BRUTE FORCE

1. Description de la faille

Une tentative d’attaque de type brute force intervient, pour une application web, au niveau de l’interface login. Le but de cette attaque est de se connecter en essayant plusieurs combinaisons login / mot de passe jusqu’à arriver à une combinaison acceptée par le système. Il est à supposer ici qu’un nombre infini de tentative est possible.

L’attaque de type Force Brute peut se faire de deux manières différentes : avec ou sans dictionnaire.

Dans le cas d’une attaque sans dictionnaire, pour chaque login connu, il faut tenter toutes les combinaisons d’un ou plusieurs caractères alphanumériques jusqu’à correspondance avec le login choisi.

Pour une attaque avec dictionnaire, il faut créer un fichier contenant par exemple les mots de passe les plus souvent utilisés. Pour chaque login connu, chaque mot de passe contenu dans le fichier créé sera testé, en espérant qu’au moins un parmi la liste corresponde.

Une telle attaque peut être un premier point d’appui pour obtenir plus de privilèges sur l’application web. De plus, si une personne utilise souvent le même mot de passe, l’attaquant pourra le réutiliser sur d’autres applications comme les réseaux sociaux.

1. Exploitation de la faille

On se place dans l’onglet Brute Force. On retrouve un espace avec deux champs à remplir : le login (username) et le mot de passe (password) associé. Il est possible de tenter de se loger en essayant plusieurs combinaisons parmi les plus courantes telles que : « root, root », « admin, admin », « administrateur, password » … On trouvera assez rapidement une combinaison login / mot de passe qui convient.

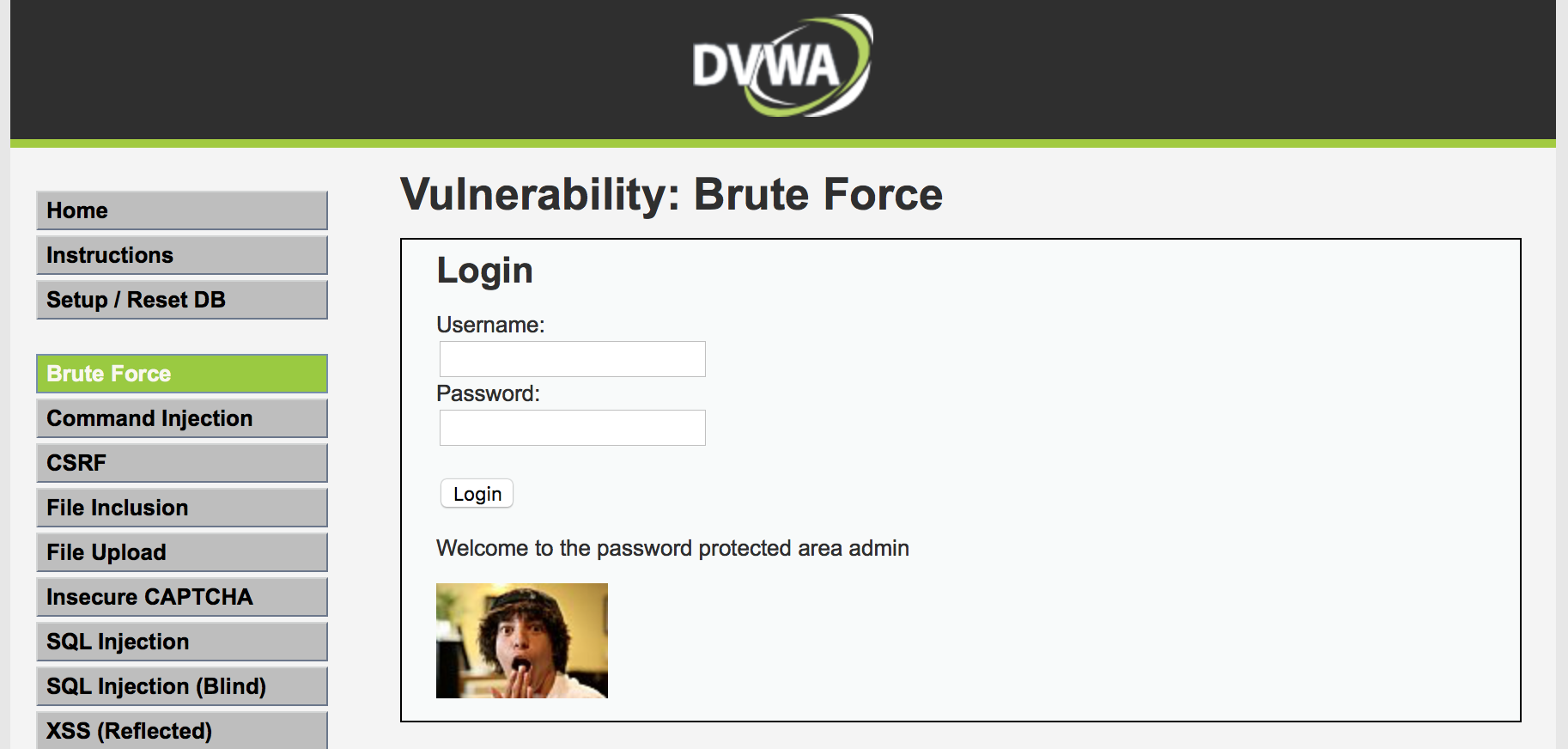
L’autre méthode s’appuie sur un dictionnaire. On crée donc un fichier, que l’on nomme « mots\_de\_passe.txt », contenant les mots de passe les plus utilisés. Il est aussi possible d’y rajouter des informations sur les utilisateurs (ville de résidence, noms des enfants, année de naissance, …) pour étendre l’éventail de recherche des combinaisons login / mot de passe.

Après le premier essai, on remarque que les champs login et mot de passe interviennent dans l’URL. <http://localhost/dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login#>.

Les essais à répétition se feront donc sur l’URL en remplaçant les champs username et password par un login choisi au préalable, et un mot de passe parmi la liste du fichier de mots de passe créé précédemment.

Après l’attaque, on remarque que la combinaison username = admin, password = password est censé fonctionner. Il est possible de vérifier en rentrant ces données dans les champs concerné.

On arrive bien à se connecter au système en tant qu’admin :



1. Protection de la faille

COMMAND EXECUTION

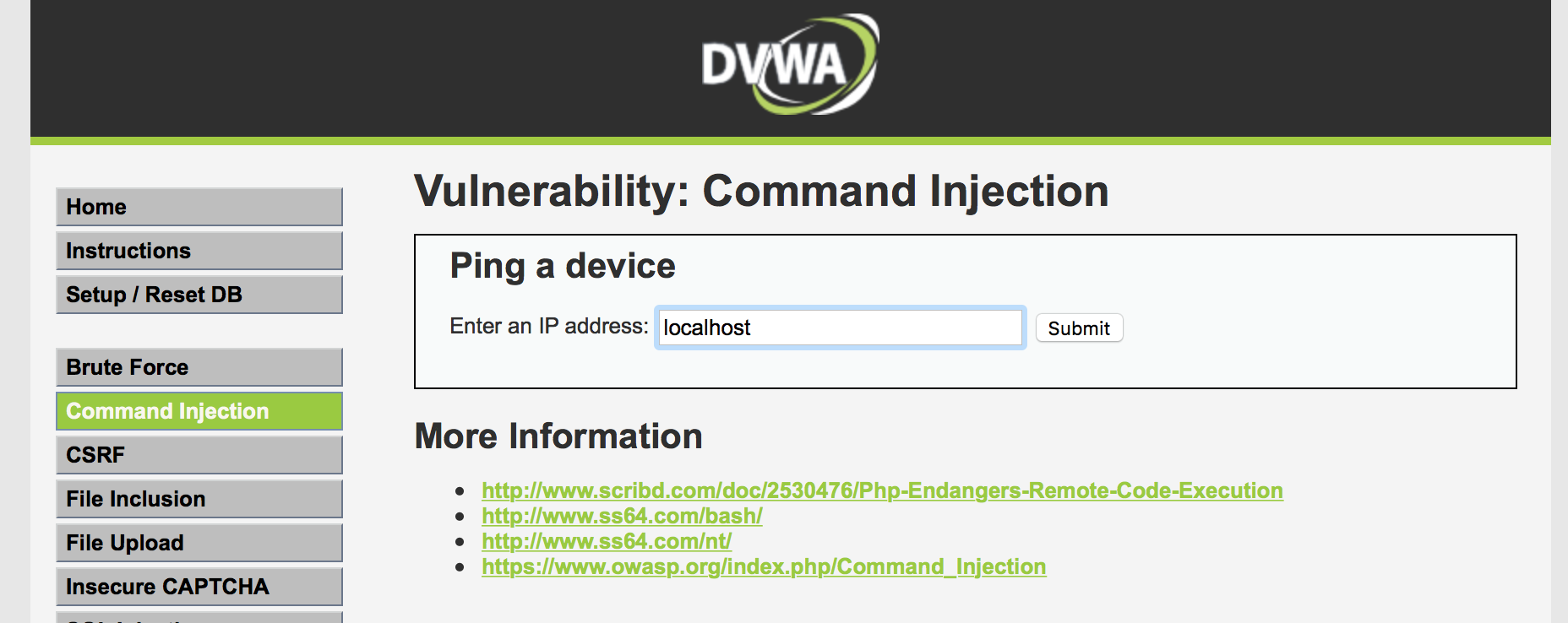
1. Description de la faille

Une tentative d’attaque par exécution de commandes consiste, comme son nom l’indique, à exécuter des commandes à partir d’un champ d’une application web. L’intérêt est ici de pouvoir exécuter ces commandes dans le serveur web. Il est à savoir que les commandes lancées dans ce serveur le sont avec les droits du serveur.

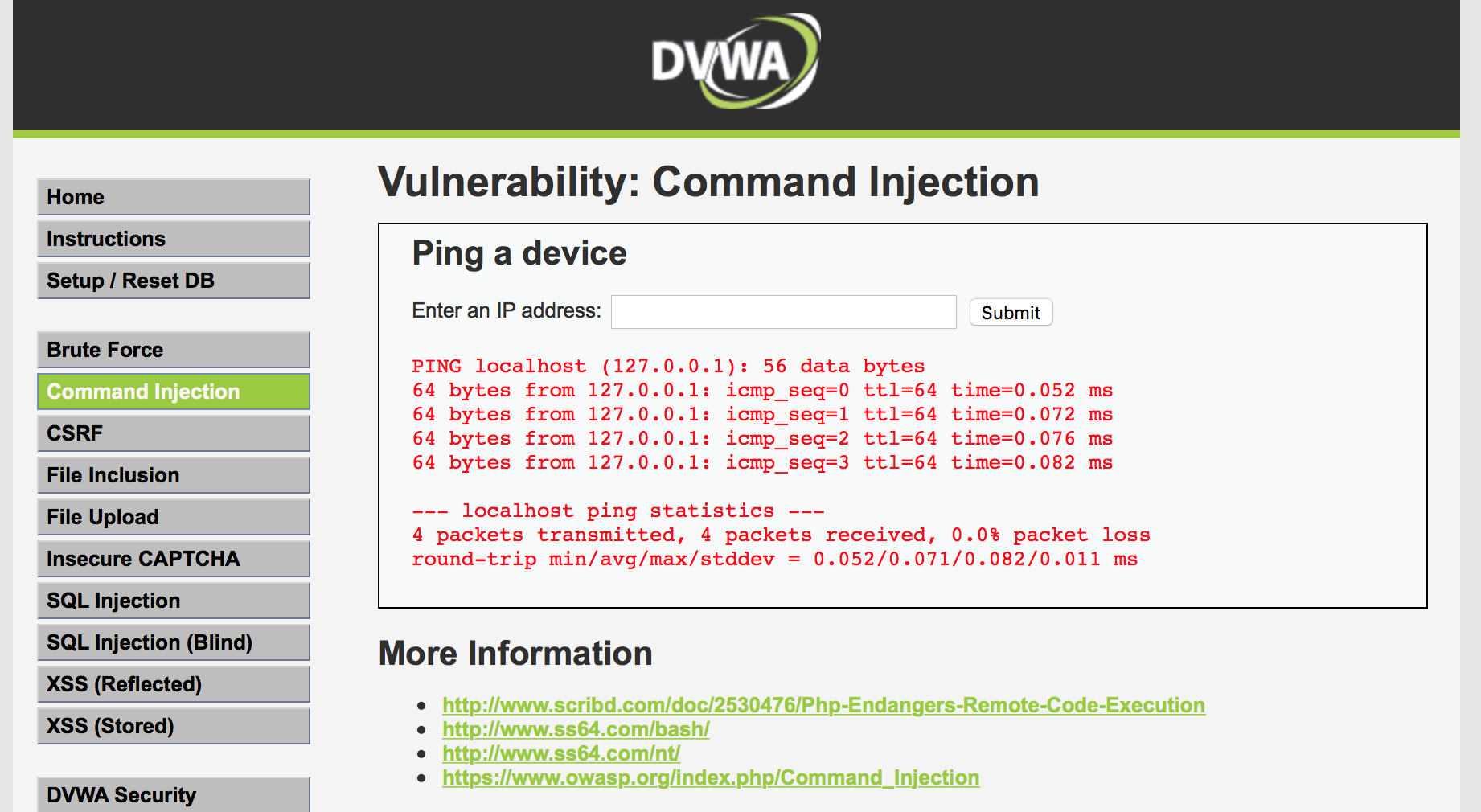
Ce type d’attaque peut servir de premier point d’entrée pour une attaque de plus grande ampleur dans l’application web visée.

1. Exploitation de la faille

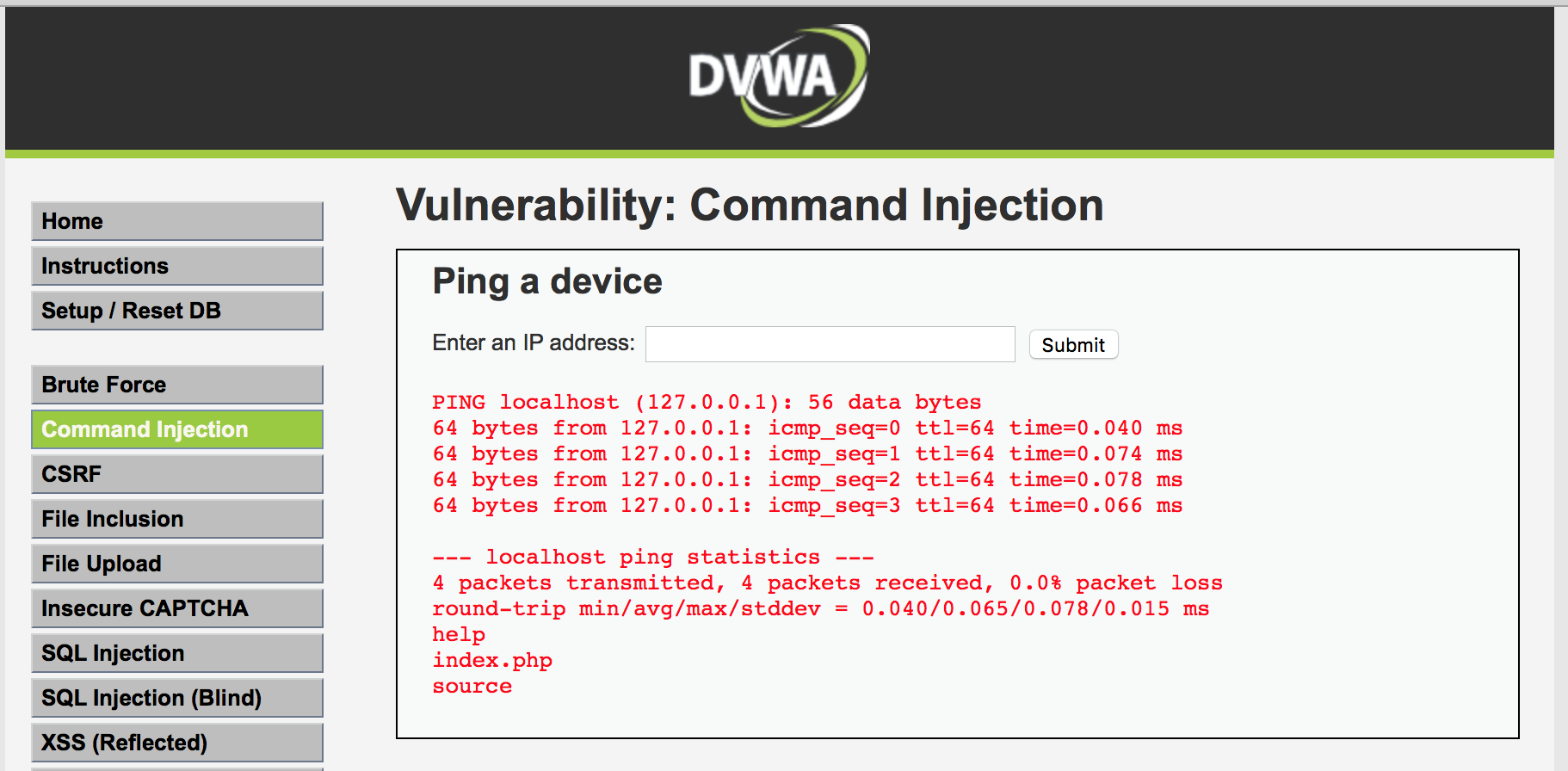
On se place dans l’onglet Command Execution. Ici on doit rentrer une adresse IP pour effectuer un ping vers cette adresse. On peut tester ce ping en entrant « localhost » :



Ce qui donne :



On peut essayer de rentrer une commande après l’adresse choisie en séparant celles-ci d’un « ; ». Par exemple, en rentrant la commande « localhost ; ls », on obtient :



On a donc un listing de l’ensemble des fichiers et des répertoires présents dans le répertoire où l’on se trouve.

Il devient alors possible de lancer des commandes à partir de cette barre de recherche. De plus, il est possible d’enchaîner les commandes en les séparant par « ; » et donc de naviguer dans les répertoires du système.

1. Protection de la faille