



En cybersécurité aussi, le savoir n'a de  
valeur que si il est partagé.

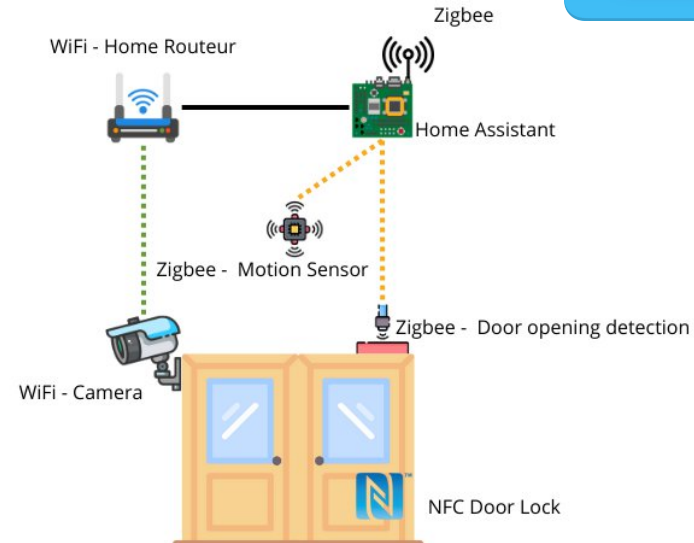
In Cybersecurity too, knowledge only  
increases in value once shared.

## Activité n°2 : Mot de passe faible sur Home Assistant

- Qu'est ce qu'est un serveur Home Assistant ?
  - Centre de contrôle d'une maison connectée
  - Compatible avec de multiples protocoles IoT : WiFi, Zigbee, ...
  - Interface personnalisable pour les besoins de l'utilisateur



- Quelques cas d'usage :
  - Gestion de l'éclairage
  - Régulation du chauffage
  - Automatisation des volets roulants
  - Surveillance et sécurité de l'habitat
  - Automatisation de scènes quotidiennes :
    - Gestion des électro-ménagés
    - Gestion des listes de courses
    - Et bien d'autres !



## Activité n°2 : Mot de passe faible sur Home Assistant

- Qu'est ce qu'est un mot de passe faible ?
  - Mot de passe trop court : moins de 12 caractères
  - Manque de diversité de caractères : uniquement des majuscules ou des minuscules
  - Des mots courants : “password”, “123456”, “abc123”
  - Des informations personnelles : “nom\_du\_chien” + “année\_naissance”
  - Réutilisation d'un même mot de passe pour plusieurs comptes
- Quels sont les risques liés aux mots de passe faibles ?
  - Accès non autorisés à vos comptes personnels
  - Usurpation de votre identité
  - Violation de votre vie privée
- La preuve par l'exemple : découverte du mot de passe par « Brute Force »

## Activité n°2 : Mot de passe faible sur Home Assistant

- Qu'est ce qu'une attaque par « Brute Force »
  - En clair : tester toutes les combinaisons possibles d'un MDP
  - Automatisation des tentatives à l'aide d'outils spécifiques
  - Probabilité de succès dépendante de la force du MDP

- Burpsuite : outil d'analyse des applications Web

- Analyse des vulnérabilités automatiques
- Interception des requêtes HTTP
- Modification de requêtes manuelle
- Repeater pour rejouer les requêtes

- Votre mission si vous l'acceptez :

*Découvrir le mot de passe du serveur HomeAssistant !*

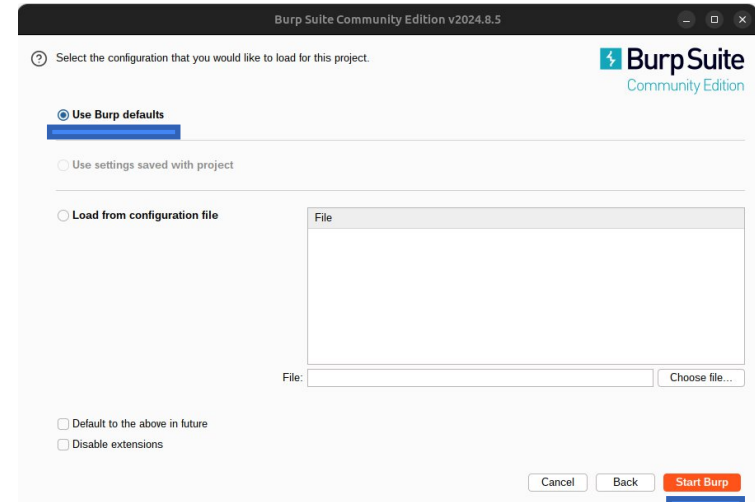
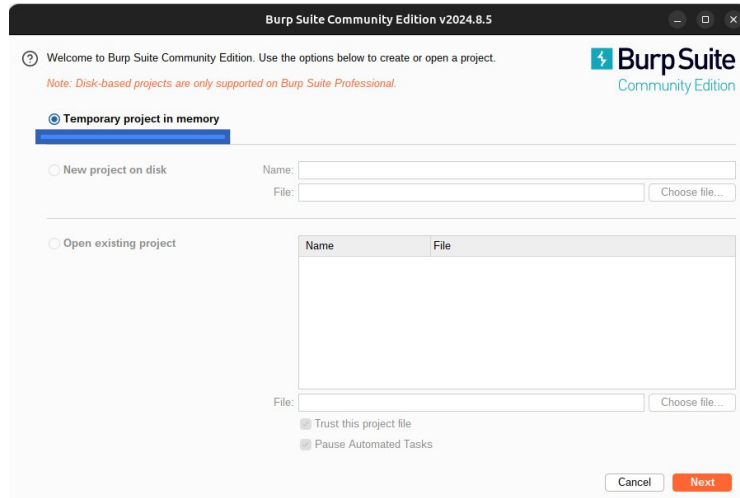


How Long Would It Take To Crack Your Password?

	Lowercase Letters Only	At Least 1 Uppercase Letter	At Least 1 Uppercase Letter + Number	At Least 1 Uppercase Letter + Number + Symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 Minute	6 Minutes
8	Instantly	22 Minutes	1 Hour	8 Hours
9	2 Minutes	19 Hours	3 Days	3 Weeks
10	1 Hour	1 Month	7 Months	5 Years
11	1 Day	5 Years	41 Years	400 Years
12	3 Weeks	300 Years	2,000 Years	34,000 Years
13	1 Year	16,000 Years	100,000 Years	2 Million Years
14	51 Years	800,000 Years	9 Million Years	200 Million Years
15	1,000 Years	43 Million Years	600 Million Years	15 Billion Years
16	34,000 Years	2 Billion Years	37 Billion Years	1 Trillion Years

## Activité n°2 : Mot de passe faible sur Home Assistant

- A vous de jouer !
  - Étape 1 : Ouvrir l'application Burpsuite depuis votre PC :
    - Sélectionnez : « Temporary Project in memory »
    - Sélectionnez : « Use Burp defaults »
    - Cliquez sur « Start Burp »

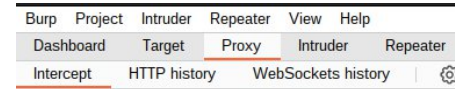


## Activité n°2 : Mot de passe faible sur Home Assistant

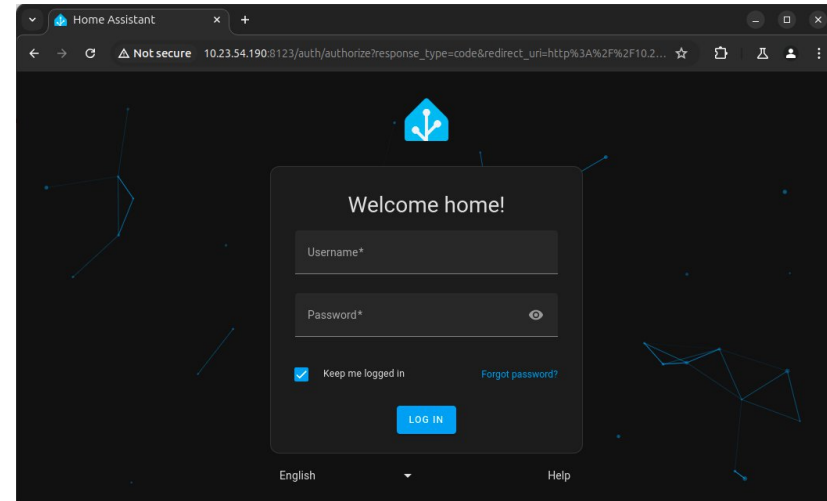
- A vous de jouer !

- Étape 2 : Ouvrez une fenêtre de connexion au serveur HomeAssistant

- Ouvrez le menu « Proxy» en haut à gauche de votre écran :
- Cliquez sur « Open browser »
- Dans la barre de recherche, renseignez l'adresse IP du serveur : <http://@IP:8123>



————— ! Premier point de contrôle ! —————

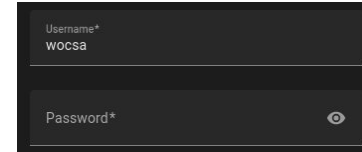


## Activité n°2 : Mot de passe faible sur Home Assistant

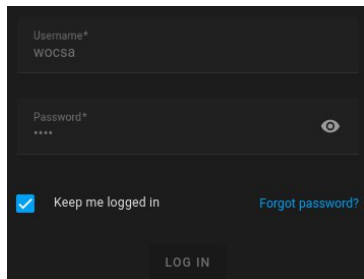
- A vous de jouer !

- Étape 3 : Récupérer de la requête de connexion au serveur Home Assistant

- Nom d'utilisateur : wocsa
- Mot de passe : ???????? —> Tentons de le découvrir !
- Dans Burpsuite, activez « Intercept » en cliquant sur le bouton :




- Retournez dans le browser et tentez d'entrer un mot de passe aléatoire : ex : toto
- Observez la requête de connexion dans Burpsuite :



```

Pretty  Raw  Hex
1 POST /auth/login_flow/b7192bdc70c80bbe95de0a8293322d8 HTTP/1.1
2 Host: 10.23.54.190:8123
3 Content-Length: 78
4 Accept-Language: en-US
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
6 Content-Type: text/plain; charset=UTF-8
7 Accept: */*
8 Origin: http://10.23.54.190:8123
9 Accept-Encoding: gzip, deflate, br
10 Connection: keep-alive
11
12 {
  "username": "wocsa",
  "password": "toto",
  "client_id": "http://10.23.54.190:8123/"
}

```

## Activité n°2 : Mot de passe faible sur Home Assistant

- A vous de jouer !

- Étape 4 : Préparer l'attaque par BruteForce dans Burpsuite

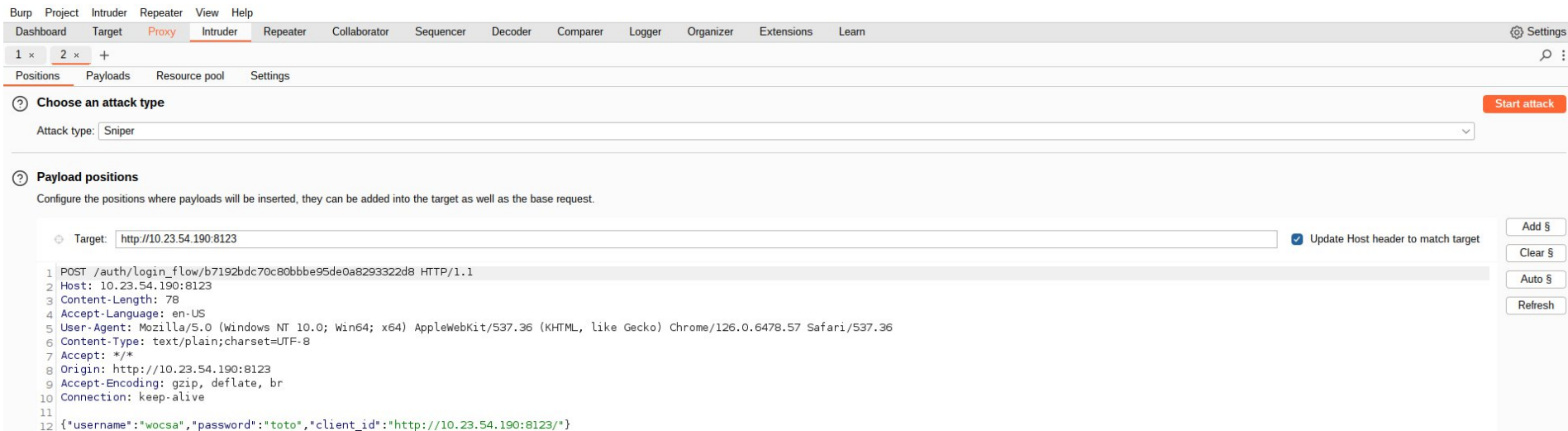
- Dans Burpsuite : Clic droit dans la requête récupérée

- Sélectionnez « Send to Intruder »

Send to Intruder

Ctrl+I

- Rendez-vous dans le menu « Intruder » : retrouvez la requête de connexion :



The screenshot shows the Burp Suite Intruder interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. The main toolbar has buttons for Dashboard, Target, Proxy, Intruder (selected), Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the toolbar, there are tabs for Positions, Payloads, Resource pool, and Settings. The 'Choose an attack type' section shows 'Attack type: Sniper' with a dropdown arrow and a 'Start attack' button. The 'Payload positions' section has a description: 'Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.' The 'Target' field is set to 'http://10.23.54.190:8123' with a checkbox for 'Update Host header to match target'. The request preview shows a POST request to '/auth/login\_flow/b7192bdc70c80bbe95de0a8293322d8' with various headers and a JSON body containing 'username': 'wocsa', 'password': 'toto', and 'client\_id': 'http://10.23.54.190:8123/'. On the right side, there are buttons for 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'.

1 x 2 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.23.54.190:8123

Update Host header to match target

1 POST /auth/login\_flow/b7192bdc70c80bbe95de0a8293322d8 HTTP/1.1

2 Host: 10.23.54.190:8123

3 Content-Length: 78

4 Accept-Language: en-US

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36

6 Content-Type: text/plain; charset=UTF-8

7 Accept: \*/\*

8 Origin: http://10.23.54.190:8123

9 Accept-Encoding: gzip, deflate, br

10 Connection: keep-alive

11

12 {"username": "wocsa", "password": "toto", "client\_id": "http://10.23.54.190:8123/"}

Add \$

Clear \$

Auto \$

Refresh



## Activité n°2 : Mot de passe faible sur Home Assistant


- A vous de jouer !

- Étape 4 : Préparer l'attaque par BruteForce dans Burpsuite

- Remplacez le mot de passe aléatoire toto par les caractères « \$\$ »

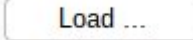
12 {"username":"wocsa","password":"toto","client\_id":"http://10.23.54.190:8123/"}

12 {"username":"wocsa","password":"\$\$","client\_id":"http://10.23.54.190:8123/"}

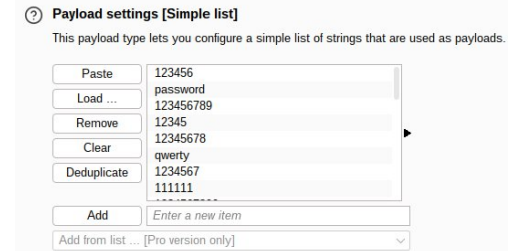
- Astuce : Utilisez le bouton  en haut à droite de votre écran

- Rendez-vous dans le sous-menu « Payload »

- Dans « Payload Settings » :

- Cliquez sur le bouton 
- Sélectionnez le fichier « Weak\_Password\_List.txt » qui se trouve sur votre bureau  
—> Cette liste contient les mots de passe à tester : 30

———— ! Deuxième point de contrôle ! ————



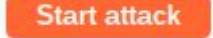
## Activité n°2 : Mot de passe faible sur Home Assistant

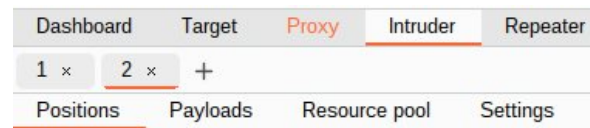
- A vous de jouer !

- Étape 5 : Lancement de l'attaque par BruteForce sur le serveur Home Assistant :

- Retournez dans le menu « Positions » :

- Lancez votre attaque :

- Appuyez sur le bouton 
- Ignorez l'alerte qui se déclenche en cliquant sur le bouton « OK »
- Une nouvelle fenêtre apparaît : observez les mots de passe être testés un à un :
- Intéressez-vous au « Status Code » et au champ « Length »
- Le mot de passe possède le « Status Code » = 200 et une « Length » = 407



Results

Positions

Payloads

Resource pool

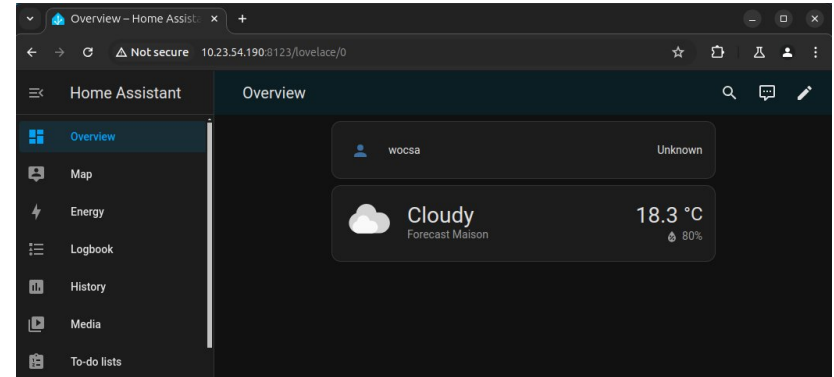
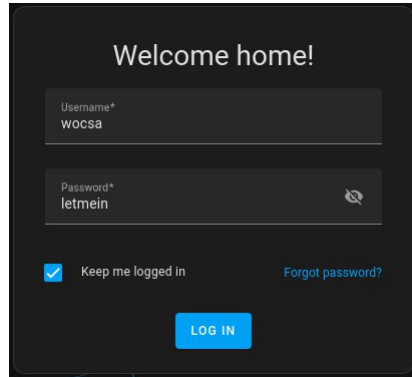
Settings

▼ Intruder attack results filter: Showing all items

Request ^	Payload	Status code	Response received	Error	Timeout	Length
19	dragon	200	1528			538
20	sunshine	200	1444			538
21	princess	200	1588			538
22	letmein	200	1250			407
23	654321	404	21			253
24	monkey	404	29			253
25	27653	404	21			253
26	1qaz2wsx	404	19			253

## Activité n°2 : Mot de passe faible sur Home Assistant

- A vous de jouer !
  - Étape 5 : Tout travail mérite salaire : obtenez votre trophée !
    - Dans le menu « Proxy », cliquez sur **Intercept is on** pour désactiver l'interception
    - Tentez de vous reconnecter au serveur avec le mot de passe trouvé sur le browser !



**Félicitations, vous avez piraté votre premier serveur home assistant !**

## Activité n°2 : Mot de passe faible sur Home Assistant

- Bilan de l'activité : Comment se protéger d'une attaque par BruteForce ?
  - Utiliser des mots de passe fort : majuscules, minuscules, chiffres et caractères spéciaux
    - Exemple : ReeX4eyH3dJq&Cv8t\$QDNvqN%AxUIx^U
  - Utiliser un gestionnaire de mot de passe : la mémoire humaine est limitée !
    - De nombreuses solutions gratuites (et payantes) existent : exemple de Bitwarden
  - Activer l'authentification multi-facteurs (MFA) sur vos comptes personnels et professionnels
    - Code temporaires sur votre smartphone, clefs d'authentification, ...
- Des questions ? Des remarques ? Discutons-en !

