Déjouer les punycode

Comment déjouer les fausses adresses internet ?
J'ai croisé 2 ou 3 articles traitant du sujet, je souhaitais à mon tour en parler, mais en ajoutant des captures afin que ce soit plus simple à comprendre.

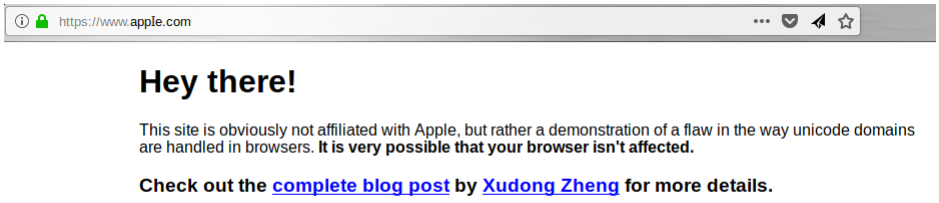
1) Internationalisation

Vous le savez sûrement l'alphabet que l'on connait n'est pas le seul utilisé dans le monde.
Les Russes en ont un, les Grecs également, les Chinois, les Arabes, les Japonnais eux aussi ont tous le leur, et il en existe d'autres.
Si les leurs sont incompréhensibles pour nous, il en est de même pour eux, il est donc légitime qu'ils puissent utiliser leurs propres caractères pour créer des noms de domaine.
C'est ce qui s'appel le *IDN* pour International Domain Name , ce sont des noms de domaines capablent d'utiliser d'autres caratères tel que les lettres accentuées, dit *punycode*.
Jusque là ce n'est pas trop génant, néanmoins vous seriez bien en peine de distinguer:

- le caractère Cyrillic "a" (U+0430)
- du caractère Latin "a" (U+0061)

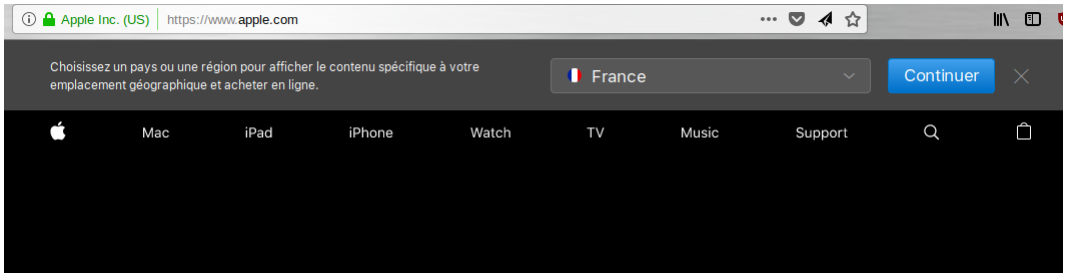
De fait ces 2 adresses vous sembleront identique:

- apple.com



Site de démonstration

- apple.com



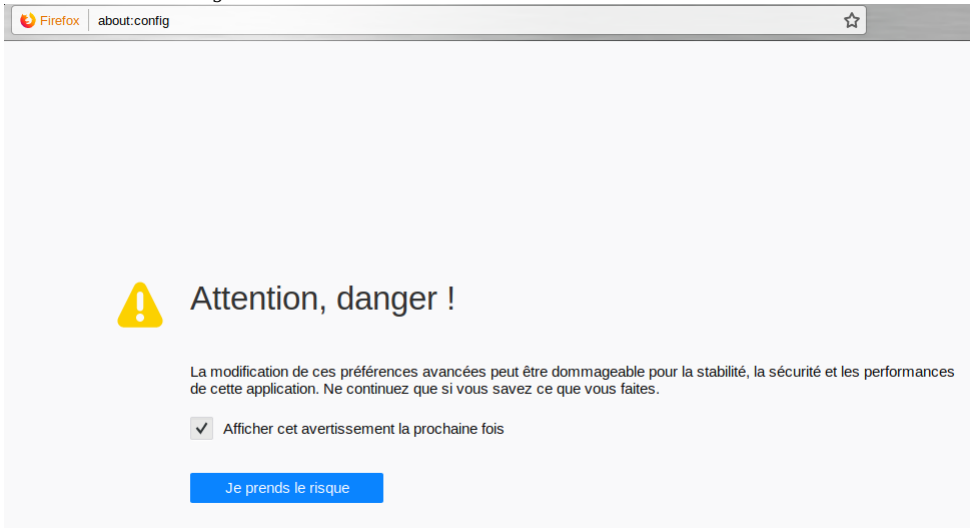
Site authentique

Le premier lien pointe vers un site de démonstration , mis en place par Xudong Zheng étudiant en mathématique à l'Université Johns Hopkins .

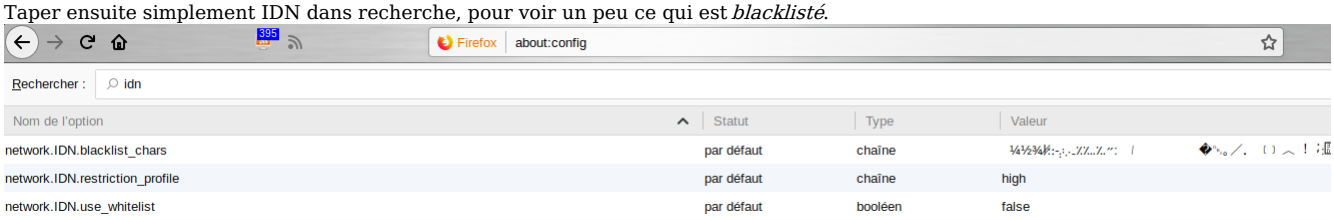
1.1) Solution

Afin de déjouer les caractères *punycode*, il y a une petite manipulation à faire dans votre navigateur Firefox.
Oui Firefox permet une configuration poussé du navigateur, il faut pour cela taper:

- `about:config` dans la barre d'adresse, et répondre *Je prends le risque*, généralement c'est à ce moment là que les gens referme leur navigateur....

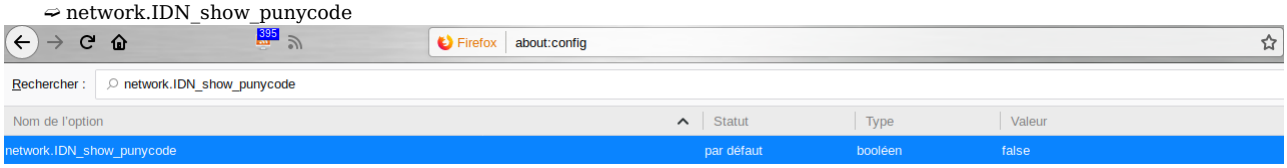


Taper ensuite simplement IDN dans recherche, pour voir un peu ce qui est *blacklisté*.

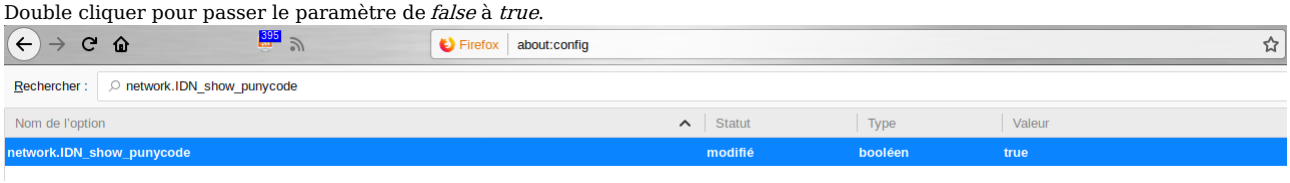


Venons en à la modification elle même pour Firefox 62, il faut modifier ce parametre:

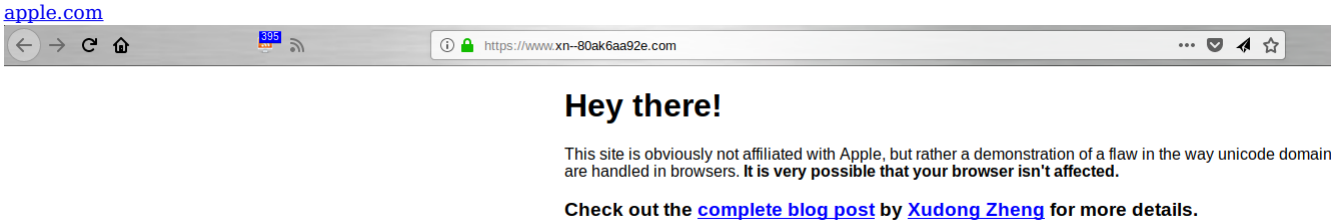
- network.IDN_show_punycode



Double cliquer pour passer le paramètre de *false* à *true*.



Refermer simplement l'onglet , puis cliquer à nouveau sur ce lien:
apple.com



Voilà, j'attendais d'arriver à cette capture pour indiquer que un **IDN** était préfixé par `xn-quelquechose.TLD`
Pour les versions de Firefox antérieur à 62 , il faut simplement chercher : `show_punycode` et passer la valeur à true.

1.2) Académie Française

La seule entité qui pourrait tout mettre par terre , ce serait l'Académie Française, si ils décidaient d'imposer l'utilisation de la cédille ou encore du é pour république, rien ne vous permettra de déjouer les **punycode**.

1.3) Source

A l'origine c'est parti d'un article du Hollandais Volant , mais je ne l'ai pas retrouvé, néanmoins je vous encourage à conserver le lien vers son blog d'un excellent niveau.

- Le Hollandais Volant
- blogmotion
- Xudong Zheng