

Guide d'attaque web par force brute en utilisant Burp Suite

Introduction :

Attaque Web par Force Brute :

Une attaque par force brute est une méthode d'attaque informatique où un attaquant tente de déchiffrer un mot de passe ou une clé en essayant toutes les combinaisons possibles jusqu'à ce qu'il trouve la bonne. Dans le contexte des applications web, une attaque par force brute implique généralement des tentatives répétées de connexion en utilisant différentes combinaisons de noms d'utilisateur et de mots de passe pour accéder à un compte.

Burp Suite :

Burp Suite est une suite d'outils de test de sécurité des applications web largement utilisée par les professionnels de la sécurité informatique et les testeurs de pénétration. Elle offre une gamme d'outils pour découvrir des vulnérabilités dans les applications web et pour effectuer des tests de sécurité.

Fonctionnalités de Burp Suite :

Les fonctionnalités de Burp Suite comprennent, mais ne se limitent pas à :

- ***Proxy Intercepteur** : Permet de surveiller, intercepter et modifier le trafic entre le navigateur web et le serveur pour analyser les requêtes HTTP/HTTPS.
- **Scanner Automatique** : Identifie automatiquement les vulnérabilités de sécurité, telles que les injections SQL, les failles XSS, les problèmes de sécurité liés aux sessions, etc.
- **Repeater** : Permet de répéter manuellement des requêtes pour tester différents scénarios et analyser les réponses du serveur.
- ***Intruder** : Facilite les attaques automatisées en effectuant des tests d'intrusion, y compris des attaques par force brute, des attaques de dictionnaire et d'autres techniques d'intrusion.
- **Sequencer** : Analyse la qualité de l'entropie des sessions, en particulier les jetons anti-CSRF, pour évaluer la robustesse des mécanismes de génération de jetons.
- **Spider** : Explore automatiquement les applications web pour cartographier la structure et identifier les points d'entrée potentiels.
- **Decoder** : Permet de décoder et d'encoder différentes formes d'encodage (base64, URL, etc.) pour analyser les données échangées.
- **Comparer** : Facilite la comparaison de deux requêtes ou réponses HTTP pour identifier les différences et les anomalies.
- **Extender** : Permet d'étendre les fonctionnalités de Burp Suite en ajoutant des extensions personnalisées écrites en langage Java.
- **Collaborator** : Facilite la détection des interactions avec des services externes lors des tests de sécurité, en particulier pour identifier les canaux de communication sortants.
- **Dashboard** : Offre une vue d'ensemble des activités de test en cours, y compris les résultats des scans et des intrusions.
- **Target** : Gère et organise les cibles des tests de sécurité, en aidant à la navigation dans les sites web testés.
- **Project Options** : Permet de configurer des options spécifiques au projet, telles que les paramètres du proxy, les règles de séquençage, etc.
- **Logger** : Enregistre les détails des requêtes et réponses, ainsi que d'autres informations pertinentes, pour un examen ultérieur.

*: Les fonctionnalités qu'on va utiliser pour notre attaque.

Relation entre Attaque par Force Brute et Burp Suite :

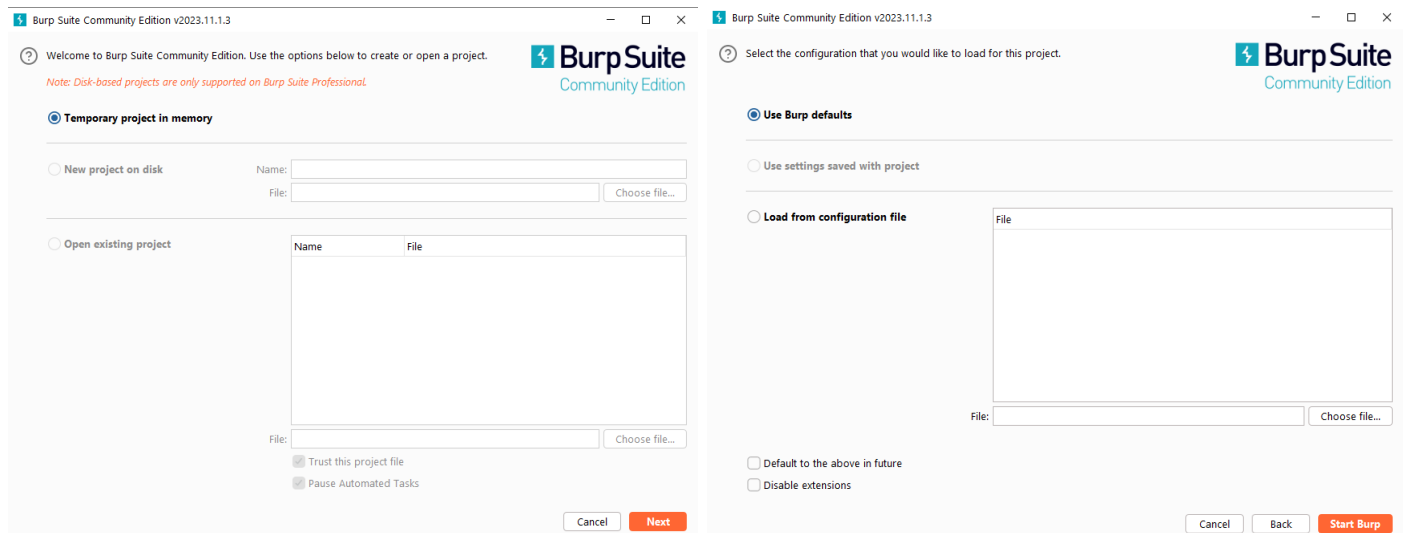
Burp Suite peut être utilisé pour effectuer des attaques par force brute grâce à son module "Intruder". L'outil Intruder de Burp Suite permet de tester la sécurité d'une application web en automatisant des attaques sur différents paramètres de requêtes, notamment les formulaires d'authentification. Cela inclut des attaques par force brute où différentes combinaisons de noms d'utilisateur et de mots de passe sont essayées pour tenter d'accéder à un compte. Cependant, il est important de noter que l'utilisation de Burp Suite à des fins d'attaque doit être effectuée légalement et éthiquement, avec l'autorisation appropriée des propriétaires de l'application testée.

Etapes de l'attaque :

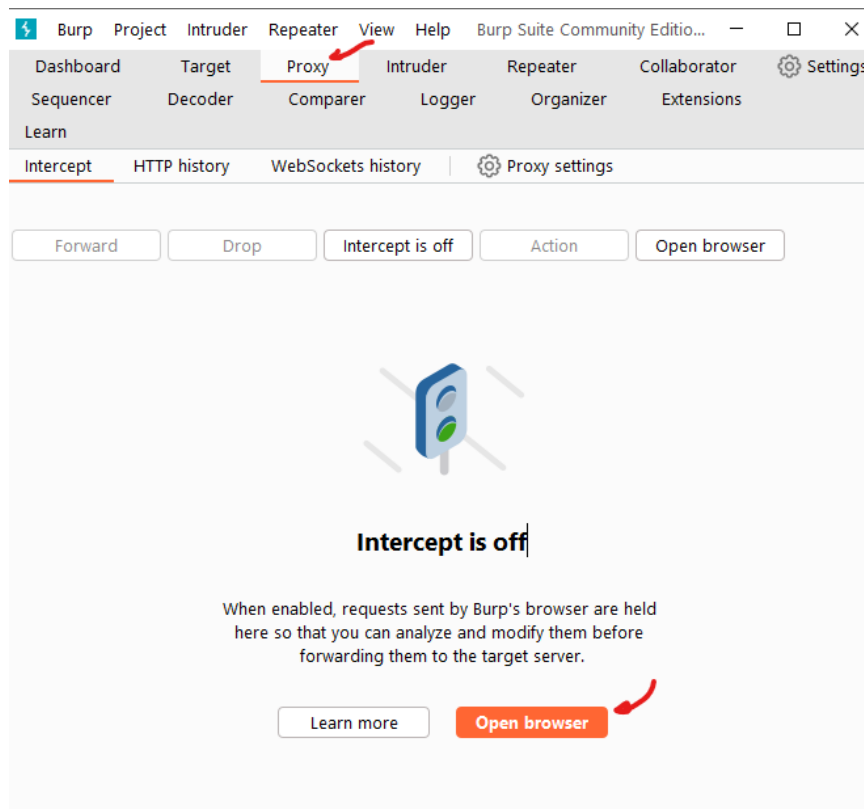
Installer Burpsuite sous Kali linux ou sous windows selon votre environnement de travail lien :

<https://portswigger.net/burp> (installation simple)

Ouvrez burp suite puis cliquez sur next et puis start burp suite



Allez sur Proxy



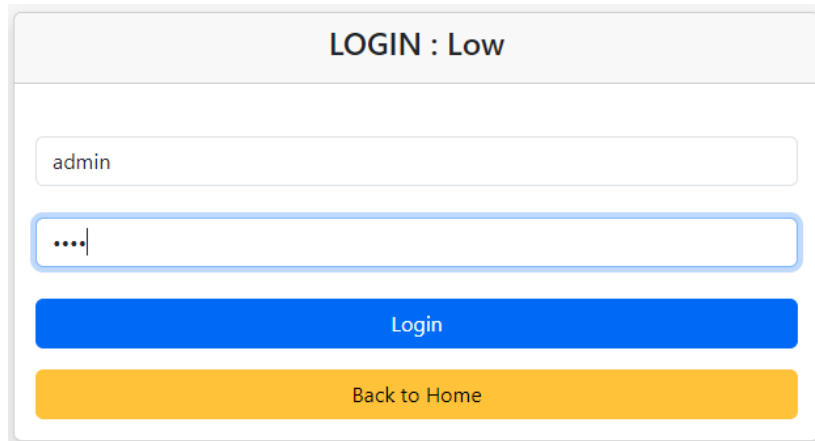
Pour surveiller, intercepter et modifier le trafic entre le navigateur web et le serveur pour analyser les requêtes HTTP/HTTPS, il faut ajouter un proxy (Un serveur proxy est un ordinateur qui intercepte et gère le trafic entre deux appareils, réseaux ou protocoles) (ceci peut être fait soi en configurant votre navigateur manuellement ou par l'ajout

d'une extension qui fera cela comme FOXYPROXY les paramètres à modifier (Nom du proxy : Burp Proxy Type : http IP : 127.0.0.1 Port : 8080))

Mais pour nous simplifier la tâche on utilisera le navigateur intégré dans burp suite

Cliquez open browser

Allez sur : http://localhost/ensab_v2/bruteForce/auth/low/login.php

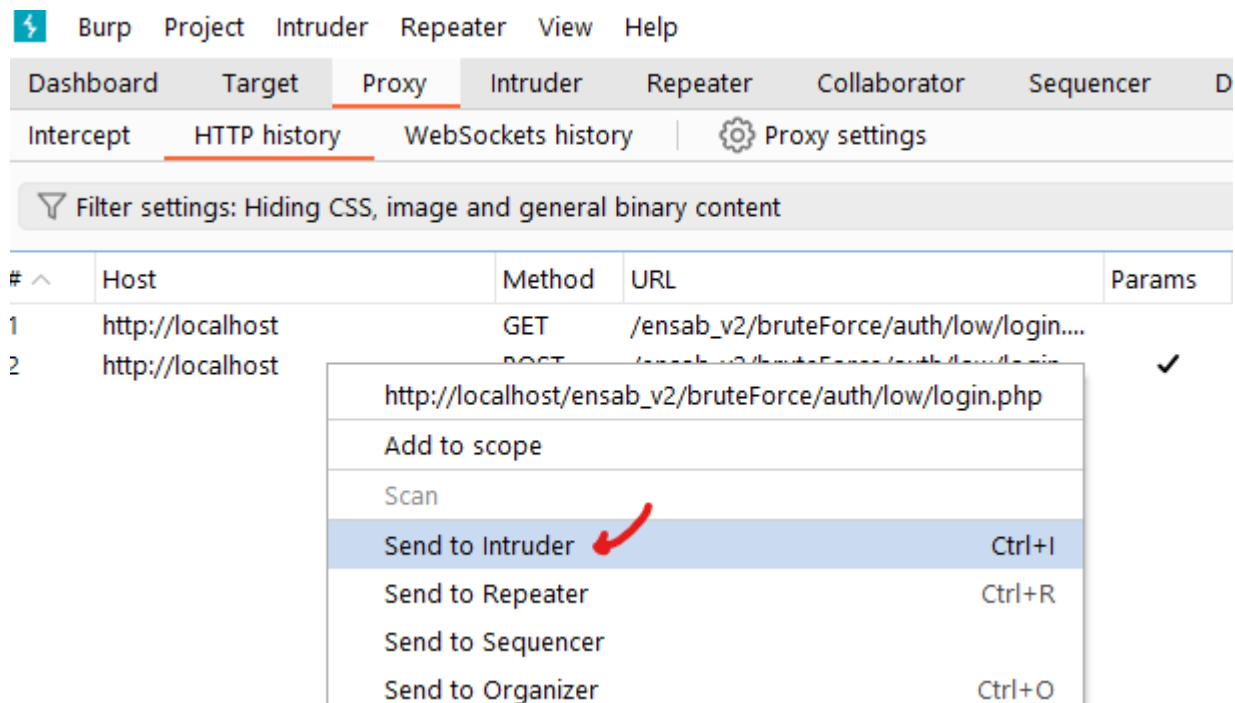


Entrez un utilisateur valide (peut être connue à l'aide de social engineering)

Et n'importe quel mot de passe

Appuyez sur login et revenez sur Burp suite

Allez sur "http history" rechercher la dernière requête faite et envoyez-la au "intruder" pour intercepter la requête et sa réponse



Sélectionner security, phpsession et la valeur du "username" cliquez "clear" pour ne pas les prendre en considération par l'intruder lors des tentatives de test des mots de passe possibles.

Sectionnez le mot de passe que vous avez saisi avant dans mon cas c'était test puis cliquez "add"

AttackSaveColumns

2. Intruder attack of http://localhost - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request ^	Payload	Status code	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	2705	
1	password123	200	<input type="checkbox"/>	<input type="checkbox"/>	2705	
2	password	302	<input type="checkbox"/>	<input type="checkbox"/>	2552	
3	qwerty	302	<input type="checkbox"/>	<input type="checkbox"/>	386	
4	123456789	302	<input type="checkbox"/>	<input type="checkbox"/>	386	
5	111111	302	<input type="checkbox"/>	<input type="checkbox"/>	386	
6	1234567	302	<input type="checkbox"/>	<input type="checkbox"/>	386	
7	dragon	302	<input type="checkbox"/>	<input type="checkbox"/>	386	

RequestResponse

PrettyRawHexRender

16<head>

17<meta charset="UTF-8">

18<meta name="viewport" content="width=device-width, initial-scale=1.0">

19<title>Brute Force | Low</title>

20<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-T3c6CoIi6uLrA9TneNEoa7RxnatzjcDSCmG1MXxSR1GAsXEV/Dwwykc2MPK8M2HN" crossorigin="anonymous">

21<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/js/bootstrap.bundle.min.js" integrity="sha384-C6RzsynM9kWDrMNbT87bh95OGNyZPhcTNXj1NW7RuBCsyN/o0JlpcV8Qyq46cDfL" crossorigin="anonymous"></script>

22<link rel="stylesheet" href="../../assets/css/style.css">

23</head>

24<body>

25<section class="mt-100">

26<div class="container-fluid">

27<div class="col-md-12">

28<div class="row">

29<div class="col-md-4 offset-md-4">

30<div class="card shadow">

31<div class="card-header">

32<h4 class="text-center">LOGIN : Low</h4>

33</div>

34</div>

Search

0 highlights

Finished

ici il faut remarquer les mots de passe avec code de statut ou plutôt le lenght différent et allez sur la réponse de cette requête puis Raw et vérifier si la réponse fourni le code de la page suivant si c'est le cas c'est bien le mot de passe correct (à vérifier)

Approche 2 ne marche pas bien dans le site ensab v2 mais plutôt sur dvwa

Si vous la première approche vous semble peut longue à faire essayez celle-ci

vous faites les mêmes étapes avant l'approche 1 mais avec dvwa/Brute Force attack n'oubliez pas de faire le niveau de sécurité à low puis vous allez sur Brute Force

InstructionsSetup / Reset DB

Brute ForceCommand InjectionCSRFFile InclusionFile UploadInsecure CAPTCHASQL InjectionSQL Injection (Blind)Weak Session IDsXSS (DOM)XSS (Reflected)XSS (Stored)CSP BypassJavaScriptAuthorisation BypassOpen HTTP Redirect

DVWA SecurityPHP InfoAbout

Security Level

Security level is currently: low.

You can set the security level to low, medium or high.

1. Low - This security level is con as an example of how web app as a platform to teach or learn

2. Medium - This setting is mainly developer has tried but failed t exploitation techniques

3. High - This option is an extens practices to attempt to secure exploitation, similar in various

4. Impossible - This level should source code to the secure sou Prior to DVWA v1.9, this level

LowSubmit

Security level set to low

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

Login

Username:

Password:

Login

Username and/or password incorrect.

Allez sur settings ici vous indiquez la condition de non validation du mot de passe qui est le message d'erreur en cas d'un mot de passe invalide

Dans notre cas "Username or password incorrect"

Positions

Payloads

Resource pool

Settings

Attack results

These settings control what information is captured in attack results.

☒ Store requests

☒ Store responses

☒ Make unmodified baseline request

☐ Use denial-of-service mode (no results)

☐ Store full payloads

Grep - Match

These settings can be used to flag result items containing specified expressions:

Paste

Load ...

Remove

Clear

Username and/or password incorrect.

Add

Username and/or password incorrect. ✓

Match type: ☒ Simple string ☐ Regex

☐ Case sensitive match

☒ Exclude HTTP headers

Cliquez sur Clear puis ajouter votre message d'erreur

Cochez "flag result..." pour marquer les mots de passe non valide et puis le mot de passe valide est celui qui n'est pas marqué.

Puis lancez l'attaque

AttackSaveColumns3. Intruder attack of http://localhost - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Username	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4644	1	
1	password123	200	<input type="checkbox"/>	<input type="checkbox"/>	4644	1	
2	password	200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4687	1	
3	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	4644	1	
4	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	4644	1	
5	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	4644	1	
6	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	4644	1	
7	dragon	200	<input type="checkbox"/>	<input type="checkbox"/>	4644	1	

RequestResponse

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Tue, 12 Dec 2023 21:59:58 GMT

3 Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4

4 X-Powered-By: PHP/8.2.4

5 Expires: Tue, 23 Jun 2009 12:00:00 GMT

6 Cache-Control: no-cache, must-revalidate

7 Pragma: no-cache

8 Content-Length: 4333

9 Keep-Alive: timeout=5, max=100

10 Connection: Keep-Alive

11 Content-Type: text/html; charset=utf-8

12

13 <!DOCTYPE html>

14

15 <html lang="en-GB">

16

17 <head>

18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

19

20 <title>

21 Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA)

22 </title>

23

0 highlights

Ressources utiles :

- <https://portswigger.net/burp>
- <https://portswigger.net/support/using-burp-to-brute-force-a-login-page>
- https://www.youtube.com/watch?v=bNLihWA_Ygw
- <https://www.youtube.com/watch?v=-0JKW3U0aU>
- <https://www.youtube.com/watch?v=Gz59MezA3r4>