Séance TP - DVWA

Création des différents attaques contre une machine DVWA

Introduction :

Le but de ce TP est d'exploiter quelques méthodes d'attaque contre un cible serveur web d'une manière légale bien sûr. Les méthodes utilisées ne sont pas exhaustives mais à titre indicatif pour enrichir votre outils disponible et vecteur d'attaque.

Mise en place de l'environnement de travail :

On estime que l'environnement de travail est déjà mis en place dans les tp précédentes comme étant une VM Kali linux (voir ce lien). On préfère l'installation du serveur victime DVWA sur kali directement (voir ce lien).

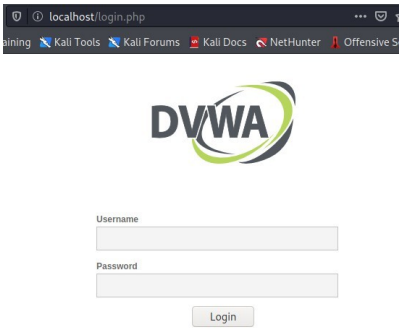
Les identifiants pour Kali linux sont: **kali:kali**

Les identifiants pour DVWA serveur: **admin:password**

Si tout était préparé d'une bonne manière, pour démarrer le serveur sur Kali, vous pouvez ouvrir votre terminal et taper:

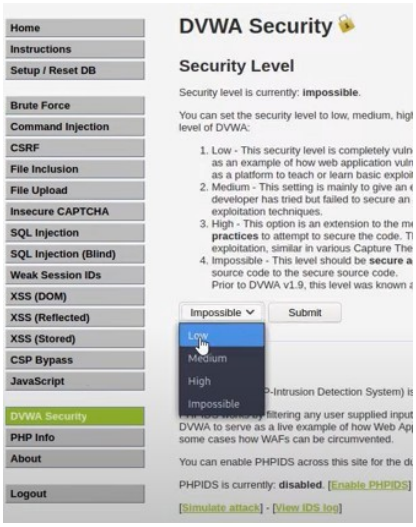
```
#démarrage du
web service
sudo apache2ctl
start
#démarrage du
DB
sudo service mysql start
```

Vous pouvez ouvrir votre browser et ouvrir le lien http://localhost/setup.php, qui va vous permettre à la fin de la page de créer de nouveau le db pour vos tests. Page résultant est:

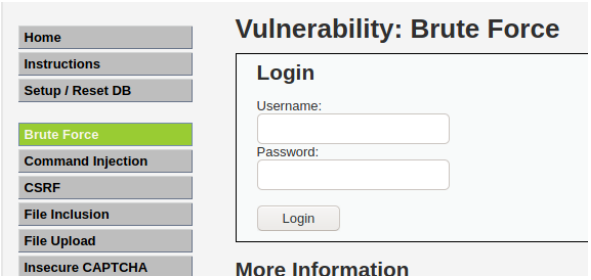


Exercice I - Attaque par Force Brute.

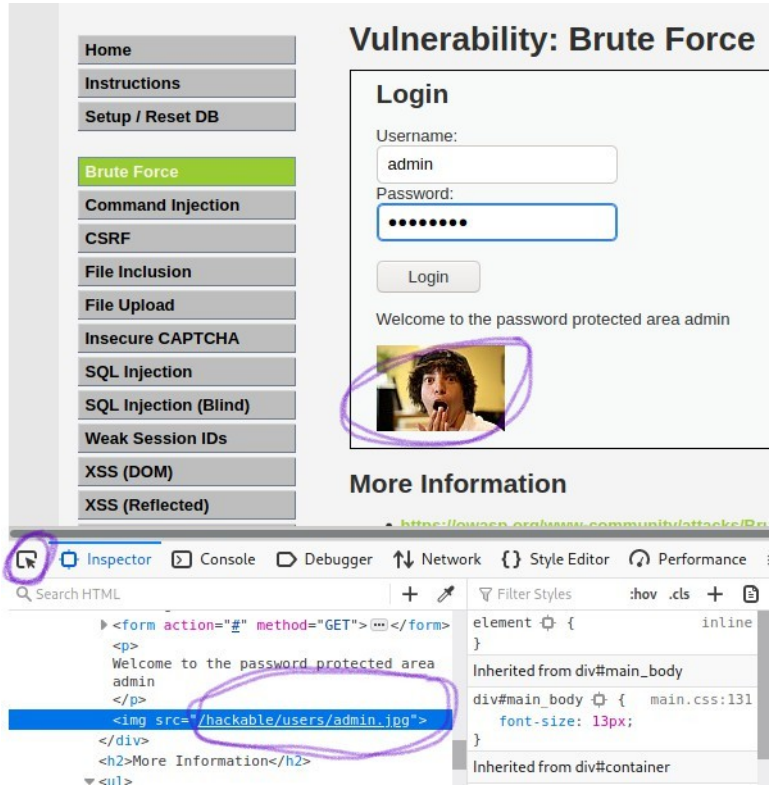
- A noter et rechercher le concept force brute
- Login dans le serveur en utilisant `admin:password`. Naviguez vers DVWA security, et choisissez l'option Low->Submit.



- Afin de choisir la difficulté d'exercice d'attaque, ces options Low - Medium - High - Impossible, sont à votre disposition pour ajuster. Certaines attaques seront possibles dans l'une, d' autres non plus.
- Afin de choisir le type d'attaque, il suffit de sélectionner à gauche dans la navigation.

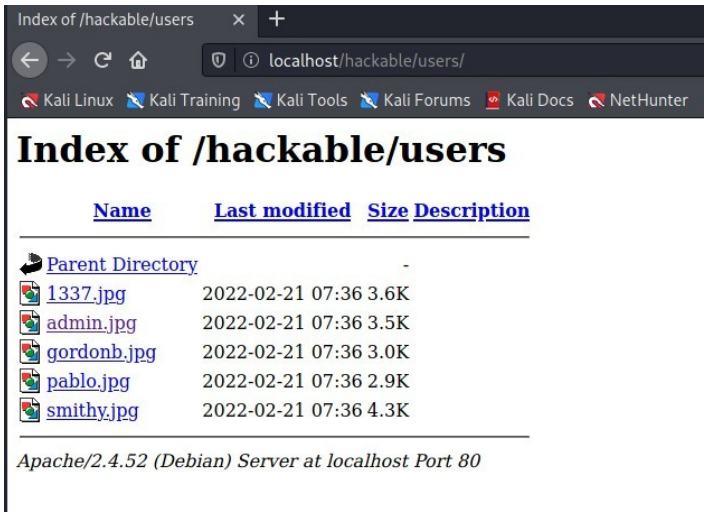


- Dans cette première partie, difficulté Low, on a pour objectif de trouver un nouvel utilisateur et son mot de passe. Au début, on va vraiment "jouer" un peu, et simplement voir le comportement de ce serveur ou application. Essayer `admin:password`. Ensuite essayer `admin:pasbonnepassword`. A noter les remarques et le comportement du système.
- A souligner cette démarche comme étant votre meilleure **attitude personnelle** durant un attaque, parce que la majorité des fois, préalablement personne ne peut connaître de quoi il s'agit le comportement d'un système ou les défenses établis.
  A souligner aussi que, à tout moment, dans n'importe quelle website, vous pouvez cliquez click-droit dans une page web, choisir **l'inspection** : `inspect` ou `inspect element` pour voir les détails comme un programmeur. Dans ces détails, on peut choisir un élément de la page et voir la source de cet élément choisi.



`src=/hackable/users/admin.jpg` est le chemin suivi dans le serveur pour sauvegarder ce fichier. Ca semble pas trop important comme information, mais du faite que vous êtes capable d'acquérir une telle information, ça va permettre de construire une image petit à petit plus claire du serveur et des fichiers sauvegarder.

- Faisons un peu d'exploitation dans ce chemin, on peut écrire directement en haut de la page, donc `http:/local/hackable/users/admin.jpg` ou bien directement click-droit sur l'image et naviguer ver "view image". Le résultat est l'image seule. Très bien. Mais le nom du folder users est intéressant, alors effaçons de ce url, le mot "admin.jpg", et voila ça ouvre en



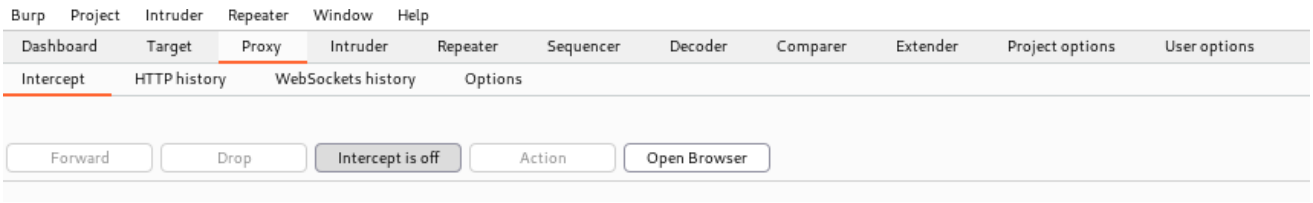
divulguant les utilisateurs présent dans le système!!!

Donc il s'agit de 5 utilisateurs, on les note!

Donc il s’agit aussi de la technologie Apache/2.5.52 Debian, on les note aussi comme étant des pièces d’informations dont on peut être utilisées plus tard ! ou pas!

- A rechercher le programme “Notepad++” ou “Cherry Tree” , pour certaines personnes ceci peut être intéressant pour prendre des notes.
- A noter et rechercher le programme “Burp Suite”, présent déjà dans Kali.
- A noter et rechercher la notion Proxy dans un réseau ou navigateur d’internet.
- Dans notre attaque de brute force, comme c’est un website, l’outil burpsuite permet une grande facilitée dans le travail, même dans la version gratuite.

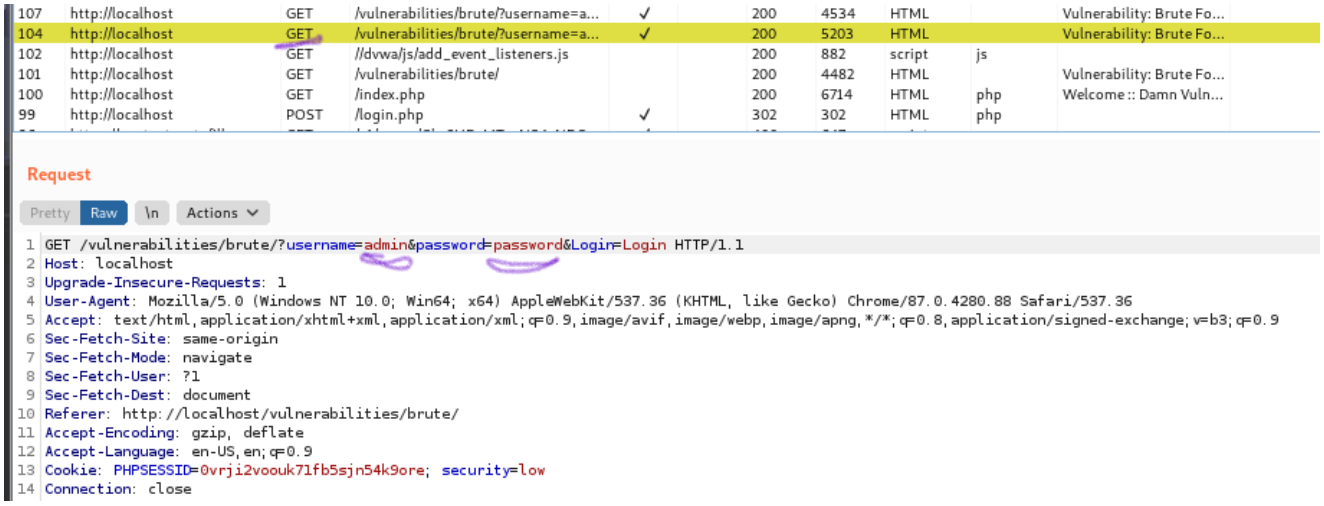
Une petite introduction du Burp Suite pour une bonne utilisation et reference dans ce TP:



- Dans l’option “Target” de la navigation: on peut choisir de limiter notre vue, notre scope, envers notre victime.
- Dans l’option “Proxy”: c’est important de noter “intercept is off”, dans ce mode tous trafic passant par Burp comme étant le proxy, ça va passer. Donc Burp Suite est le proxy, middleman, et pas d’intervention en tant que trafic qui passe à travers. Vous êtes en train d’enregistrer seulement ce qui ce passe a travers vous. Cette option Proxy nécessite que votre navigateur browser soit configuré à choisir ce proxy, ce 127.0.0.1 port 80 comme étant le proxy du kali website ou bien le IP du kali au cas ou vous faites le test à partir d’une autre machine. Pour simplifier notre environnement d’attaque, on peut faire l’attaque en cliquant sur “Open Browser” présent à la droite du “intercept is off”.
  Intercept is on, sert à arrêter la response ou l’envoie des messages web. Peut être pour construire une attaque en changeant la réponse ou quelque chose dans le paquet avant de l’envoyer envers le serveur… Pour le moment, “is off” est bien, pour voir et analyser le trafic qui passe.
- Dans l’option “http history” : on peut voir le trafic, on peut choisir les paquets importants et mettre “highlight” en rouge ou jaune . Voir des paquets ici sert bien à construire une idée comment les choses fonctionnent, ce qui va être important pour pouvoir les déranger ou bien les modifier.

- Dans Burp, sélectionner l’option “Proxy”, “Intercept”, “Open Browser” pour ouvrir et travailler sur un navigateur qui a le Burp comme étant un proxy sans faire la configuration.
- Dans ce nouveau navigateur on peut continuer notre TP, c’est un navigateur normal. Essayer d’ouvrir http://127.0.0.1/login.php ou http://localhost/login.php. Retournez dans Burp, naviguez vers “Target” et choisissez 127.0.0.1 ou localhost, puis click-droit, “Add to scope”. Cela va permettre de voir d’une manière distincte les paquets échangés.
- Analysez le trafic en navigant vers “Proxy” ensuite “Http history”. essayer de faire un login normal. Examiner le contenu des paquets.

❑ Essayer de trouver le paquet responsable du Login. Voyez l’image ci dessous



107	http://localhost	GET	/vulnerabilities/brute/?username=a...	✓	200	4534	HTML		Vulnerability: Brute Fo...
104	http://localhost	GET	/vulnerabilities/brute/?username=a...	✓	200	5203	HTML		Vulnerability: Brute Fo...
102	http://localhost	GET	//dvwa/js/add_event_listeners.js		200	882	script	js	
101	http://localhost	GET	/vulnerabilities/brute/		200	4482	HTML		Vulnerability: Brute Fo...
100	http://localhost	GET	/index.php		200	6714	HTML	php	Welcome :: Damn Vuln...
99	http://localhost	POST	/login.php	✓	302	302	HTML	php	

Request

Pretty Raw \n Actions

```
GET /vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: localhost
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/vulnerabilities/brute/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=0vrji2voouk71fb5sjn54k9ore; security=low
Connection: close
```

- Vous pouvez cliquer click-droit et choisir “Highlight” en jaune ou rouge pour une meilleure visibiltée.
- Click-droit pour sélectionner “Send to Intruder”
- Naviguez vers l’option “Intruder”, choisissez dans “Attack Type” l’option “Cluster Bomb”
- Dans ce paquet, on a besoin juste comme variable `username=§admin§` et `password=§password§`. Ils sont colorés en bleu. En fait l’annotation §§ détermine ce qui sera utilisée comme variable durant l’attaque. Alors effacez les autres annotations §, d’une manière que les seules variable utilisée pour le moment sont username et password.

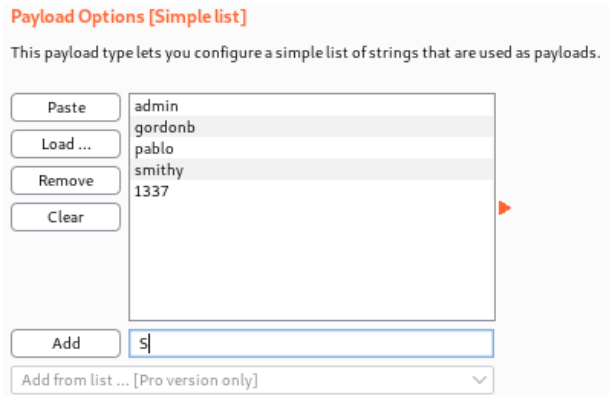
```
GET /vulnerabilities/brute/?username=§admin§&password=§password§&Login=Login HTTP/1.1
Host: localhost§
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/vulnerabilities/brute/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=0vrji2voouk71fb5sjn54k9ore; security=low
Connection: close
```

- Naviguez vers “Payloads” pour déterminer qu’est ce qu’on va remplir ces variables.

  Dans “Payload set” on choisit le “1” (c’est le username car c’est le premier variable rencontrée dans le paquet”.

  Dans “Payload type” on choisit “Simple list” (c’est le type des informations utilisée pour remplir cette variable 1, on choisit Simple List parce que on peut créer une simple liste de 5 noms d’utilisateur, d’une manière manuelle, parce qu'on a trouvé ces cinq utilisateurs dans parti 7 de notre exercice: gordonb pablo smithy 1337.

  Dans “Payload Options”, utilisez “Add” pour ajouter chaque utilisateur ci-dessus, afin d’aboutir à une simple liste.



❑ Pour bien définir le deuxième variable, alors de nouveau, on sélectionne:

Dans "Payload set" on choisit le "2" (c'est le password car c'est la deuxième variable rencontrée dans le paquet".

Dans "Payload type" on choisit "Simple list" (mais ici on va choisir un fichier tout entier qui contient des mots de passe probable).

Dans "Payload Options" choisissez "Load" et naviguer vers `/usr/share/dict/wordlist-probale.txt`.

❑ Commencez l'attaque en appuyant sur "Start Attack" située en haut de la page à droite. Commentez et analysez les résultats.

Vous pouvez faire un tri par longueur du paquet réponse. Les attaques qui ont eu du succès ont une différente longueur de réponse.

❑ Difficulté Medium:

Sélectionnez difficulté medium comme on a fait dans l'étape Ex1-parti 2.

Sélectionnez Brute Force, et remarquez à la fin de la page à droite "View Help". Lisez le contenu et notez le changement dans le paragraphe "Medium Level".

Vous pouvez refaire l'exercice dans cette difficulté et remarquer les changements.

❑ Partie supplémentaire:

Burp Suite n'est pas le seul outil, ni la seule méthode, je vous invite à rechercher "wfuzz" et "hydra" qui sont déjà présents dans le terminal dans Kali. Une simple lecture du manuel va vous permettre d'y utiliser. L'importance de ces outils est parfois la vitesse dans l'exécution.