

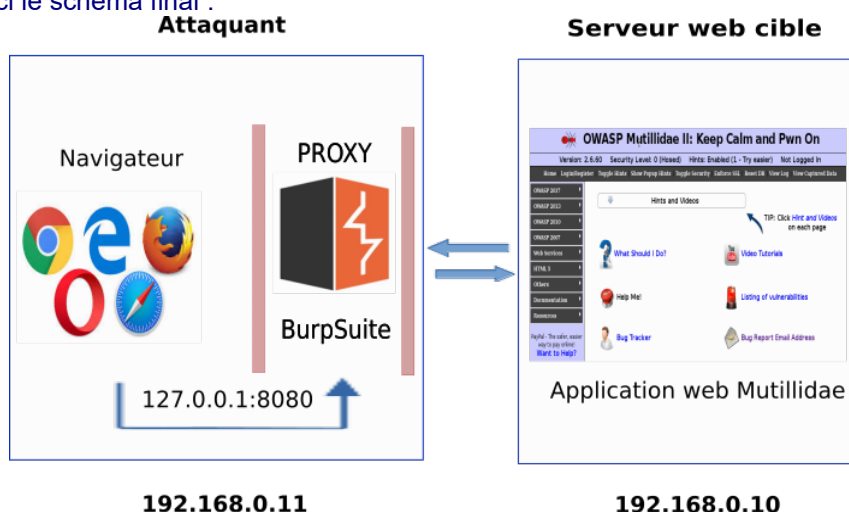
OWASP : Mise en place de la plateforme d'apprentissage

I Architecture générale.....	1
II Préparation des machines.....	2
1 Description des machines.....	2
2 Mise à jour des paquets.....	2
III Préparation de Mutillidae.....	2
1 Présentation de Mutillidae.....	2
2 Installation de Mutillidae.....	3
2.1 Installation.....	3
2.2 Initialisation de la configuration.....	5
IV Préparation de BurpSuite.....	6
1 Présentation de BurpSuite.....	6
2 Installation de BurpSuite.....	6
2.1 Installation.....	6
2.2 Configuration du navigateur.....	8
2.3 Première capture de paquet.....	9
V Pistes d'exploitation pédagogique.....	11

I Architecture générale

L'objectif est d'installer les outils permettant de disposer de la plateforme de test des différentes activités.

Pour rappel, voici le schéma final :



Deux machines sont nécessaires : une machine servant pour l'attaque et une autre machine servant de serveur web cible à attaquer.

→ La machine attaquante :

Elle dispose d'un environnement graphique de bureau avec un navigateur. Le proxy BurpSuite est installé. Le navigateur est configuré pour faire transiter les requêtes par le proxy BurpSuite.

→ La machine cible :

Il s'agit du serveur web, sans bureau, hébergeant l'application web cible Mutillidae. L'application Mutillidae comporte des pages web vulnérables aux attaques étudiées dans ce côté labo.

Ces installations peuvent être réalisées par l'enseignant afin que les étudiants disposent directement de la plateforme d'apprentissage.

II Préparation des machines

1 Description des machines

Deux machines sont nécessaires, une première servant à héberger le serveur Mutillidae et une seconde faisant office de client et contenant Burpsuite et les autres outils nécessaires à l'exécution des défis.

Il est fortement recommandé de réaliser ces installations à l'aide d'un outil de virtualisation (VMWare, VirtualBox...).

MACHINES	RÔLES	ADRESSES IP
Serveur Debian	Serveur web hébergeant la plateforme Mutillidae.	192.168.0.10/24
Client Debian	Machine disposant des outils permettant de réaliser les attaques (navigateur, BurpSuite...).	192.168.0.11/24

Mutillidae sera installé sur une machine de type Debian Stretch sans bureau (www.debian.org).

Pour la machine cliente, nous utiliserons aussi une machine de type Debian 9 disposant d'un bureau et d'un navigateur de type Firefox. L'installation des outils présentés peut se faire sur d'autres distributions. Il est aussi possible de s'orienter vers la distribution Kali qui intègre de nombreux logiciels permettant de faire des tests de pénétration.

2 Mise à jour des paquets

Sur les deux machines, la mise à jour des paquets se fait avec la commande suivante :

```
#apt update && apt upgrade
```

III Préparation de Mutillidae

1 Présentation de Mutillidae

Mutillidae est une plateforme pédagogique mise en place par le groupe OWASP (Open Web Application Security Project) qui permet d'étudier les attaques associées aux applications web. Il s'agit de scripts PHP destinés à se familiariser avec les technologies web (protocole HTTP, AJAX...) et aux vulnérabilités qui en découlent.

Cet enseignement se fait à travers plusieurs activités qui ciblent chaque problème de sécurité du TOP10 d'OWASP (injection SQL, XSS, manipulation des en-têtes HTTP, vol de session...). Chaque activité donne accès à une page comportant un défi que l'utilisateur doit accomplir. Les scripts sont disponibles en version non sécurisée afin de tester les vulnérabilités. Des versions sécurisées permettent de vérifier que les attaques échouent avec un minimum de contrôles sur les données saisies dans les formulaires.

Dans l'activité 1, seule la partie sur la notion d'injection sera testée.



OWASP Mutillidae II: Web Pwn in Mass Production

2 Installation de Mutillidae

2.1 Installation

→ Pré-requis

L'installation se fait **sur le serveur Debian 9** et nécessite les manipulations suivantes comme pré-requis :

```
#apt install php7.0-xm1 libapache2-mod-php php-mysql mysql-server apache2 apache2-utils php-xm1  
php-gd php-imap php-gettext php-curl zip
```

Ces commandes permettent d'installer Apache, MySQL serveur, PHP 7 et leurs dépendances.

Il faut créer ensuite un utilisateur spécifique dans MySQL pour l'application Mutillidae. On commence donc par se connecter à la base de données :

```
#mysql
```

Une fois la console Mysql/MariaDB ouverte, créer l'utilisateur et lui donner des droits :

```
CREATE USER 'mutillidae'@'localhost' IDENTIFIED BY 'password';  
GRANT ALL PRIVILEGES ON *.* to 'mutillidae'@'localhost';
```

Ne pas oublier d'appliquer les nouveaux droits :

```
#FLUSH PRIVILEGES;
```

→ Téléchargement et décompression de Mutillidae

Le téléchargement de **la dernière version de Mutillidae** peut se faire à l'aide de la commande wget.

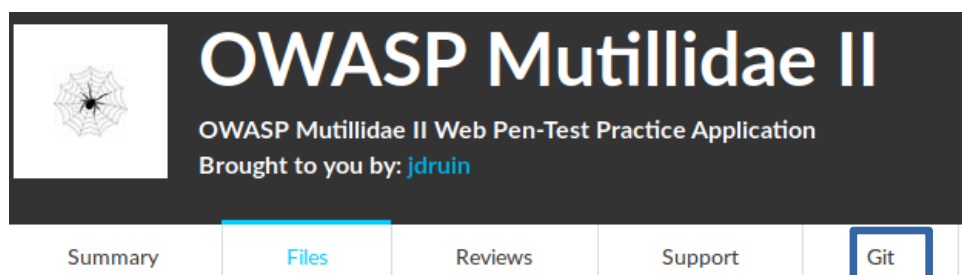
```
wget https://sourceforge.net/projects/mutillidae/files/mutillidae-project/LATEST-mutillidae-2.6.62.zip
```

Il est aussi possible d'utiliser une ancienne version de Mutillidae. Pour récupérer **une version précédente** de Mutillidae, il faut passer par le site de **Sourceforge** via le cheminement indiqué ci-dessous. Attention à ne pas utiliser la version 2.6.60 à cause d'un bug sur un des défis de l'activité 2 (énumération des logins).

1- Aller sur le site de Sourceforge associé au projet OWASP Mutillidae :

Le lien est le suivant : <https://sourceforge.net/projects/mutillidae/files/mutillidae-project/>

2- Une fois sur la page d'accueil du projet, cliquer sur le lien **Git**.



3- Sur la page suivante, cliquer sur le lien **History**.



4- Cliquer ensuite sur la version voulue. Par exemple, pour la version 2.6.62 :



5- Cliquer sur **Browse code at this version**, puis sur **Download Snapshot**.



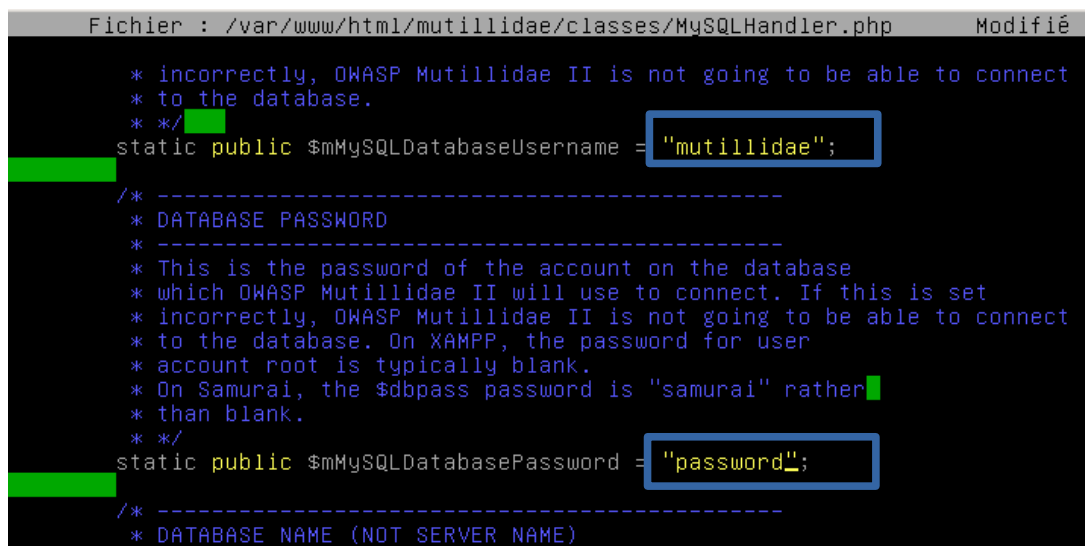
Le téléchargement de Mutillidae peut alors s'effectuer directement en cliquant sur la version voulue ou à l'aide de la commande `wget` en récupérant le lien.

L'archive récupérée se décompresse avec la commande *unzip* et doit être déplacée à la racine du serveur web en transférant la propriété de tout le répertoire à l'utilisateur *www-data*.

```
#mv mutillidae/ /var/www/html/mutillidae
```

```
#chown -R www-data /var/www/html/mutillidae
```

Il faut ensuite modifier le fichier *MySQLHandler.php* en indiquant l'utilisateur et son mot de passe. Il faut donc un éditeur de texte et modifier ce fichier situé dans */var/www/html/mutillidae/classes/*.



```
Fichier : /var/www/html/mutillidae/classes/MySQLHandler.php  Modifié

    * incorrectly, OWASP Mutillidae II is not going to be able to connect
    * to the database.
    */
static public $mMySQLDatabaseUsername = "mutillidae";

/* -----
 * DATABASE PASSWORD
 * -----
 * This is the password of the account on the database
 * which OWASP Mutillidae II will use to connect. If this is set
 * incorrectly, OWASP Mutillidae II is not going to be able to connect
 * to the database. On XAMPP, the password for user
 * account root is typically blank.
 * On Samurai, the $dbpass password is "samurai" rather
 * than blank.
 */
static public $mMySQLDatabasePassword = "password";

/* -----
 * DATABASE NAME (NOT SERVER NAME)
```

2.2 Initialisation de la configuration

Puis, via le navigateur de la machine cliente, un premier test peut être effectué en saisissant dans l'url : *<ip-nom-serveur>/mutillidae*.

En cas de page blanche, il faut relancer le serveur apache avec la commande suivante :

```
#service apache2 restart
```

La page qui apparaît permet de finaliser l'installation.

The database server at 127.0.0.1 appears to be offline. Try to [setup/reset the DB](#) to see if that helps. Check the error message below for more suggestions.

Note: On some older installations, this message could be a false positive. You can opt-out of these warnings below.

Il faut cliquer sur le lien *setup/reset the DB*. L'accès à l'application se fait en saisissant dans l'url *<ip-ou-nom-serveur>/mutillidae*.


OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

[OWASP 2017](#)
[OWASP 2013](#)
[OWASP 2010](#)
[OWASP 2007](#)
[Web Services](#)
[HTML 5](#)
[Others](#)
[Documentation](#)
[Resources](#)

PayPal - The safer, easier way to pay online!
[Want to Help?](#)

 **Hints and Videos**

 [What Should I Do?](#)

 [Help Me!](#)

 [Bug Tracker](#)

 [Video Tutorials](#)

 [Listing of vulnerabilities](#)

 [Bug Report Email Address](#)

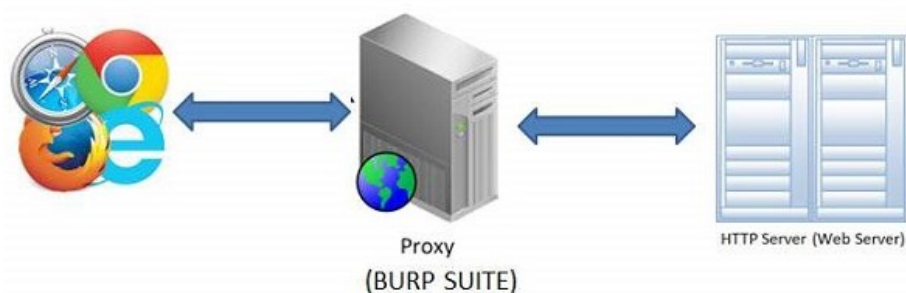
TIP: Click [Hint and Videos](#) on each page

IV Préparation de BurpSuite

1 Présentation de BurpSuite

BurpSuite est une plateforme qui permet d'effectuer des tests de sécurité sur les applications web. Elle joue le rôle d'un proxy qui se positionne entre le navigateur de l'attaquant et le serveur contenant l'application web à tester. Il capture les requêtes effectuées afin de pouvoir les analyser, les modifier et les rejouer en modifiant les paramètres. Grâce à ces captures, il est alors possible de tester les vulnérabilités comme les injections SQL ou le XSS. BurpSuite incorpore les outils suivants :

- ❖ un proxy qui permet d'intercepter les requêtes entre le navigateur et l'application cible ;
- ❖ un scanner d'applications web ;
- ❖ un outil permettant de découvrir les champs d'une page dans le but de pouvoir les exploiter ;
- ❖ un outil d'intrusion permettant d'effectuer des attaques spécifiques afin d'exploiter certaines vulnérabilités ;
- ❖ un outil de répétition permettant la modification avant envoi des requêtes ;
- ❖ un séquenceur pour tester la randomisation des sessions.



BurpSuite est donc un excellent outil pour relever les défis de Mutillidae.

 Burpsuite sera nécessaire uniquement lors de certaines activités.

2 Installation de BurpSuite

2.1 Installation

L'installation se fait sur la machine cliente. Nous avons utilisé une Debian 9 graphique. BurpSuite est disponible en version gratuite et en version payante avec des fonctionnalités avancées. Nous installerons la version gratuite.

Le téléchargement se fait via le lien suivant en utilisant un navigateur:

```
portswigger.net/burp
```

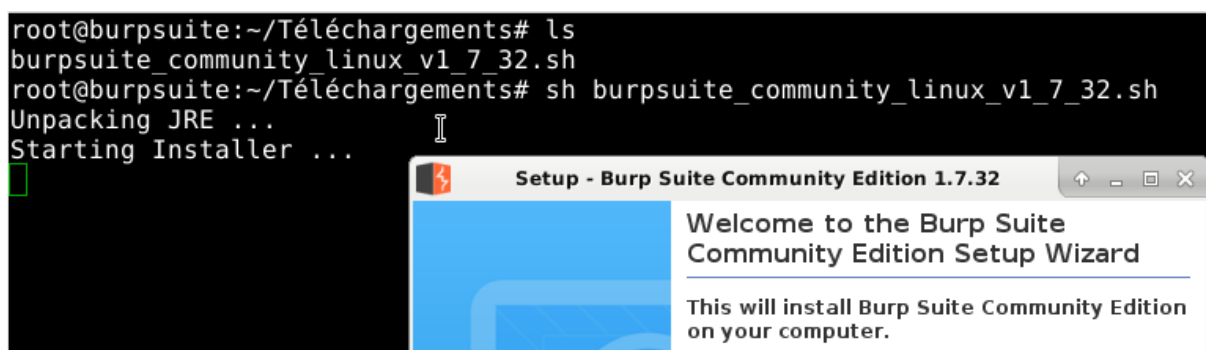
Choisir la version communautaire et cliquer sur le bouton **Download**. Puis, choisir la version pour Linux (64 bits).

Le script téléchargé doit être exécutable.

```
chmod +x burpsuite_community_linux_v1_7_32.sh
```

Le lancement de l'installation peut commencer.

```
sh burpsuite_community_linux_v1_7_32.sh
```



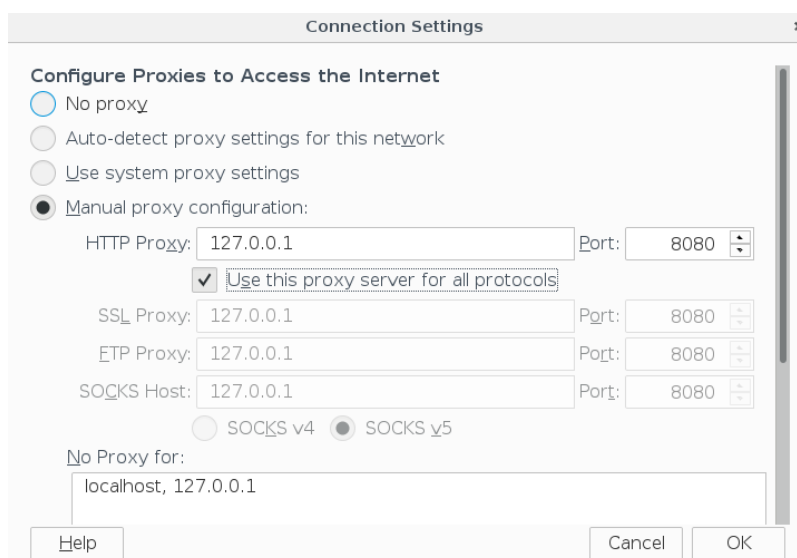
Il ne reste plus qu'à finaliser l'installation en cliquant sur le bouton **Next** et en laissant les valeurs par défaut.

2.2 Configuration du navigateur

Lorsqu'il sera nécessaire d'utiliser Burpsuite, le navigateur devra être configuré pour l'utiliser en tant que proxy. Avec Firefox, il faut aller dans Édition puis *Préférences* ou saisir *about:preferences* dans l'url afin d'accéder aux options avancées de configuration.

Puis, dans l'onglet réseau, il faut cliquer sur paramètres et faire référence au proxy BurpSuite. L'écoute se fait sur le port 8080.

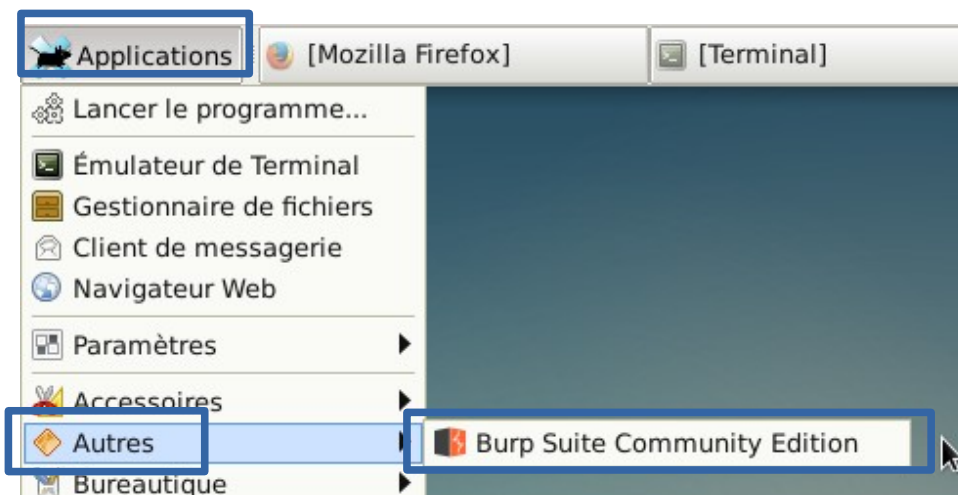
Ensuite, il faut indiquer l'adresse de bouclage 127.0.0.1¹ ainsi que le port d'écoute 8080.



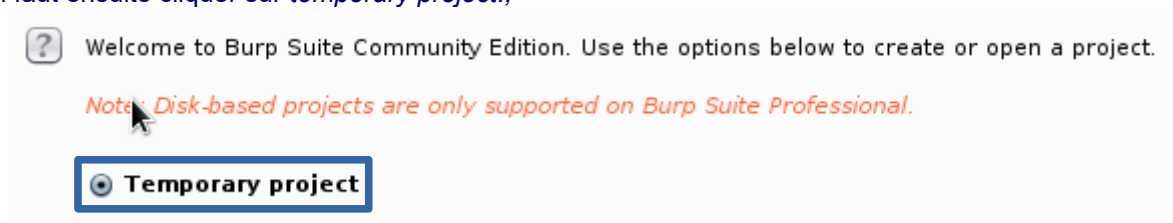
¹ Si le navigateur utilisé et Burpsuite sont sur le même poste.

2.3 Première capture de paquet

Une fois l'installation terminée, BurpSuite apparaît dans le sous menu **Autres** du menu **Applications** (environnement graphique xfce4) et peut être démarré.



Il faut ensuite cliquer sur *temporary project*.,



Puis un autre clic sur *suivant* et enfin sur *burp defaults*.

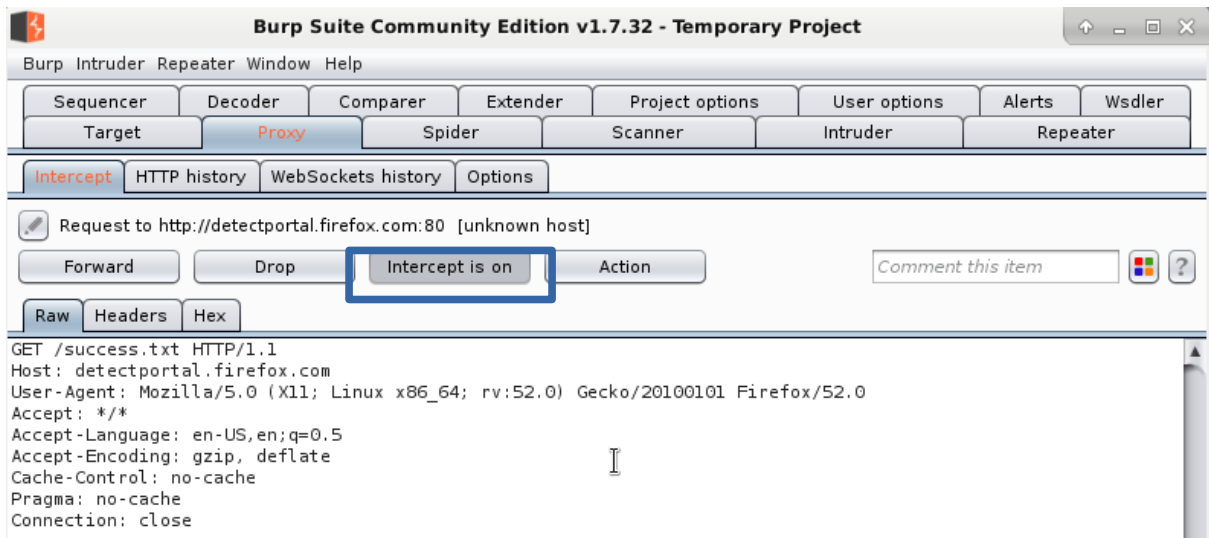


Enfin, il faut cliquer sur le bouton **Start Burp**.

Le répertoire d'installation de BurpSuite se situe par défaut dans `/usr/local/BurpSuiteCommunity`. Pour effectuer une première interception de requête, il faut cliquer sur l'onglet *Proxy*, puis sur *Intercept* et vérifier la présence du bouton *intercept is on*.

Lors de l'accès à un site depuis le navigateur, chaque requête est capturée par BurpSuite. Le clic sur le bouton *Forward* permet de passer à la requête suivante. En attendant ce clic, le proxy se met en attente avant d'envoyer les données vers le serveur web.

Pour désactiver la capture, il suffit de cliquer sur 'intercept is on'.



V Pistes d'exploitation pédagogique

→ Objectif :

L'objectif est de couvrir en partie ou en totalité les problématiques de sécurité associées aux 10 activités de ce côté labo. Cet objectif rentre dans le cadre de la démarche CyberEdu lancée en novembre 2017.

→ Installations :

Si les étudiants SLAM ne sont pas à l'aise avec les travaux d'installations sous Linux, l'enseignant peut leur mettre à disposition des modèles de machines virtuelles prêtes pour être clonées.

→ Travail individuel:

Les activités 1 à 10 peuvent être réalisées individuellement par les étudiants qui devront disposer d'un clone des deux machines BurpSuite et Mutillidae. Le travail peut être séquentiel, activité après activité. Les activités étant indépendantes, l'enseignant peut ponctuellement faire travailler les étudiants sur une activité particulière en cas de manque de temps.

→ Travail en groupe:

L'enseignant peut répartir les étudiants par groupes de deux en les affectant à des activités différentes. Par exemple, un groupe traite l'activité 1 sur les injections et produit un compte rendu documenté. Un autre groupe traite, en parallèle, l'activité 3 sur le XSS et produit aussi un compte rendu documenté.

A la fin de la séance, l'enseignant organise **une synthèse** durant lequel chaque groupe rend compte aux autres de son travail via des manipulations vidéo-projetées. Ainsi, un groupe n'ayant pas travaillé sur une activité pourra bénéficier de la sensibilisation de sécurité correspondante via le compte rendu des autres groupes. Cette démarche permet de couvrir plus rapidement les différentes activités.

→ Durée de travail :

Lorsque les machines sont prêtes, chaque activité doit pouvoir se traiter en une heure. Le dossier documentaire de chaque activité de ces côtés labo comprend de nombreuses captures d'écrans de façon à guider les étudiants dans les manipulations demandées (ce qu'il faut faire, ce qui est censé s'afficher à l'écran si les activités sont traitées avec succès).

Lors d'un travail en groupe, la phase de synthèse devra être guidée par l'enseignant en fixant une limite de temps au compte rendu de chaque groupe de façon à couvrir l'ensemble des activités traitées. Les comptes rendus des différents groupes seront mis à disposition de tous les étudiants.

→ Évaluation :

L'évaluation de chaque activité peut porter sur deux items :

- le succès dans la réalisation des défis demandés ;
- la qualité du compte rendu rédigé et comportant des captures d'écrans.