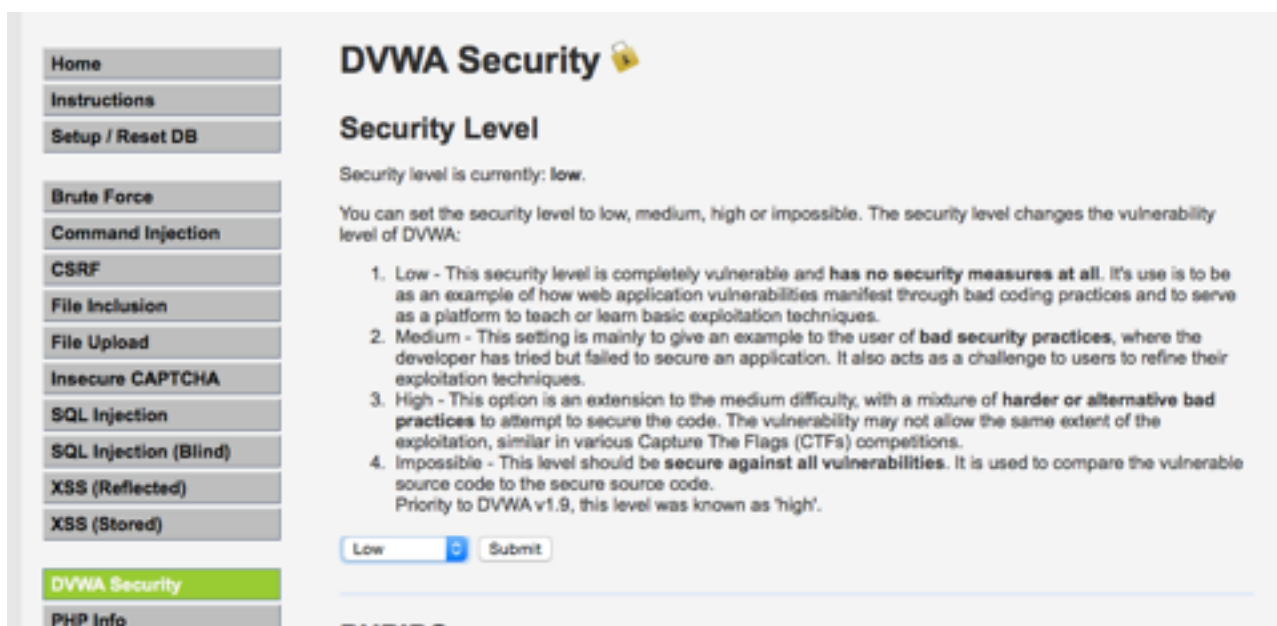
En dehors des séances de TP, le serveur DVWA sera désactivé, mais il est possible d'installer une version locale pour s'entraîner. Pour cela, suivre les indications sur le site officiel de l'application: <http://www.dvwa.co.uk>

Note: pensez à utiliser Firefox afin de vous connecter. Certains navigateurs tels que Chrome ou Safari bloqueront une partie des exercices.

Prise en main de l'outil.

Les identifiants de connexion sont admin/password.

Dans la page DVWA security, il est possible de régler le niveau de difficulté des différents exercices. Nous vous conseillons de faire chaque exercice les niveaux "low" puis "medium".



The screenshot shows the DVWA Security interface. On the left is a sidebar menu with links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), XSS (Reflected), XSS (Stored), DVWA Security (highlighted), and PHP Info. The main content area is titled 'DVWA Security' with a lock icon. Below the title is the 'Security Level' section. It states 'Security level is currently: low.' and explains that the security level can be set to low, medium, high, or impossible. A list of four levels is provided: 1. Low (completely vulnerable), 2. Medium (bad security practices), 3. High (extension to medium difficulty), and 4. Impossible (secure against all vulnerabilities). At the bottom, there is a dropdown menu currently set to 'Low' and a 'Submit' button.

Exercices

1 - Reflected XSS

A l'aide du formulaire fourni, nous allons exécuter du code Javascript qui sera exécuté sur la machine cliente après soumission du formulaire.

- affichez un message pop-up de type "alert" après soumission du formulaire
- affichez les cookies de l'utilisateur
- redirigez l'utilisateur sur Google

2 - Stored XSS

Les attaques de type stored XSS sont très proches des attaques de type Reflected XSS. Etant donné que vous travaillerez tous sur le même serveur, il est possible que vous ne puissiez accéder à la page de l'exercice.

Dans ce cas, rendez vous à cette page (<http://172.20.128.66/setup.php>) et faire un reset de la base de données.

Afin de ne pas gêner le travail de vos camarades, les exercices seront légèrement modifiés:

- modifiez le titre de la page afin qu'il affiche votre nom
- inserez le cookie de l'utilisateur dans le commentaire
- remplacez le logo de DVWA par celle-ci: <http://i.imgur.com/soPydKo.gif>
- remplacez le formulaire afin que, lors de la soumission, l'utilisateur ouvre google en cherchant son nom

3 - SQL injection

Cet exercice concerne les injections SQL. A l'aide du formulaire fourni, nous allons injecter des commandes SQL permettant d'extraire un certain nombre de données du système.

- la liste des utilisateurs du système
- trouver tous les utilisateurs dont le nom contient la lettre "A"
- la version de la base de données utilisée
- l'hôte sur lequel la base de données est hébergée

4 - Blind SQL injection

Dans les attaques de type blind, le résultat n'est pas affiché directement dans la page d'où l'injection est réalisée.

Votre but sera de trouver les mêmes informations que pour l'exercice précédent.

5 - Un peu de tout

Corsons un peu le jeu maintenant. Vous savez comment exécuter vos propres commandes SQL sur le serveur et récupérer les cookies des autres utilisateurs.

Créez une table "cookies_<votre nom>" dans la base de données et stockez-y les identifiants de sessions des utilisateurs NDWA. Utilisez la page d'injection SQL pour découvrir les