

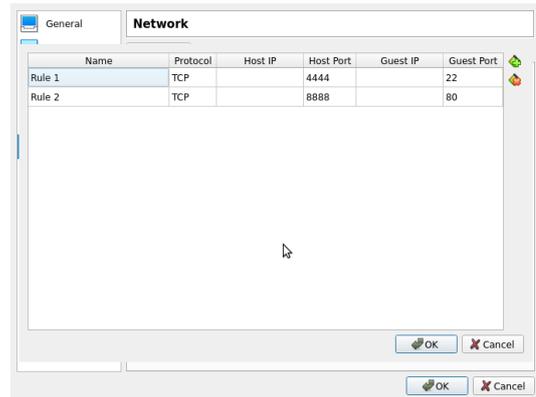
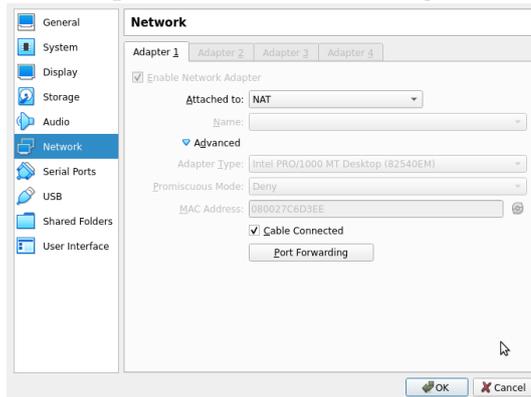
Sécurité des Applications Web

■ ■ ■ Utilisation de la plateforme DVWA

Vous téléchargerez la VM DVWA.ova sur http://p-fb.net/fileadmin/Init_securite/DVWA.ova

- login : pef
- mot de passe : student

Vous vérifierez que votre VM est bien configurée :



Vous pourrez accéder à la VM depuis votre poste de la salle de TP :

▷ en SSH par :

```

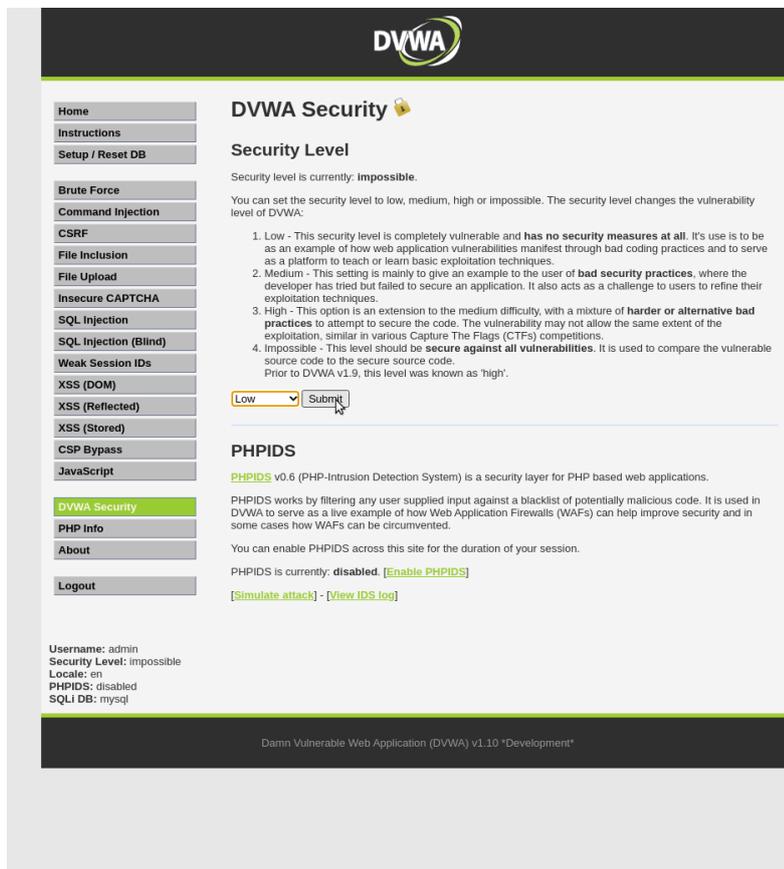
xterm
$ ssh pef@localhost -p 4444
    
```

▷ en HTTP dans votre navigateur : <http://localhost:8888/DVWA/>

Pour l'application Web DVWA :

- login : admin
- password : password

Vous configurerez la sécurité de l'application Web DVWA à « low » ⇒



Attention

Pour chaque **page d'activité** de l'application Web DVWA, vous avez :

- un bouton `View source` qui vous permet de voir le code PHP utilisé par le serveur Web pour gérer l'activité ;
- un bouton `View Help` qui vous donne des informations et des réponses visibles en sélectionnant le texte.
- des liens vers des ressources pour approfondir vos connaissances ou simplement comprendre de quoi on parle.

⇒ **Lisez les !**

■ ■ ■ Attaque Brute Force

1 – Vous essaieriez l'attaque « *brute force* » décrite dans le support de cours disponible à http://p-fb.net/licence3/Init_securite/cours/DVWA_crack.pdf à la page 43.

Le script bash est disponible sur la VM en connexion SSH avec l'utilisateur `student`.

- α. vous vous connectez à l'application web DVWA en tant qu'utilisateur `admin` depuis votre navigateur ;
- β. vous récupérez le « *cookie* » de session présent dans votre navigateur, à l'aide du mode « *inspect* » du navigateur (clic droit sur la page) ;
- γ. vous vous connectez par SSH à la VM avec le compte `pef` ou `student` ;
- δ. vous personnalisez le script `bruteforce` présent dans le répertoire `/home/pef` avec le `cookie`.
- ε. vous vérifierez que vous obtenez bien le mot de passe associé à `admin`.

Questions sur le script « *bruteforce* » :

- a. à quoi sert la commande « *curl* » ?
- b. à quoi sert le **cookie** que l'on copie depuis le navigateur ?
- c. que se passe-t-il si vous **ne mettez pas** le `cookie` ?
En ajoutant l'option `-v` à la commande `curl` vous obtiendrez une trace de l'échange par TCP avec le serveur Web.
- d. comment le script sait-il que le **mot de passe est le bon** ?

■ ■ ■ Attaque par injection de commande

2 – Essayez les attaques par « *injection de commande* » :

- a. Quels sont les **droits Unix** des commandes que vous pouvez lancer ?
- b. Que pouvez vous faire avec l'**injection de commande** et les **droits** ?
- c. Proposez des « *injections* » **intéressantes** :
 - ◇ **modification du contenu du site web** : modifiez la page accessible à l'adresse : `http://localhost:8888/`
 - ◇ **accès à des contenus interdits** : recherchez les fichiers intéressants.
 - ◇ **Autres** ? changement de mot de passe ? téléchargement de contenu dans le site web pour l'héberger à l'insu de l'administrateur ?

■ ■ ■ Attaque par SQL injection

3 – a. Testez les différentes **SQL injection** proposées dans le cours à partir de la page 45.

- b. Lisez la **documentation** associée avec les liens proposés et le bouton `View Help`.
- c. Dans le **cours à la page 46**, vous avez une injection SQL :
 - ◇ que permet-elle d'obtenir ?
 - ◇ Est-ce que l'on pouvez faire sans elle ?
 - ◇ Regardez le code SQL utilisé sur par le site (bouton `View Source`) : pourquoi lors de l'injection SQL a-t-on des infos `ID`, `First name` et `Surname` ?
- d. Essayez l'injection SQL décrite à la page 47 du cours.

- e. en fouillant dans la documentation de l'application Web DVWA, pouvez vous trouver le mot de passe d'accès direct à la BD et afficher le contenu de la table users :

```
xterm
$ mysql -u dvwa -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 46
Server version: 10.6.7-MariaDB-2ubuntu1.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> connect dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Connection id:      47
Current database: dvwa

MariaDB [dvwa]> select * from users;
+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user      | password |
+-----+-----+-----+-----+-----+
...
```

- f. Comment sont stockés les « mots de passe » des utilisateurs ?
- g. Comment fonctionne le script « crackpwd » disponible sur la VM dans le répertoire /home/pef ?