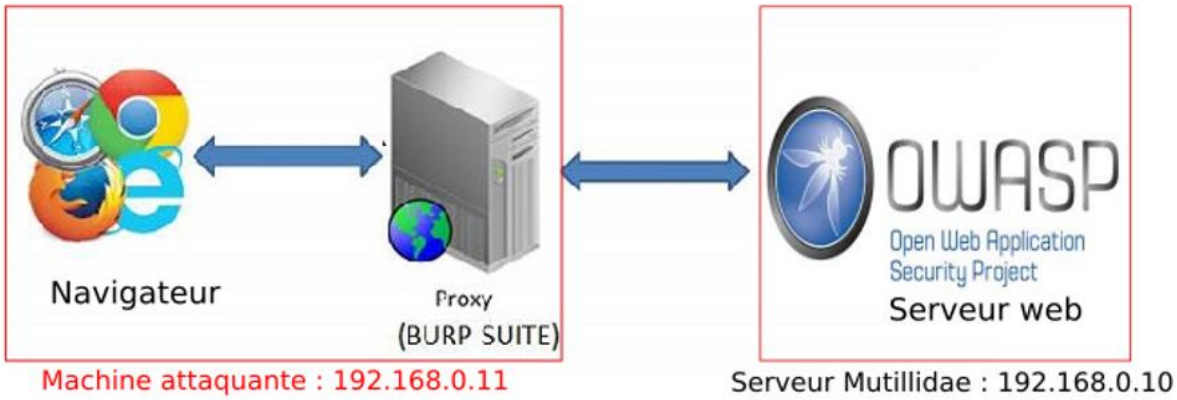
PPE 3.1

Exploitation d’une plateforme d’apprentissage des vulnérabilités des applications web.

⚠ Toutes les manipulations décrites sont réalisées uniquement sur la plateforme pédagogique présentée. Elles ne doivent EN AUCUN CAS être testées sur d'autres sites web.

1. **L'environnement.**



Pour accéder à Mutillidae : dans une fenêtre de navigateur : http://192.168.0.10/mutillidae

Vous devez créer un compte sur la plateforme.

Le niveau de sécurité du code mis en place est indiqué en haut de la page près des informations d'authentification.

Security Level: 0 (Hosed)	Absence de contrôle de sécurité.
Security Level: 1 (Client-side Security) Logged In	Contrôles des informations saisies coté client.
Security Level: 5 (Server-side Security) In	Contrôles des informations saisies coté serveur

Le niveau de sécurité du code mis en œuvre se modifie en cliquant sur le lien *Toggle Security*.

Toggle Security

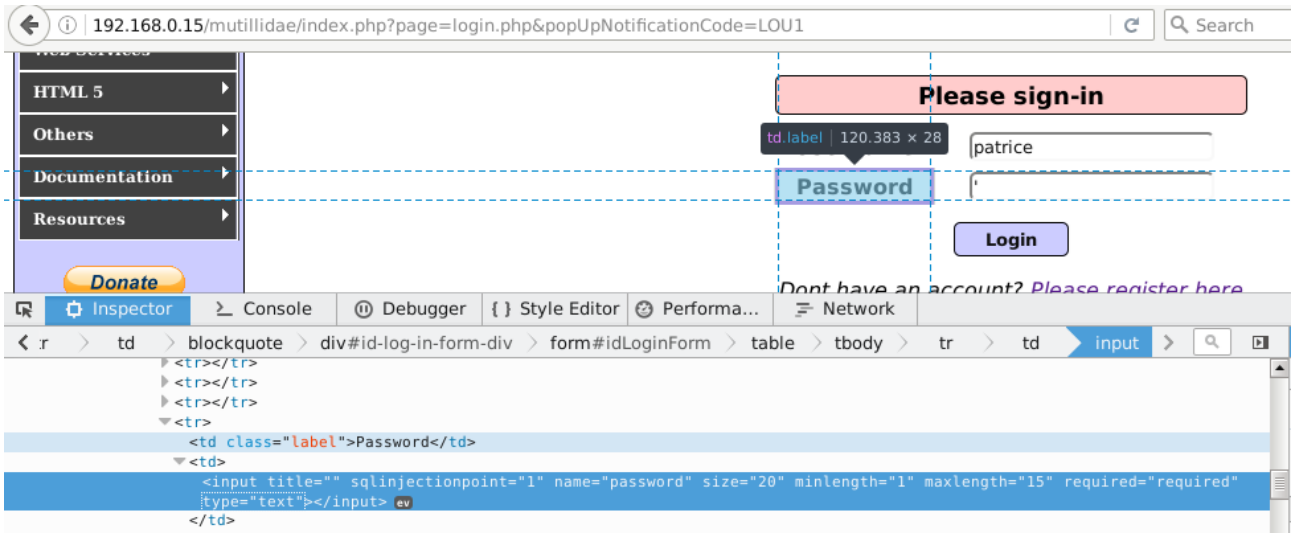
Chaque niveau de sécurité est disponible sur le même script PHP. Ces scripts sont stockés sur le serveur dans le répertoire /var/www/html/mutillidae/.

2. Découverte de la sensibilité SQLi.

La plateforme Mutillidae offre des pages sensibles à la faille SQLi.

Afin de valider la sensibilité SQLi, aller sur la page permettant de se connecter. Il faut aussi penser à vérifier que le niveau de sécurité sélectionné est 0 (Hosed).

Il suffit alors de saisir une quote dans le champ associé au mot de passe.



Dans cet exemple, l'outil Web developper de Firefox a été utilisé afin de rendre visible les données saisies dans le champ associé au mot de passe. Cette manipulation n'est pas indispensable pour relever les défis présentés. Elle sert uniquement à illustrer la saisie de la quote.

Lors du clic sur le bouton Login, une erreur apparaît dévoilant la sensibilité SQLi.

Error Message

Failure is always an option	
Line	170
Code	0
File	/var/www/html/mutillidae/classes/MySQLHandler.php
Message	/var/www/html/mutillidae/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 2 client_info: 5.5.50 host_info: 127.0.0.1 via TCP/IP) Query: SELECT * FROM accounts WHERE username='patrice' AND password='' (0) [Exception]
Trace	#0 /var/www/html/mutillidae/classes/MySQLHandler.php(282): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 /var/www/html/mutillidae/classes/SQLQueryHandler.php(350): MySQLHandler->executeQuery('SELECT * FROM a...') #2 /var/www/html/mutillidae/user-info.php(191): SQLQueryHandler->getUserAccount('patrice', '') #3 /var/www/html/mutillidae/index.php(615): require_once('/var/www/html/m...') #4 {main}
Diagnotic Information	Error attempting to display user information
Click here to reset the DB	

Ce message d'erreur est particulièrement instructif pour une personne malveillante…

3. Les défis.

Premier défi : Extraction de données

Le but est d'obtenir la liste de tous les utilisateurs. Pour lancer le défi, il faut suivre le cheminement suivant : OWASP 2017 => A1 – Injection (SQL) => SQLi – Extract Data => User Info (SQL).

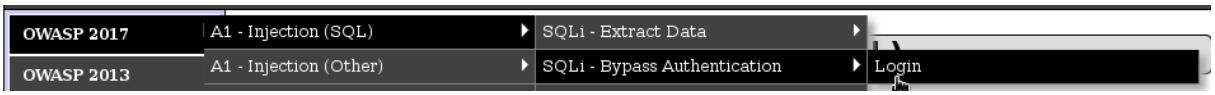
Le nom du script PHP sur le serveur est *user-info.php*.

En temps normal, cette page permet d'afficher le détail des informations d'un compte utilisateur.

Deuxième défi : se connecter en tant qu'administrateur.

Troisième défi : se connecter à un compte quelconque.

Le but est de s'authentifier à l'aide du compte de **toto**. Pour lancer le défi, il faut suivre le cheminement suivant : OWASP 2017 => A1 – Injection (SQL) => SQLi – Bypass Authentication => Login.



Le nom du script PHP sur le serveur est *login.php*. En temps normal, cette page offre un formulaire d'authentification.

Quatrième défi : Modifier le niveau de sécurité.

Vérifier que les défis précédents échouent lorsque l'on change le niveau de sécurité.

Cinquième défi : Etude du code fourni.

En vous aidant du code de Mutillidae, vous devez développer un formulaire d'authentification (en respectant le modèle MVC) où l'injection SQL sera impossible.

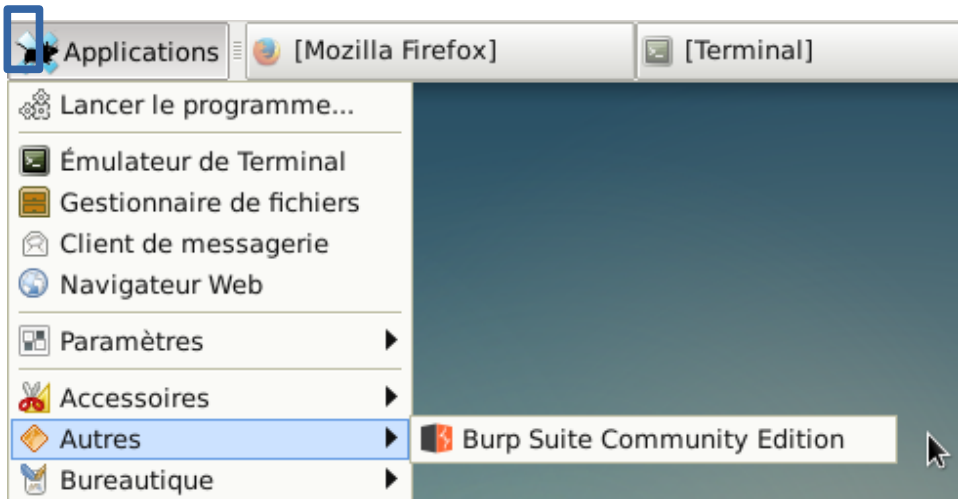
Comme vous travaillez en binôme, vous utiliserez bien évidemment github !

Pour la suite…

Vous devez réaliser les défis de l'activité 2. Vous aurez besoin pour cela de « Burp Suite », qui est installé sur la machine cliente.

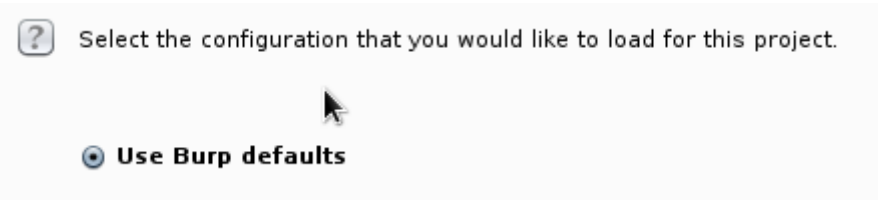
Prise en main :

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*.

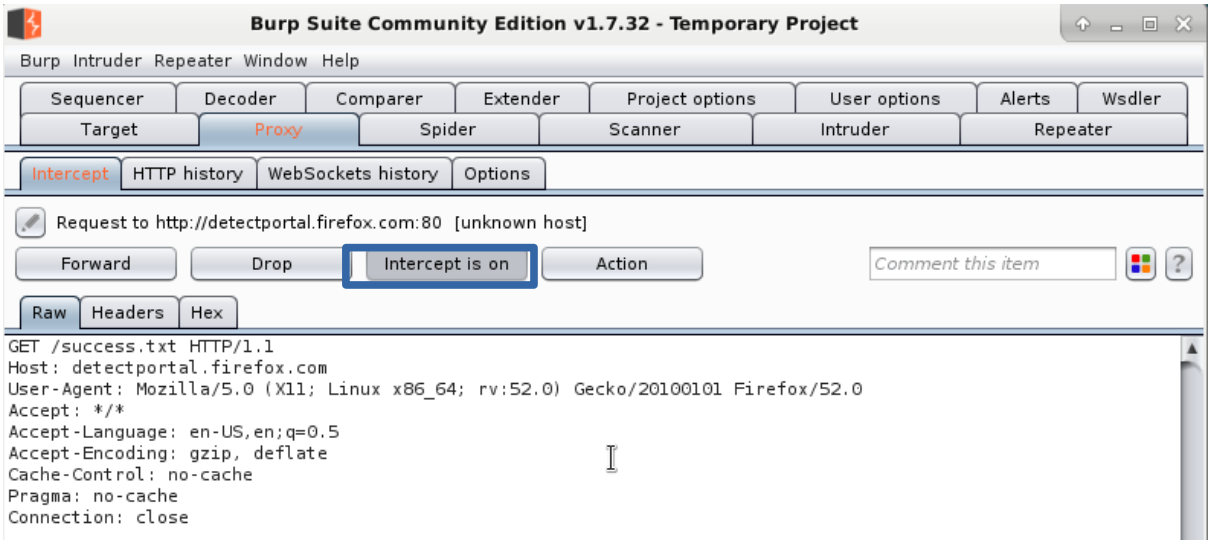


Enfin, il faut cliquer sur le bouton **Start Burp**.

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'.



1. Démarrer BurpsSuite en suivant le cheminement suivant : **Temporary project** => **Use Burp defaults**. Aller dans l'onglet **Proxy** puis sur **Intercept**, vérifier que le proxy est désactivé (**Intercept is off**).
2. Retourner sur la page d'accueil de Mutillidae et cliquer sur le lien **Login/Register** en haut à gauche.

3. Saisir un login dans le champ **Username** et un mot de passe dans le champ **Password** sans cliquer sur le bouton **Login**.
4. Dans l'outil BurpSuite, activer le proxy en cliquant sur **Intercept is off**. Le bouton devient **Intercep is on**.
5. Revenir sur la page d'authentification de Mutillidae et cliquer sur le bouton **Login**.
6. Revenir sur BurpSuite et cliquer sur le bouton **Forward** dans le sous onglet **Intercept** de l'onglet **Proxy**. Le nom des champs est visible dans l'onglet **Raws**.