

Fireforce

Guide utilisateur



Table des matières

Fireforce.....	1
Installation.....	3
Logiciel requis.....	3
Récupération de l'exécutable.....	3
Installation.....	3
Utilisation de deux profils Firefox en même temps (optionnel).....	3
Création d'un deuxième profil sur Windows.....	3
Création d'un deuxième profil sur Mac.....	3
Création d'un deuxième profil sur Linux.....	3
Lancement de deux profil en même temps sur Windows.....	3
Lancement de deux profil en même temps sur Mac.....	4
Lancement de deux profil en même temps sur Linux.....	4
Utilisation.....	4
Cas supportés.....	4
Chargement de dictionnaires.....	4
Informations requises pour lancer l'attaque.....	4
Lancement de l'attaque.....	5
Génération de mot de passe.....	6
Informations requises pour lancer l'attaque.....	6
lancement de l'attaque.....	7
Attaque sur deux champs en même temps.....	9
informations requises pour lancer l'attaque.....	9
Lancement de l'attaque.....	10
Aide.....	12

Installation

Logiciel requis

L'extension est compatible avec toutes les versions du navigateur Firefox entre la 1.5 et la 3.5.x.

Récupération de l'exécutable

L'extension est disponible depuis plusieurs sources :

- <http://www.scrt.ch/pages/fireforce/fireforce.xpi>
- <https://addons.mozilla.org/fr/firefox/addon/64765>

Installation

Glisser le fichier « fireforce.xpi » dans votre navigateur et cliquer sur installer.

Utilisation de deux profils Firefox en même temps (optionnel)

Pendant son utilisation, l'extension bloquera votre profil de Firefox. Il est donc conseillé de l'exécuter depuis un profil différent et de lancer les 2 profils en même temps.

Création d'un deuxième profil sur Windows

Exécuter cette commande dans Démarrer > Exécuter.

```
firefox.exe -profilemanager
```

Cliquer ensuite sur « Créer un profil...>

Création d'un deuxième profil sur Mac

Exécuter cette commande dans un terminal.

```
/Applications/firefox.app/Contents/MacOS/firefox -profilemanager
```

Cliquer ensuite sur « Créer un profil...>

Création d'un deuxième profil sur Linux

Exécuter cette commande dans une console.

```
firefox -profilemanager
```

Cliquer ensuite sur « Créer un profil...>

Lancement de deux profil en même temps sur Windows

Exécuter cette commande dans Démarrer > Exécuter (en supposant que dev soit le nom de votre 2^{ème} profil).

```
firefox.exe -P dev -no-remote
```


Lancement de l'attaque

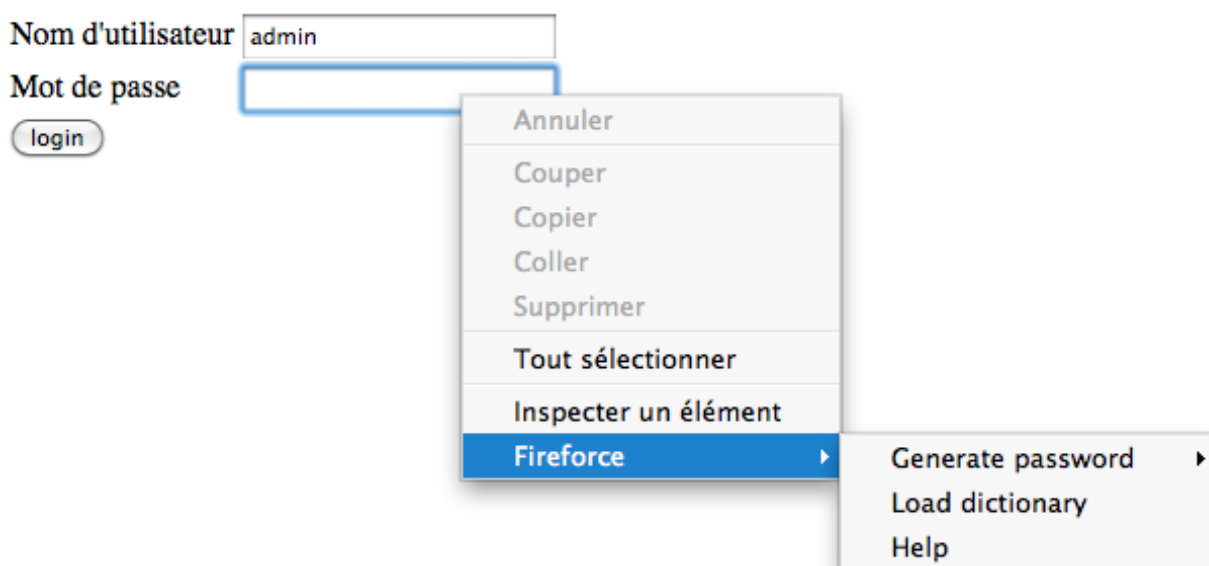
Situation : Nous voulons le mot de passe de l'utilisateur « admin ». Nous chercherons dans le dictionnaire de mot de passe common-passwords.txt.

- Remplir le champ Nom d'utilisateur avec la valeur « admin »

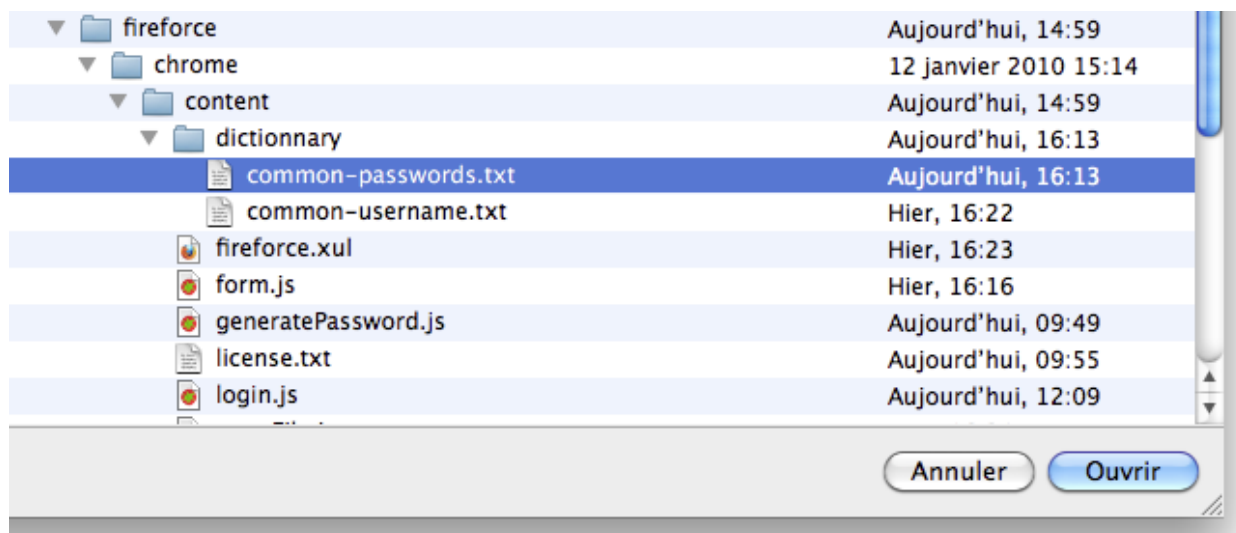
Nom d'utilisateur

Mot de passe

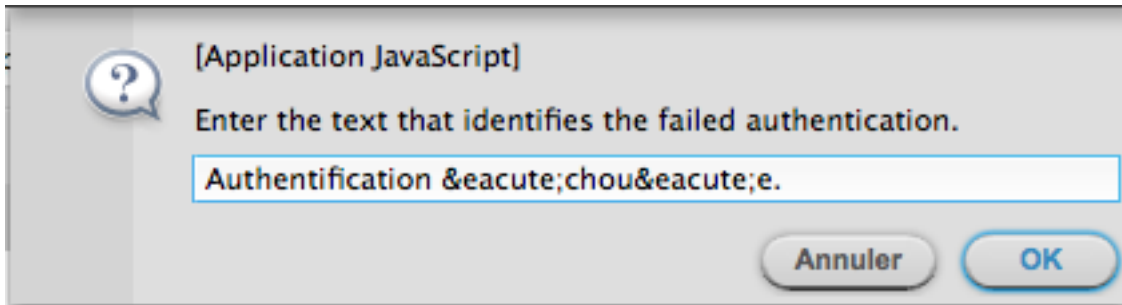
- Faire un clic droit dans le champ Mot de passe et choisir: Fireforce > Load Dictionary



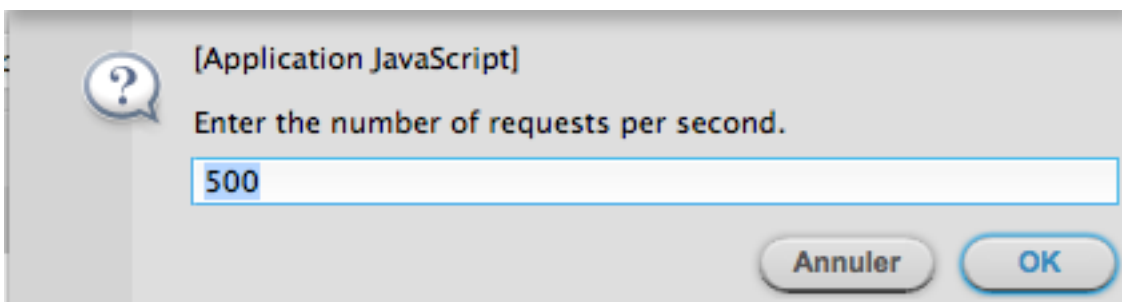
- Choisir le ou les dictionnaires depuis l'explorateur. (Appuyer sur la touche « shift » pour sélectionner plusieurs dictionnaires).



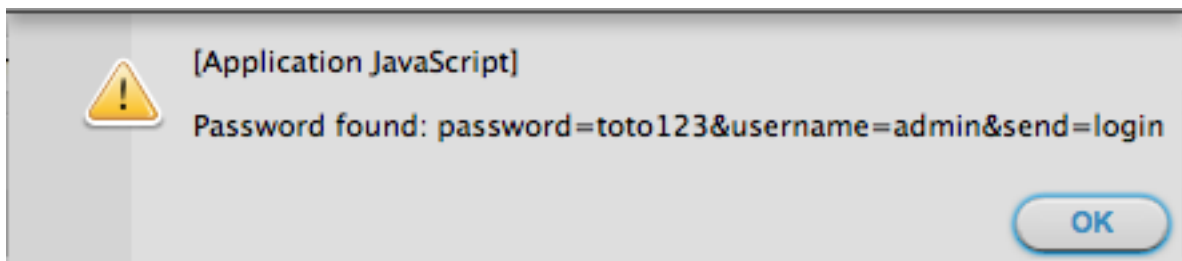
- Entrer le message d'erreur qui identifie une erreur d'authentification.



- Entrer le nombre de requêtes envoyées au serveur.



- Attente du résultat.
Dans notre cas, le mot de passe a été trouvé.



Génération de mot de passe

Informations requises pour lancer l'attaque

- Un message contenu dans la page retournée par le serveur en cas d'échec de l'authentification.

Attention! Dans certain cas, le message affiché à l'écran n'est pas exactement celui codé dans la source de la page (code des accents, etc). Le message doit être celui écrit dans la source de la page et non celui affiché.

Exemple: Le message affiché à l'écran est « Authentification échouée. » alors que le texte dans la source est « Authentification échouée ».

Authentification échouée.

Nom d'utilisateur

Mot de passe

login

```
<tr>
  <td>Authentification échouée.</td>
</tr>
<tr>
  <td>Nom d'utilisateur</td>
  <td>
```

- Le nombre de caractères minimum.
- Le nombre de caractères maximum.
- Le nombre de requêtes envoyées en même temps au serveur.(dépend du temps moyen de réponse du serveur et de la qualité de la connexion. Par défaut ce nombre est de 500).

lancement de l'attaque

Situation : Nous voulons le mot de passe de l'utilisateur « admin ». Nous n'avons pas de dictionnaire alors nous voulons générer les mots de passe. Nous allons essayer les mots de passe en minuscule jusqu'à 4 caractères.

- Remplir le champ Nom d'utilisateur avec la valeur « admin »

Nom d'utilisateur

Mot de passe

login

- Faire un clic droit dans le champ Mot de passe et choisir: Fireforce > Generate Password > a-z

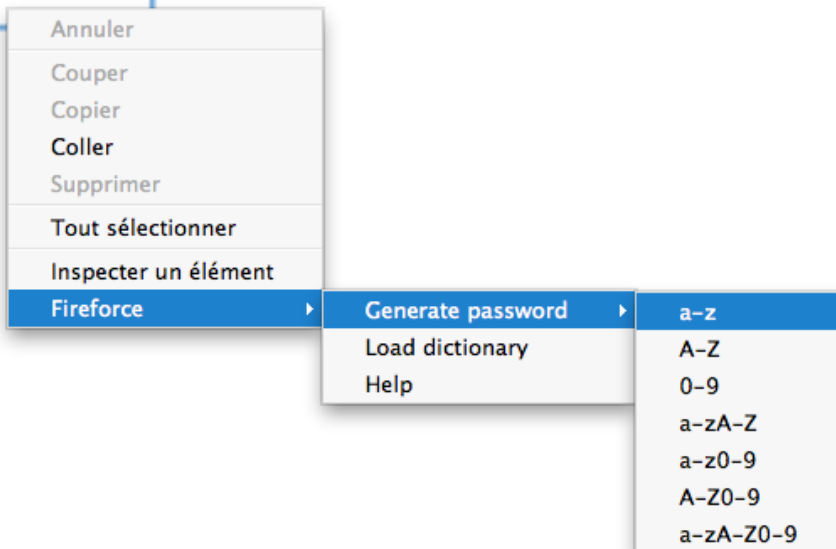
Nom d'utilisateur

admin

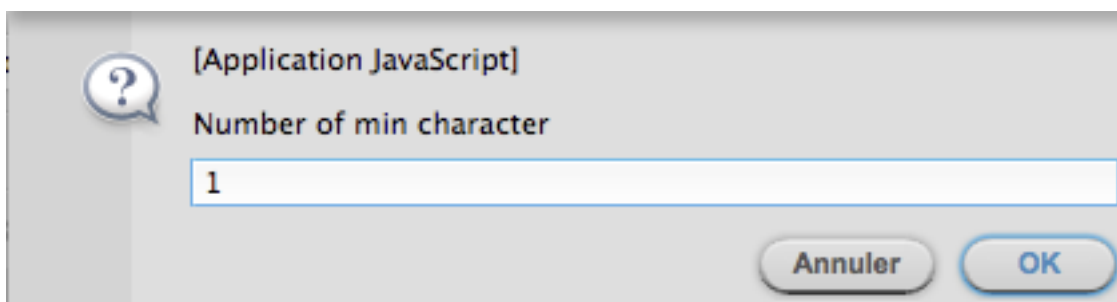
Mot de passe

|

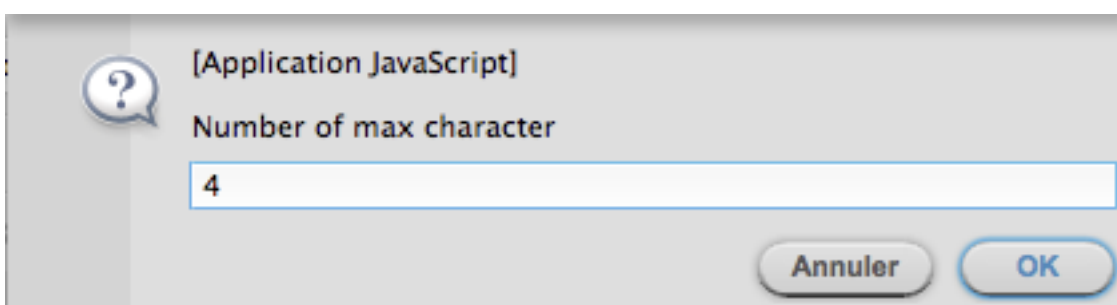
login



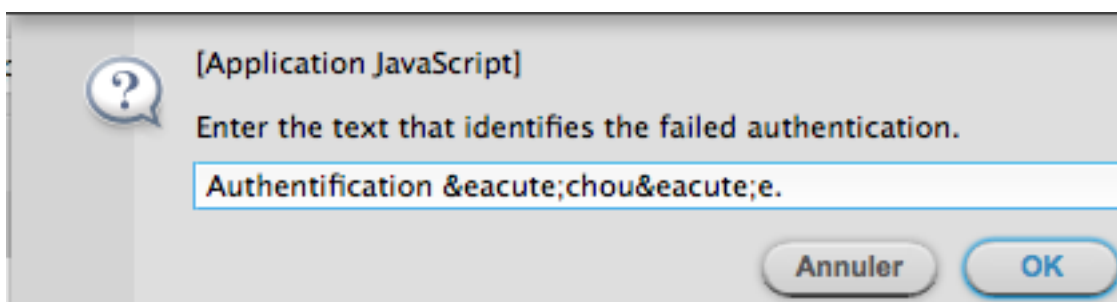
- Entrer la longueur minimale.(1)



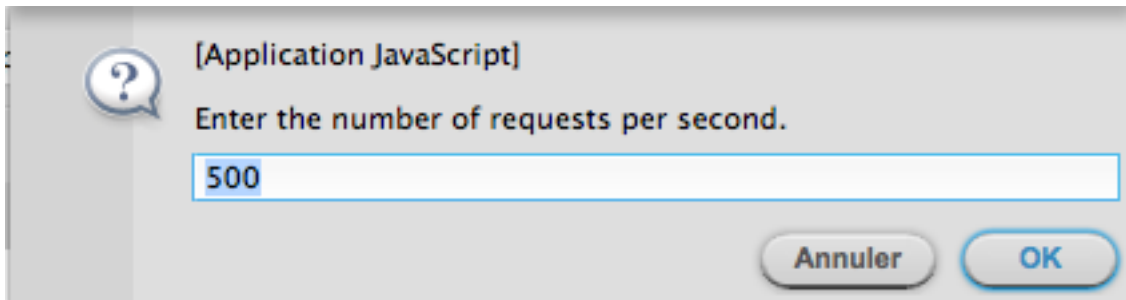
- Entrer la longueur maximale.(4)



- Entrer le message d'erreur qui identifie une erreur d'authentification.

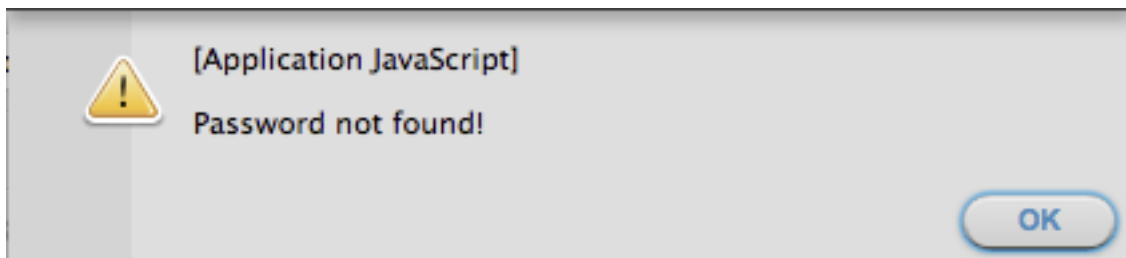


- Entrer le nombre de requêtes envoyées au serveur.



- Attente du résultat.

Dans notre cas, aucun mot de passe n'a été trouvé.



Attaque sur deux champs en même temps

informations requises pour lancer l'attaque

- Un message contenu dans la page retournée par le serveur en cas d'échec de l'authentification.

Attention! Dans certain cas, le message affiché à l'écran n'est pas exactement celui codé dans la source de la page (code des accents, etc). Le message doit être celui écrit dans la source de la page et non celui affiché.

Exemple: Le message affiché à l'écran est « Authentification échouée. » alors que le texte dans la source est « Authentification échouée. ».

Authentification échouée.

Nom d'utilisateur

Mot de passe

login

```
<tr>
  <td>Authentification échouée.</td>
</tr>
<tr>
  <td>Nom d'utilisateur</td>
  <td>
    ..
  </td>
</tr>
```

- Le nombre de caractères minimum.(si le générateur de mot de passe est utilisé)
- Le nombre de caractères maximum.(si le générateur de mot de passe est utilisé)
- Le nombre de requêtes envoyées en même temps au serveur.(dépend du temps moyen de réponse du serveur et de la qualité de la connexion. Par défaut ce nombre est de 500).

Lancement de l'attaque

Situation : Nous voulons tester une série de noms d'utilisateur avec une série de mots de passe. Les utilisateurs sont dans le fichier common_username.txt et les mots de passe dans le fichier common_passwords.txt.

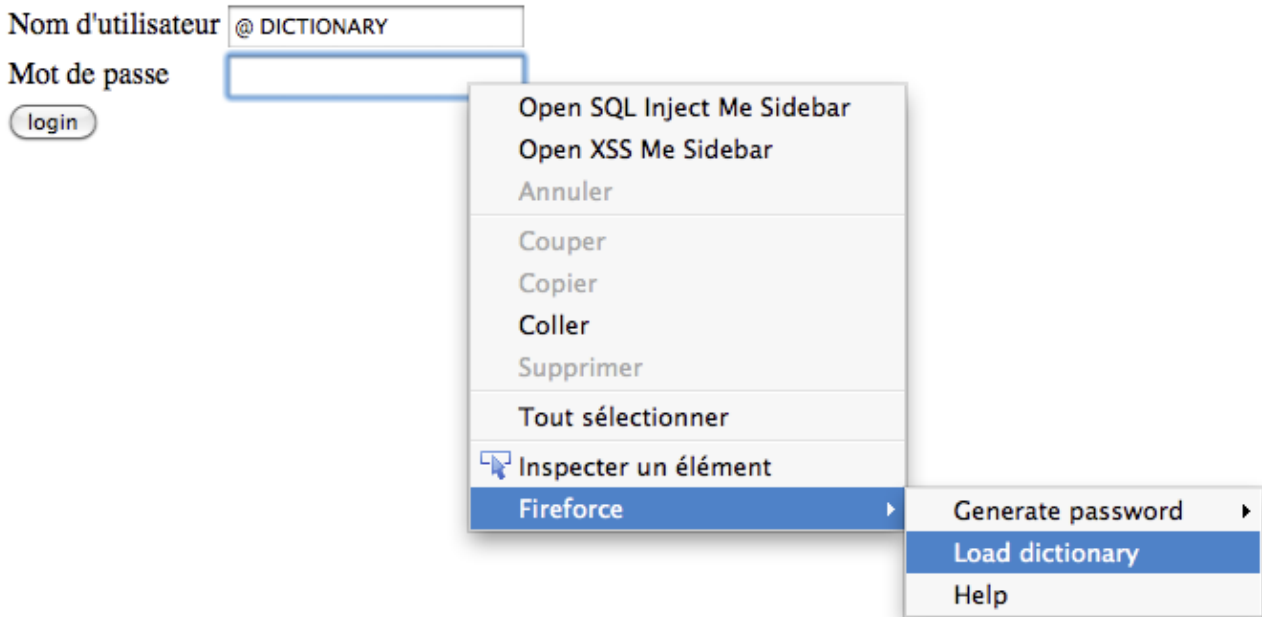
- Remplir le champ Nom d'utilisateur avec la valeur « @ DICTIONARY »

Nom d'utilisateur

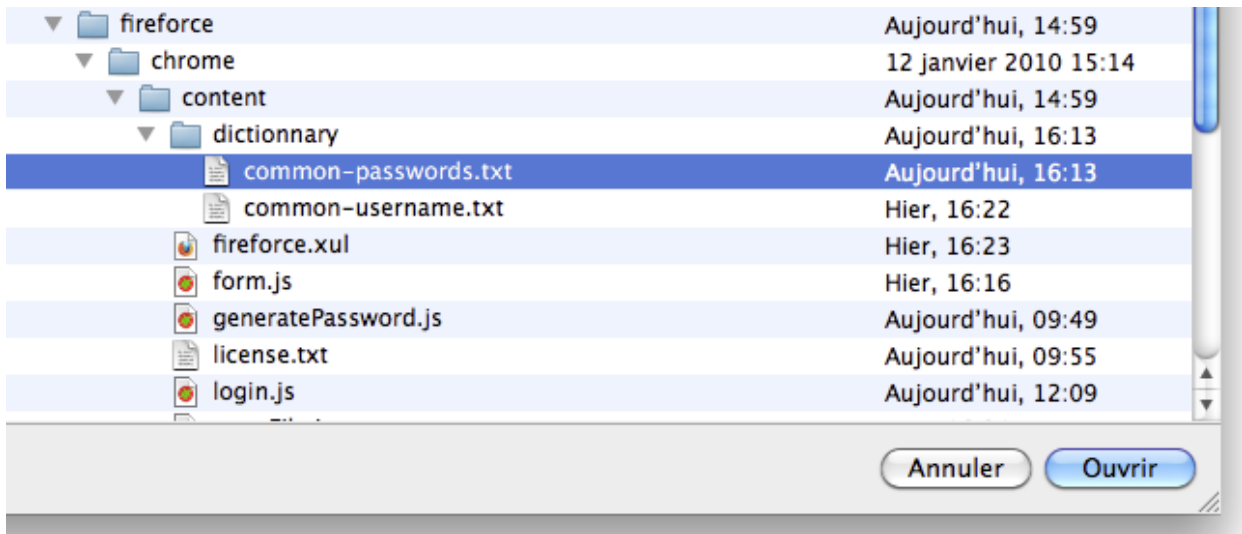
Mot de passe

login

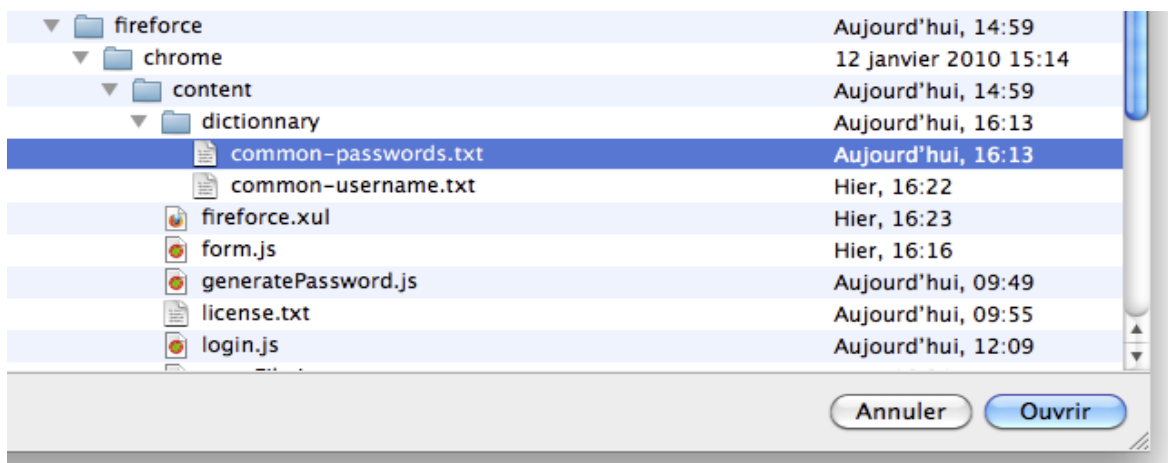
- Faire un clic droit dans le champ Mot de passe et choisir: Fireforce > Load Dictionnary



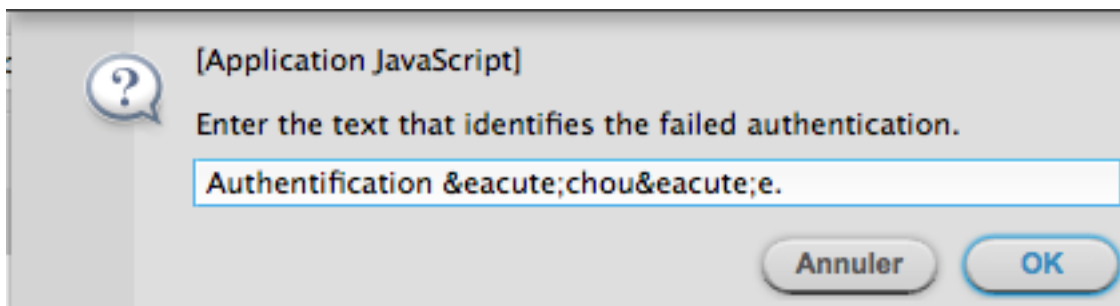
- Choisir le ou les dictionnaires utilisés pour les mots de passe depuis l'explorateur. (Appuyer sur la touche « shift » pour sélectionner plusieurs dictionnaires).



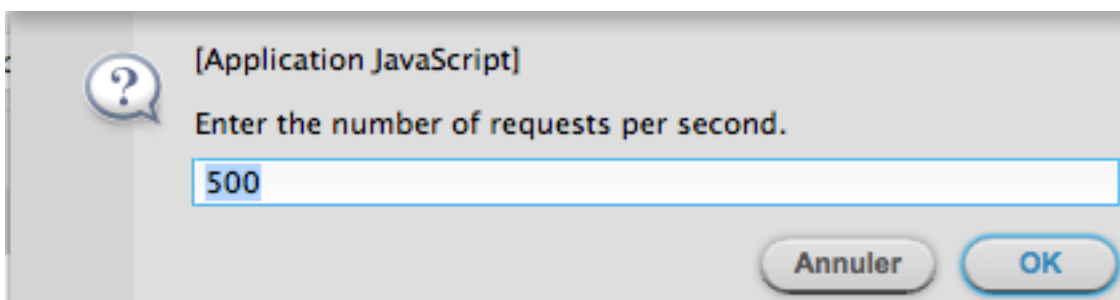
- Choisir le ou les dictionnaires utilisés pour les noms d'utilisateur depuis l'explorateur. (Appuyer sur la touche « shift » pour sélectionner plusieurs dictionnaires).



- Entrer le message d'erreur qui identifie une erreur d'authentification.



- Entrer le nombre de requêtes envoyées au serveur.



- Attente du résultat.

Le champ qui contient le valeur « @ DICTIONARY » peut uniquement être testé avec un dictionnaire. Il n'est donc pas possible de faire une attaque en générant les noms d'utilisateur et les mots de passe.

Aide

Pour obtenir de l'aide, faire un clic droit et choisir Help. Une redirection sera faite sur la page de présentation de l'extension sur le site web de la société SCRT. Il est possible de télécharger les mises à jour et les guides d'installation depuis cette page.