

Fireforce

User Manual



Table of Contents

Fireforce.....	1
Installation.....	3
Required Software.....	3
Recovery of the executable.....	3
Installation.....	3
Using two Firefox profiles simultaneously (optional).....	3
Creating a second profile on Windows.....	3
Creating a second profile on Mac.....	3
Creating a second profile on Linux.....	3
Launch of two profile at the same time on Windows.....	3
Launch of two profiles simultaneously on Mac.....	3
Launch of two profile at the same time on Linux.....	4
Use.....	4
Case incurred.....	4
Loading dictionaries.....	4
Information required to launch the attack.....	4
Launching the attack.....	4
Generate Password.....	6
Information required to launch the attack.....	6
Launching the attack.....	6
Attack on two fields at the same time.....	8
Information required to launch the attack.....	8
Launching the attack.....	9
Help.....	10

Installation

Required Software

The extension is compatible with all versions of the Firefox browser between 1.5 and the 3.5.x.

Recovery of the executable

The extension is available from several sources:

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

Installation

Drag the file "fireforce.xpi in your browser and click on install.

Using two Firefox profiles simultaneously (optional)

During use, the extension will block your Firefox profile. It is therefore advisable to run it from a different profile and launch the 2 profiles at the same time.

Creating a second profile on Windows

Run this command from Start> Run.

```
firefox.exe -profilemanager
```

Then click on "Create Profile ..."

Creating a second profile on Mac

Run this command in a terminal.

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

Then click on "Create Profile ..."

Creating a second profile on Linux

Run this command in a console.

```
firefox -profilemanager
```

Then click on "Create Profile ..."

Launch of two profile at the same time on Windows

Run this command in Start> Run (assuming that dev is the name of your 2nd profile).

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

Launch of two profiles simultaneously on Mac

Run this command in a terminal (assuming that dev is the name of your 2nd profile).

```
/Applications/Firefox.app/Contents/MacOS/firefox-bin -P dev -no-remote
```

Launch of two profile at the same time on Linux

Run this command in a console. (Assuming that dev is the name of your 2nd profile)

```
firefox -P dev -no-remote
```

You can now install and use the extension in a second profile to avoid the first one from being blocked.

Use

Case incurred

The extension runs out attacks on form fields sent by POST or GET to the server.

The page can not be protected by an anti-brute force (blocking ip after n false passwords, captcha, etc. ...)

Loading dictionaries

Information required to launch the attack

A message returned by the page to indicate a failed authentication.

Warning! In some cases, the message displayed on the screen is not the same as in the source of the page (code accents, etc.). The message that must be written is the one found in the page source and not necessarily the one displayed by the browser.

- The number of requests sent simultaneously to the server. (Depends on the average response time of server and connection quality. By default this number is 500).

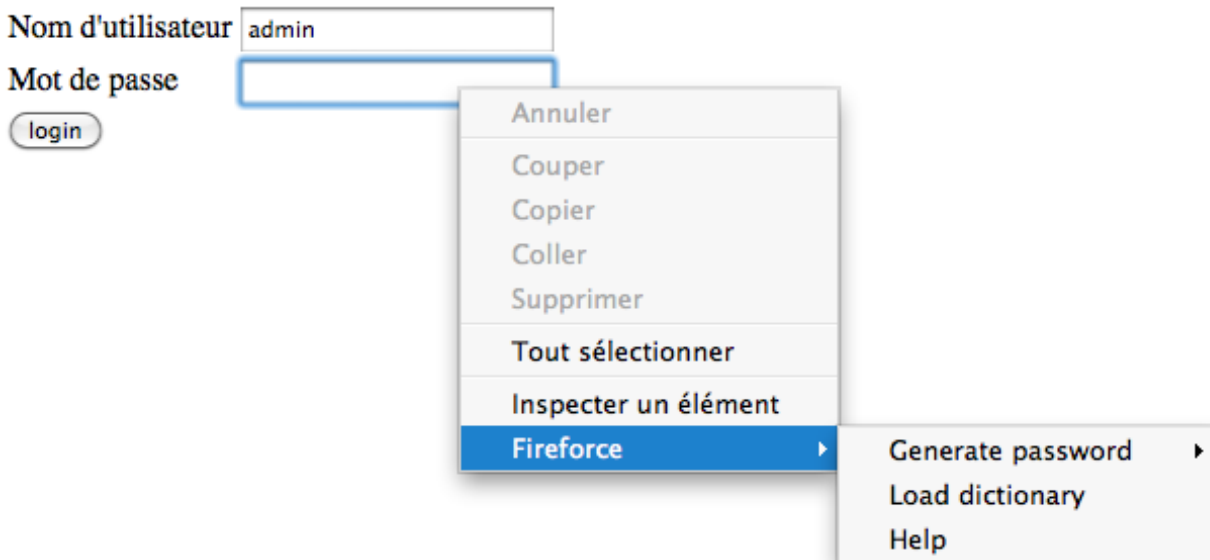
Launching the attack

Example: We want the password for user "admin". We look in the dictionary of common password-passwords.txt.

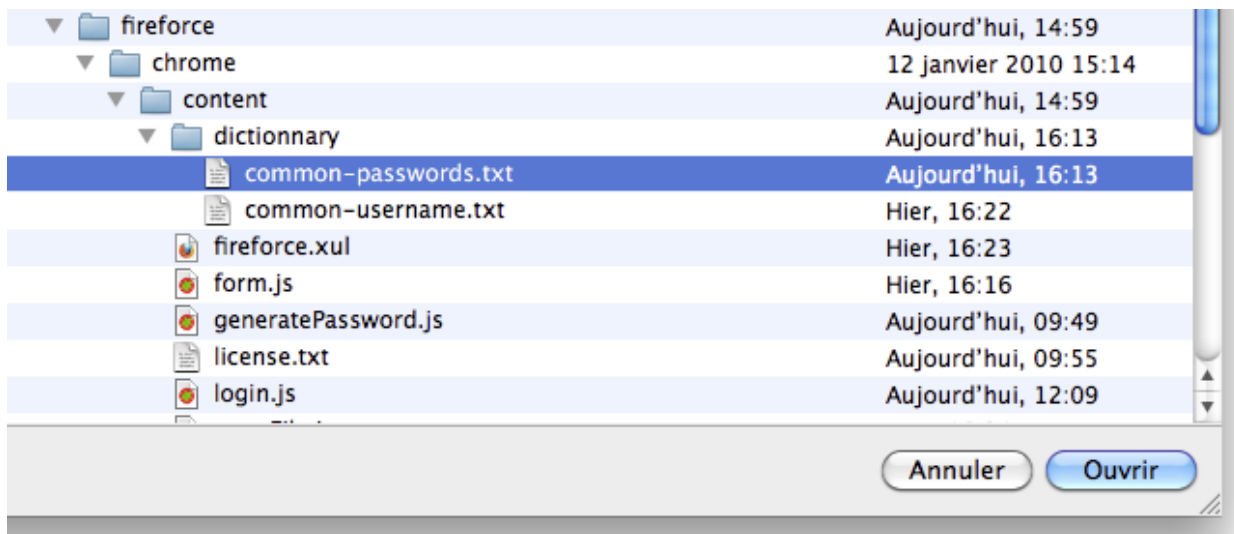
- Complete the Username field with the value "admin"

Nom d'utilisateur	<input type="text" value="admin"/>
Mot de passe	<input type="password"/>
<input type="button" value="login"/>	

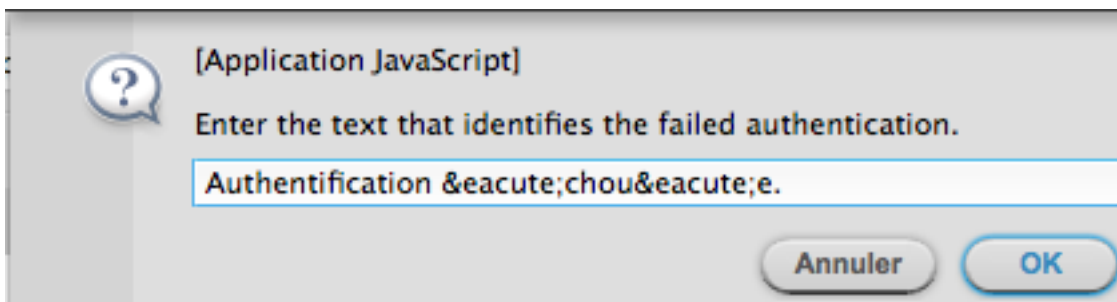
- Right click in the Password field and select: Fireforce> Load Dictionary



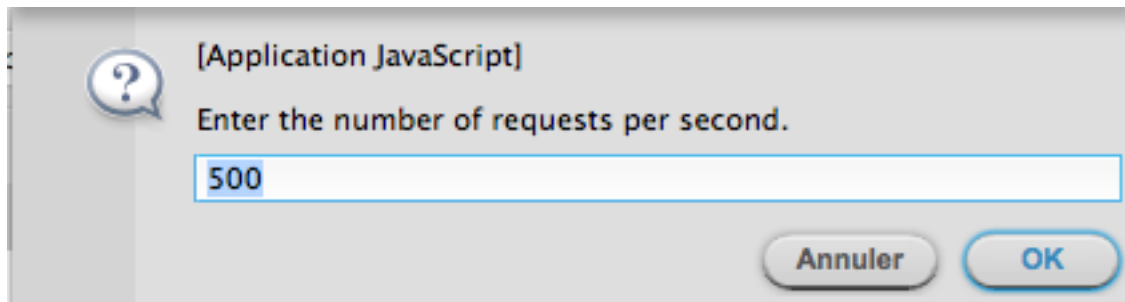
- Choose the dictionary from the explorer. (Press the "shift" key to select multiple dictionaries).



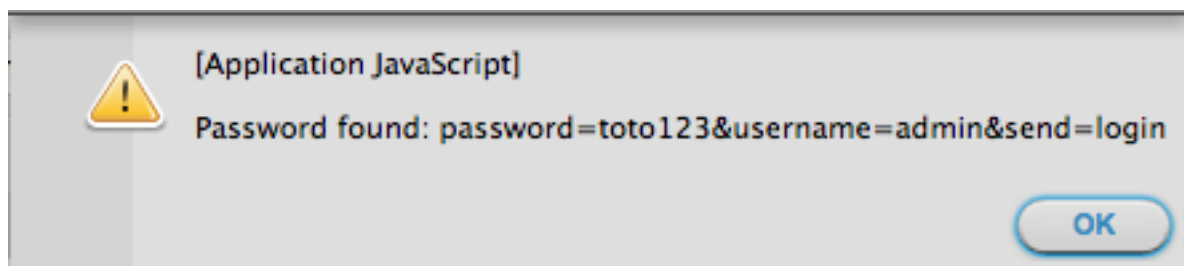
- Enter the text that identifies the failed authentication.



- Enter the number of requests sent to the server.



- Pending the results.
In our case, the password has been found.



Generate Password

Information required to launch the attack

A message returned by the page to indicate a failed authentication.

Warning! In some cases, the message displayed on the screen is not the same as in the source of the page (code accents, etc.). The message that must be written is the one found in the page source and not necessarily the one displayed by the browser.

- The number of requests sent simultaneously to the server. (Depends on the average response time of server and connection quality. By default this number is 500).
- The minimum number of characters.
- The maximum number of characters.

Launching the attack

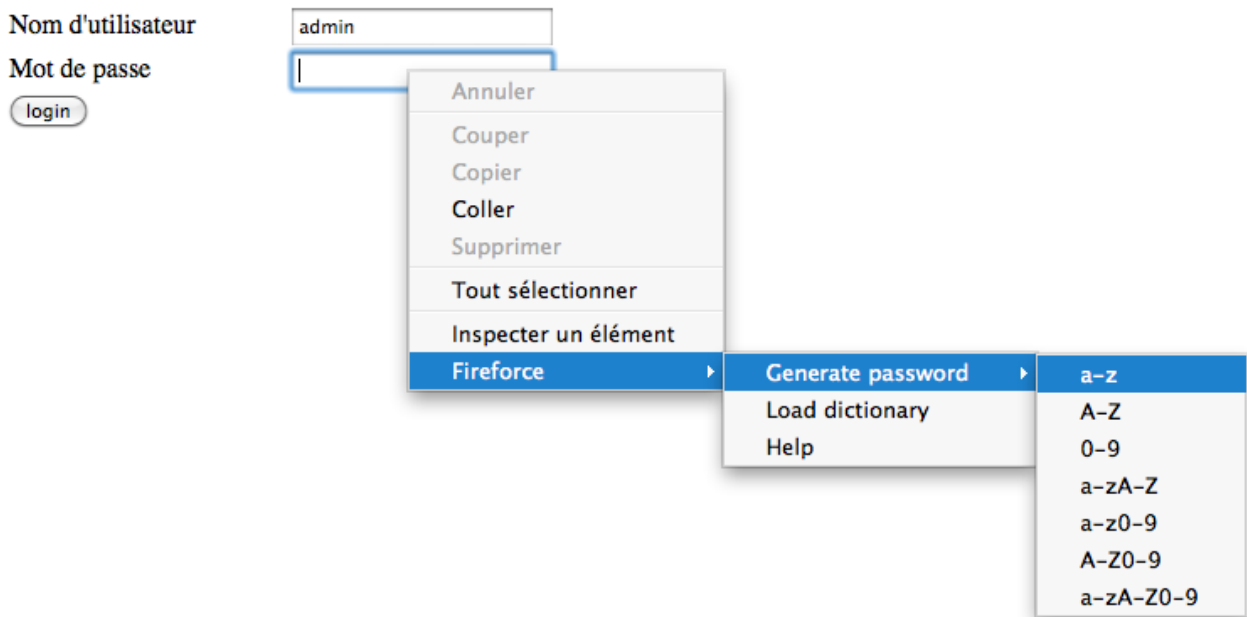
Example: We want the password for user "admin". We do not have a dictionary so we want to generate passwords. We will try passwords up to 4 lowercase characters.

- Complete the Username field with the value "admin"

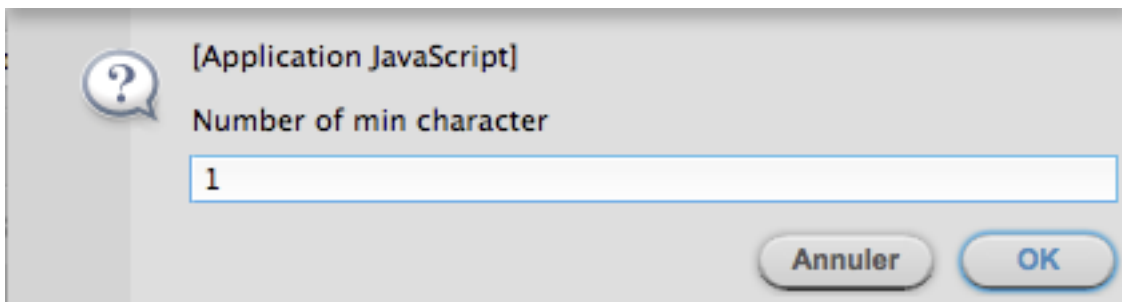
Nom d'utilisateur

Mot de passe

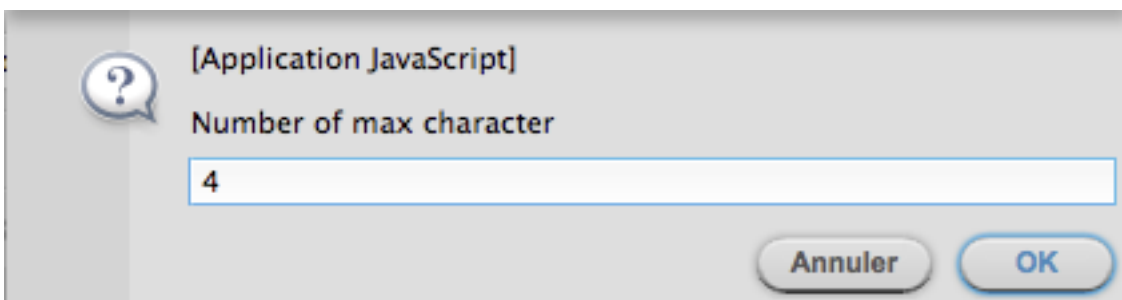
- Right click in the Password field and select: Fireforce> Generate Password > a-z



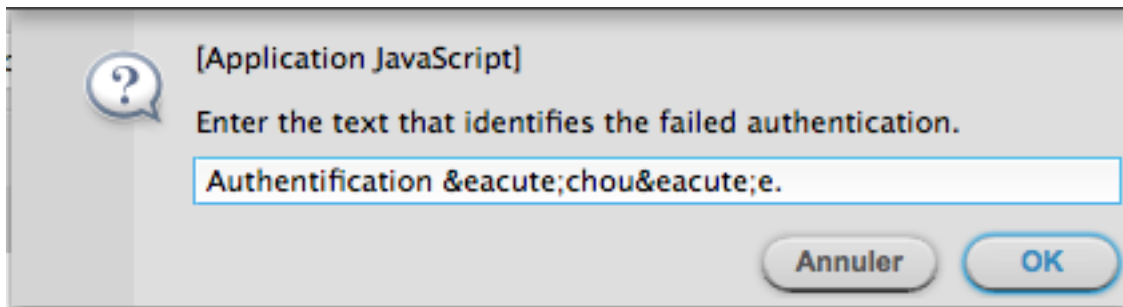
- Enter the minimum length. (1)



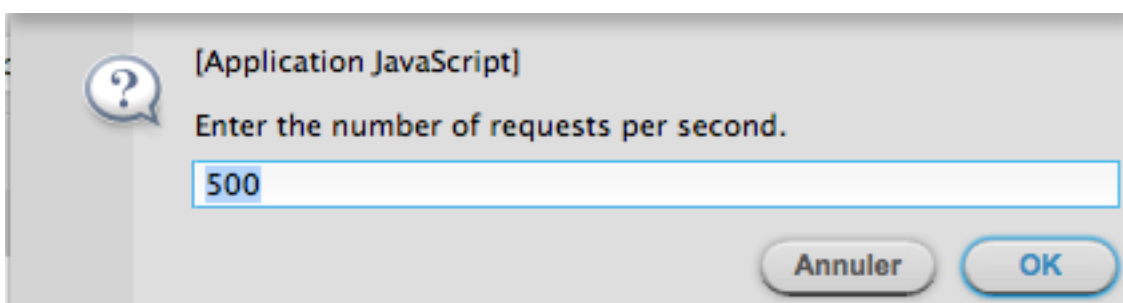
- Enter the maximum length. (4)



- Enter the text that identifies the failed authentication.

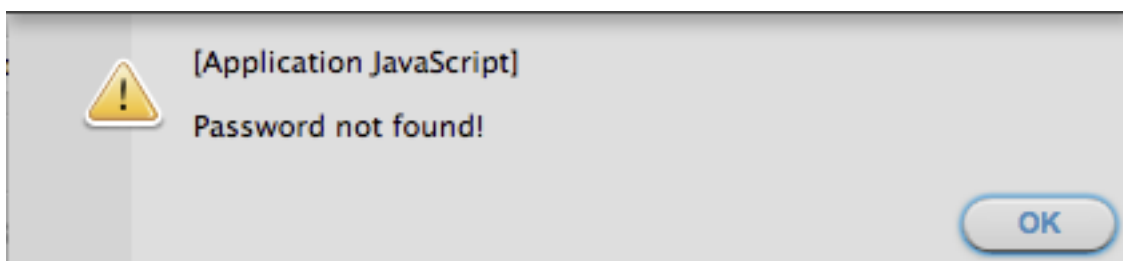


- Enter the number of requests sent to the server.



- Pending the results.

In our case, no password has been found.



Attack on two fields at the same time

Information required to launch the attack

A message returned by the page to indicate a failed authentication.

Warning! In some cases, the message displayed on the screen is not the same as in the source of the page (code accents, etc.). The message that must be written is the one found in the page source and not necessarily the one displayed by the browser.

- The number of requests sent simultaneously to the server. (Depends on the average response time of server and connection quality. By default this number is 500).
- The minimum number of characters. (If the generator password is used)
- The maximum number of characters. (If the generator password is used)

Launching the attack

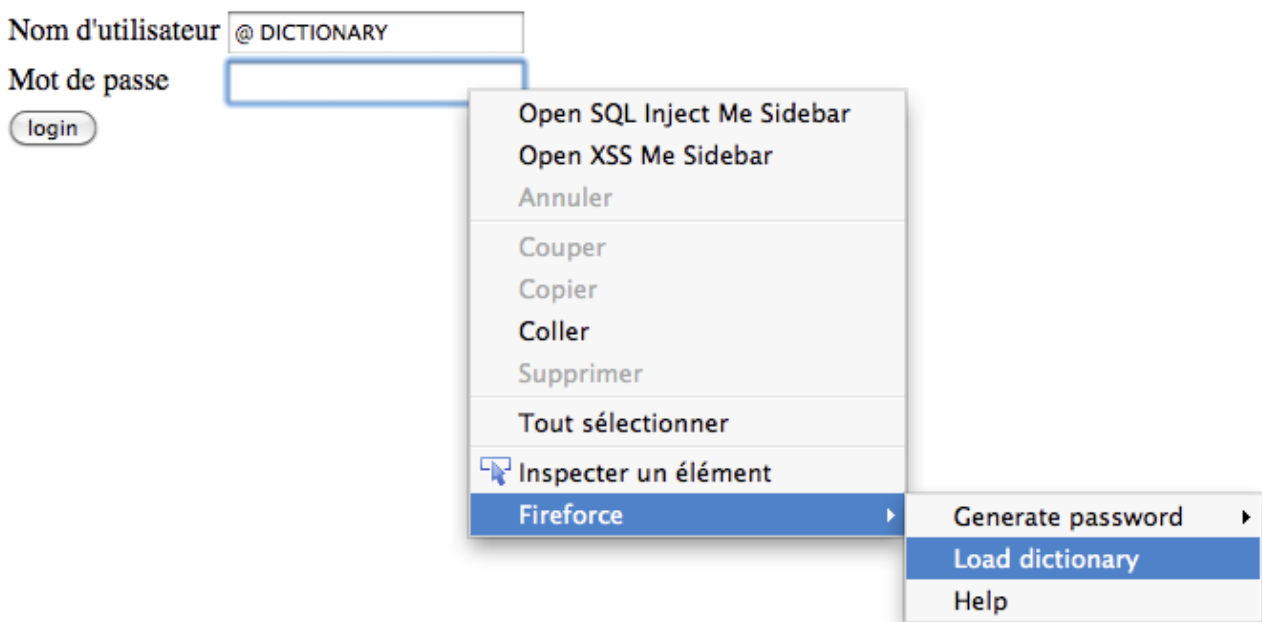
Example: We want to test a series of user names with a series of passwords. Users are in the file common_username.txt and passwords in the file common_passwords.txt.

- Complete the Username field with value "@ DICTIONARY"

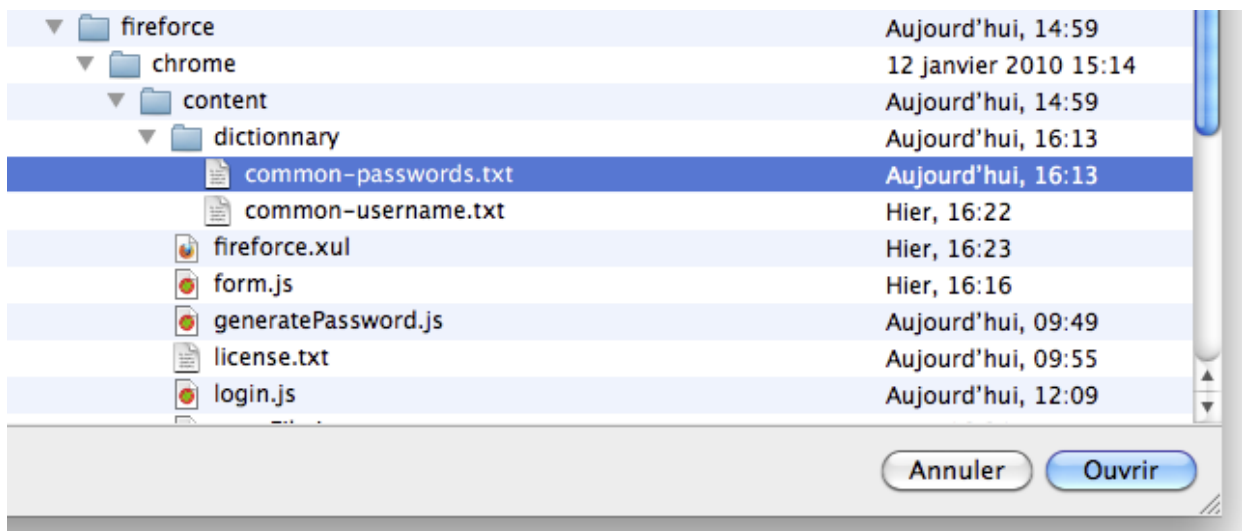
Nom d'utilisateur

Mot de passe

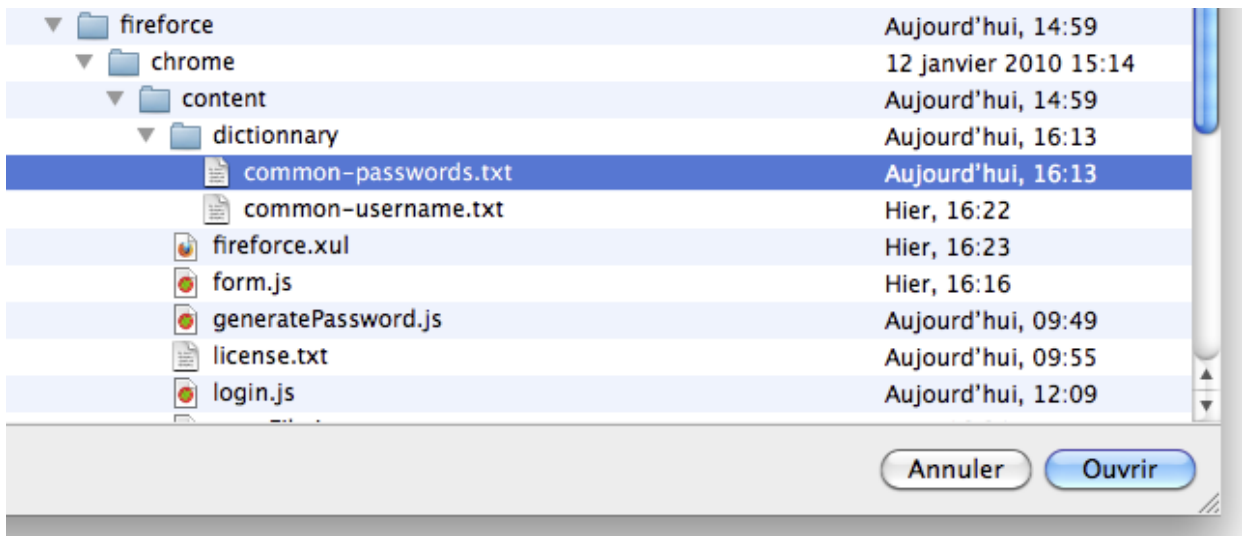
- Right click in the Password field and select: Fireforce> Load Dictionary



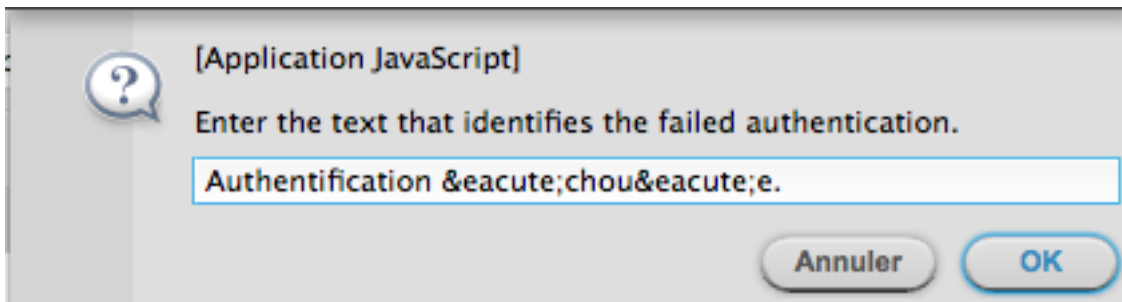
- Choose the dictionary from the explorer. (Press the "shift" key to select multiple dictionaries).



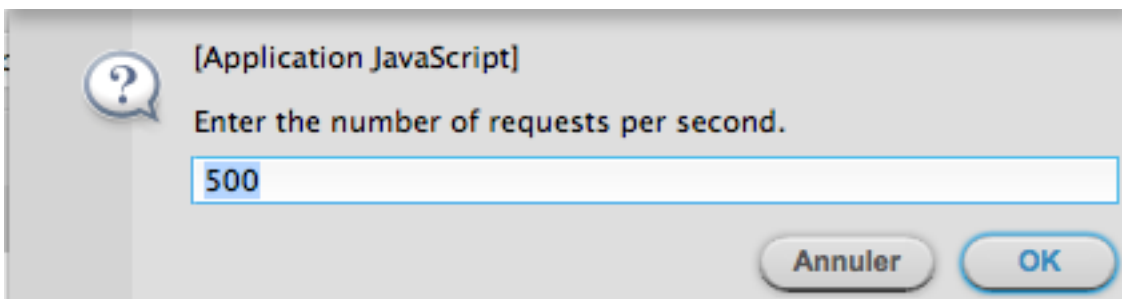
- Choose the dictionary for username from the explorer. (Press the "shift" key to select multiple dictionaries).



- Enter the text that identifies the failed authentication.



- Enter the number of requests sent to the server.



- Pending the results.

The field that contains the value "@ DICTIONARY" can only be tested with a dictionary. It is not possible to attack by generating the usernames and passwords.

Help

To get help, right click and choose Help. A redirection will be made on the presentation page of the extension to the website of the company SCRT. You can download the updates and installation guides from this page.