OWASP ZAP

Introdução

- Filosofia: "Você não pode construir aplicações seguras se não conhece como elas são atacadas"
- Problema: "Os desenvolvedores acham que testes de segurança são magia-negra"
- Solução: Ensinar o básico para desenvolvedores

OWASP Zed Attack Proxy

- Lançado em Setembro de 2010
- Facilidade de uso é uma premissa
- Detalhadas páginas de documentação
- Open Source
- Internacionalizado
- Multi-plataforma
- ...

Instalando o ZAP

- Vá em: http://code.google.com/p/zaproxy
- Em Downloads...

Se preparando para o ZAP

- O navegador normalmente faz diversas requisições
  - O endereço que você está acessando
  - Atualizações
  - Extensões
  - Reputação do domínio
  - ...

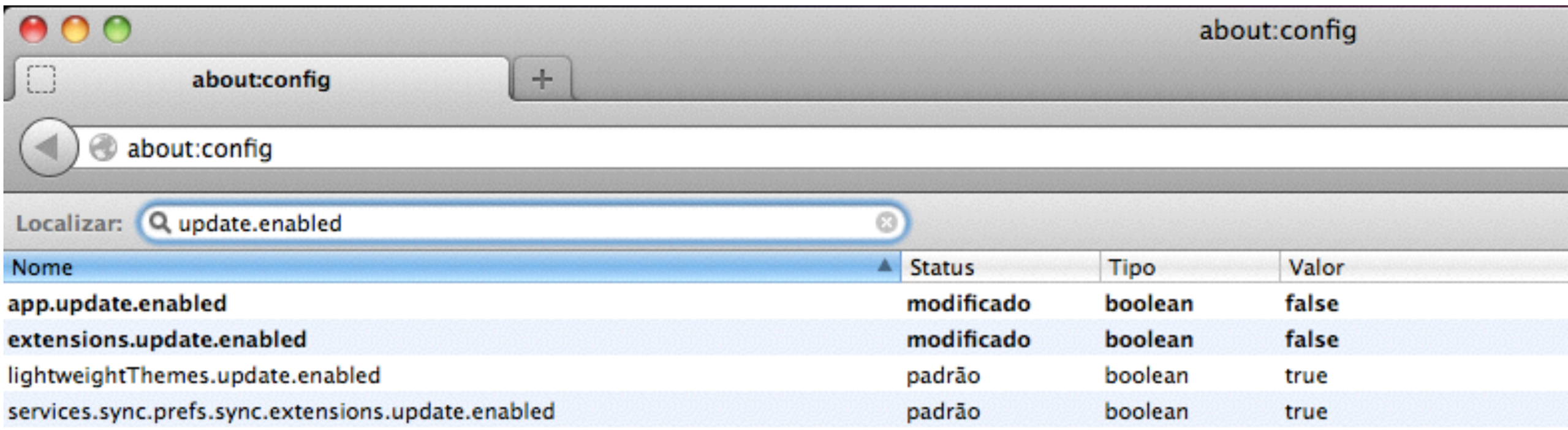
Se preparando para o ZAP

- O ideal é separar um navegador para usar com o ZAP e outro para usar normalmente.
- No exemplo a seguir, usamos o Firefox com o ZAP e outro navegador normalmente.

Limpando o Firefox

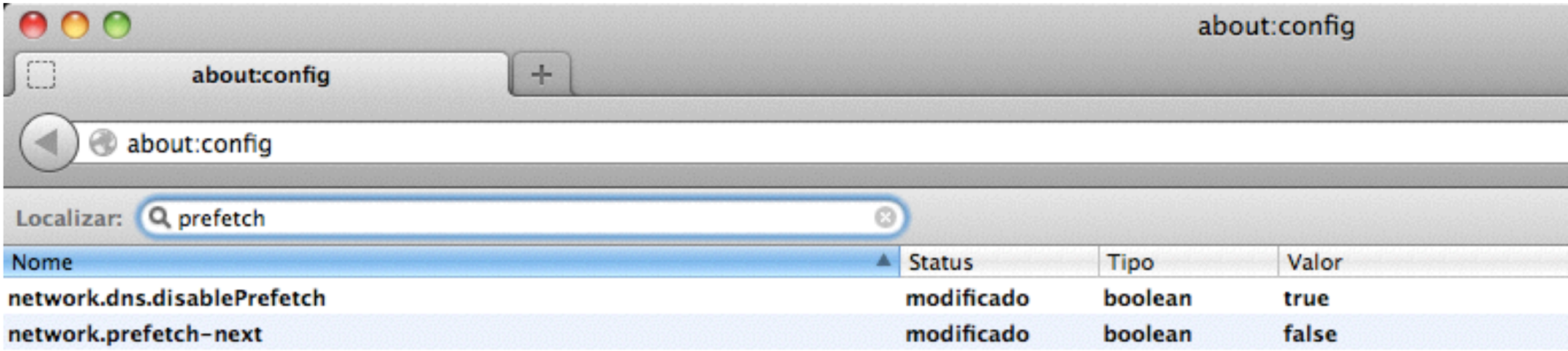
- Desabilite as extensões que fazem conexão com a internet

Desative os updates de extensões



Desative o Pipelining

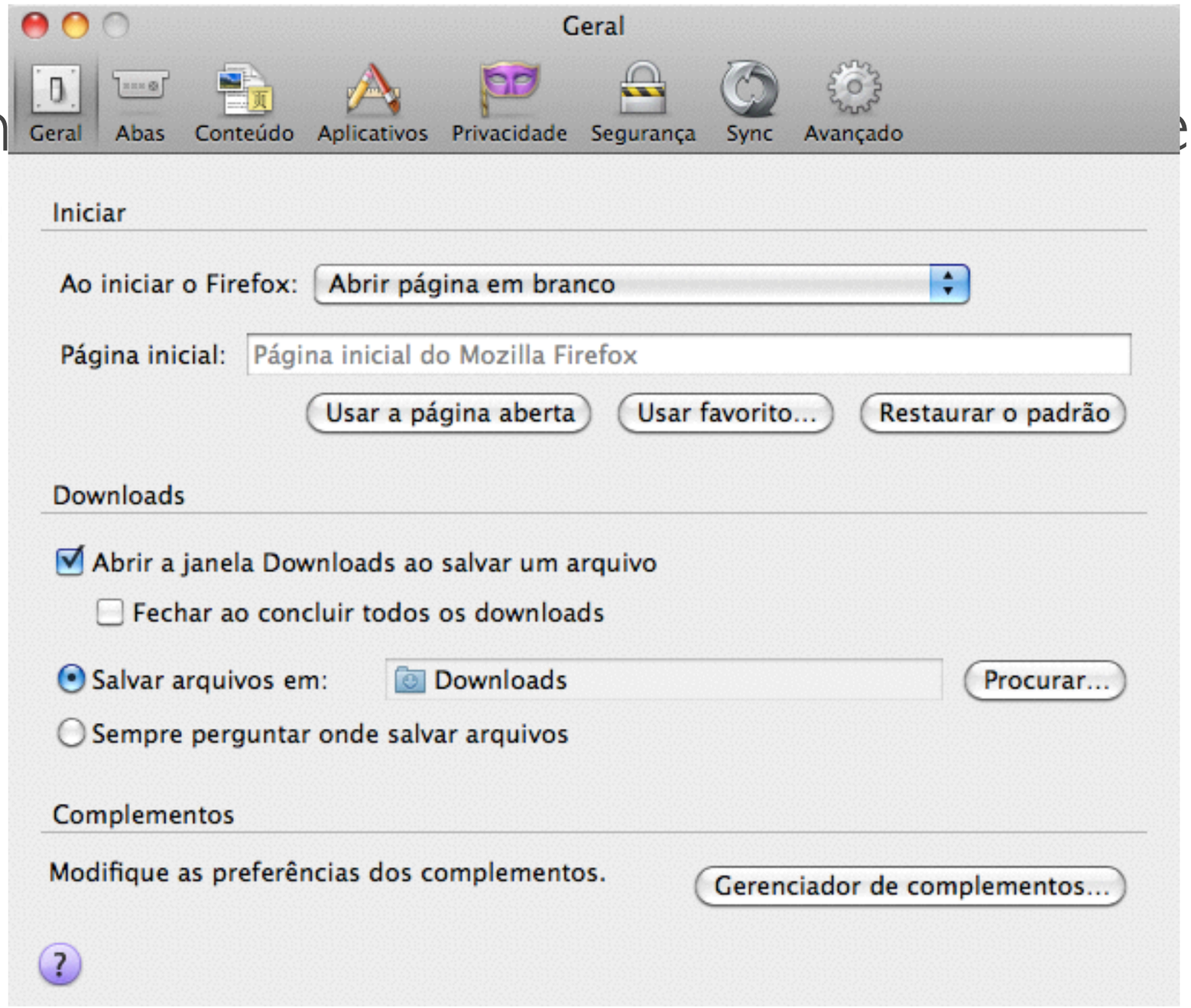
Desative o Pre-fetching



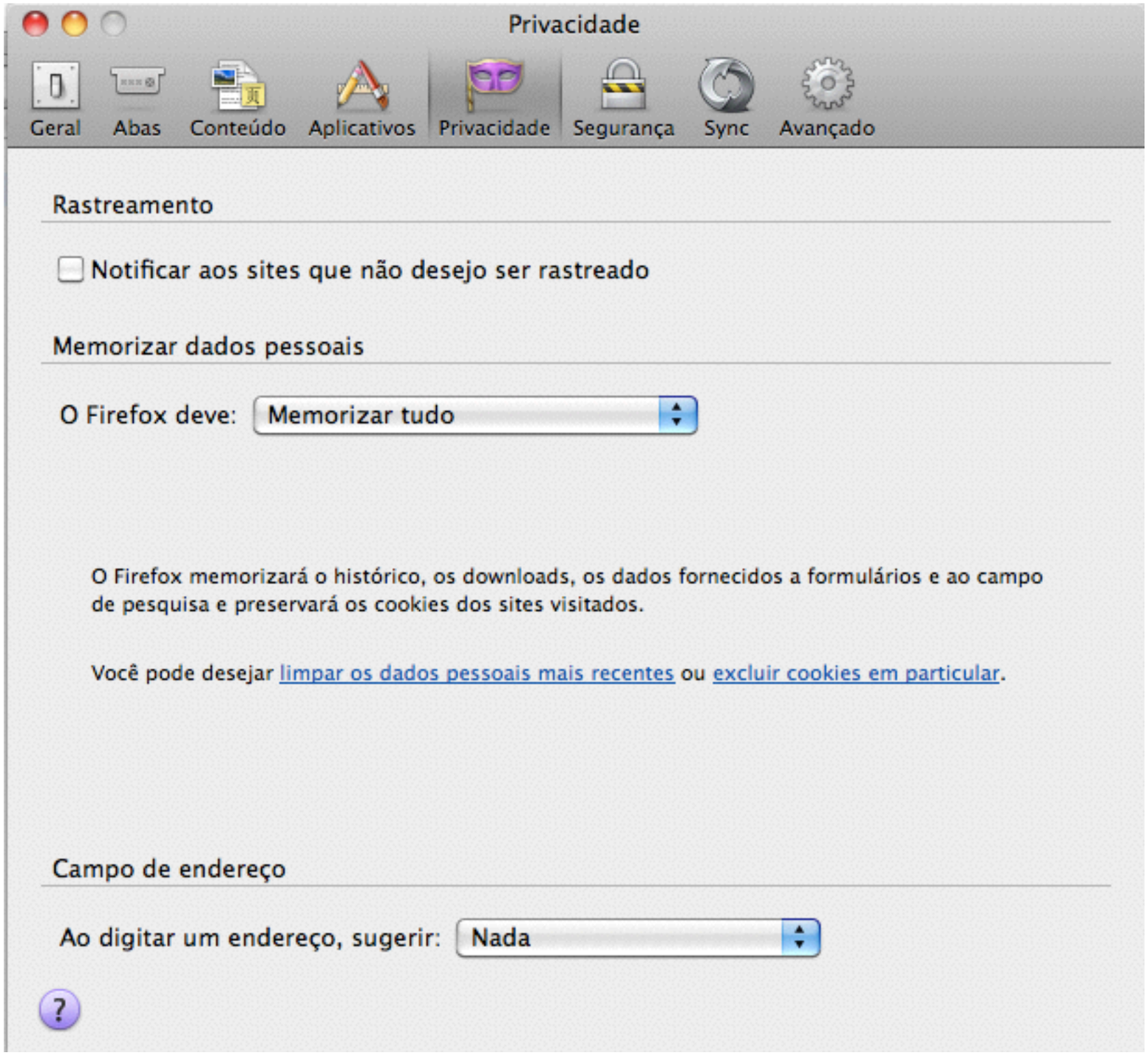
Apague os favoritos

Mude a home page

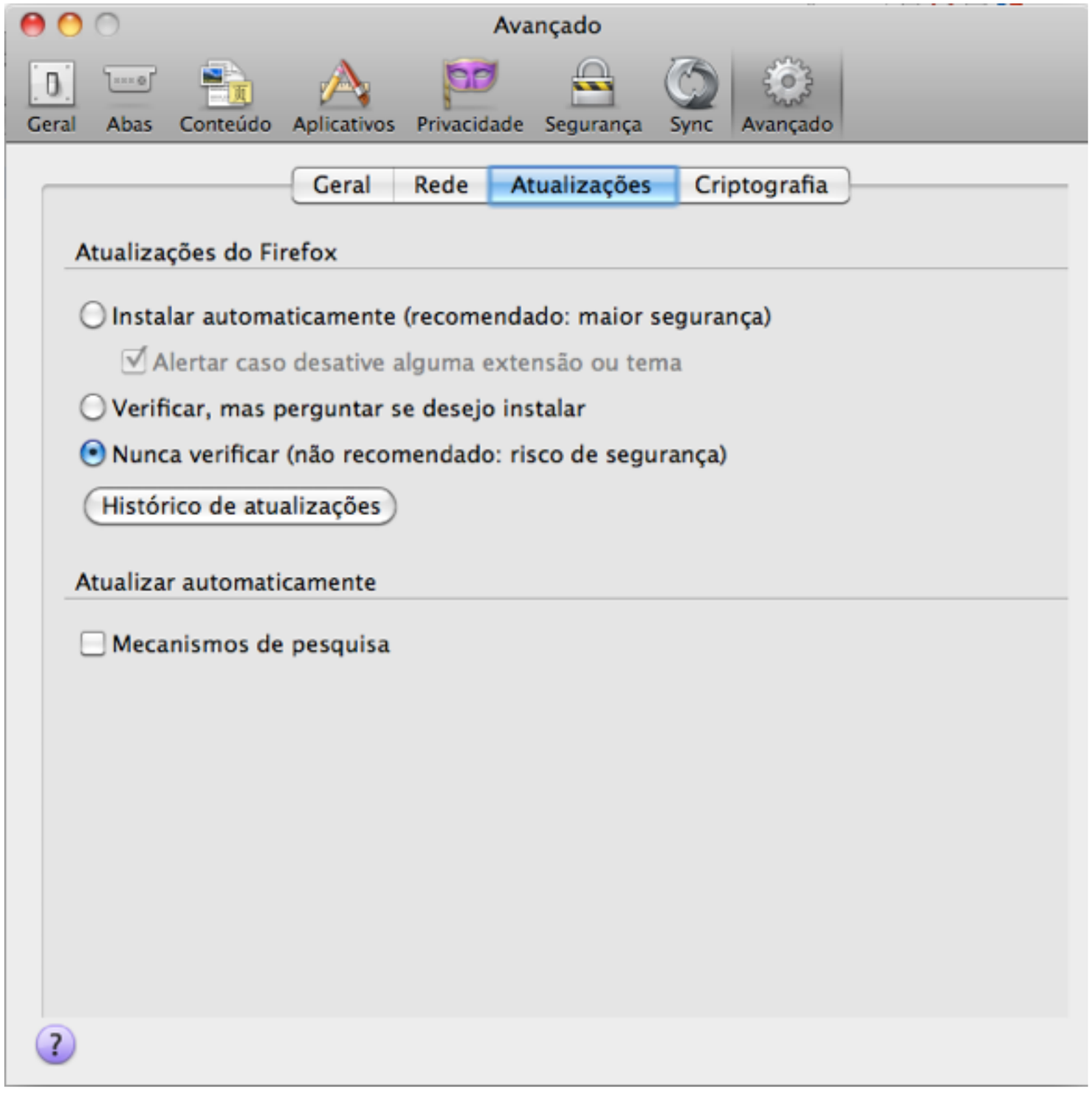
- Vá em … como: about:



Desative as sugestões de página

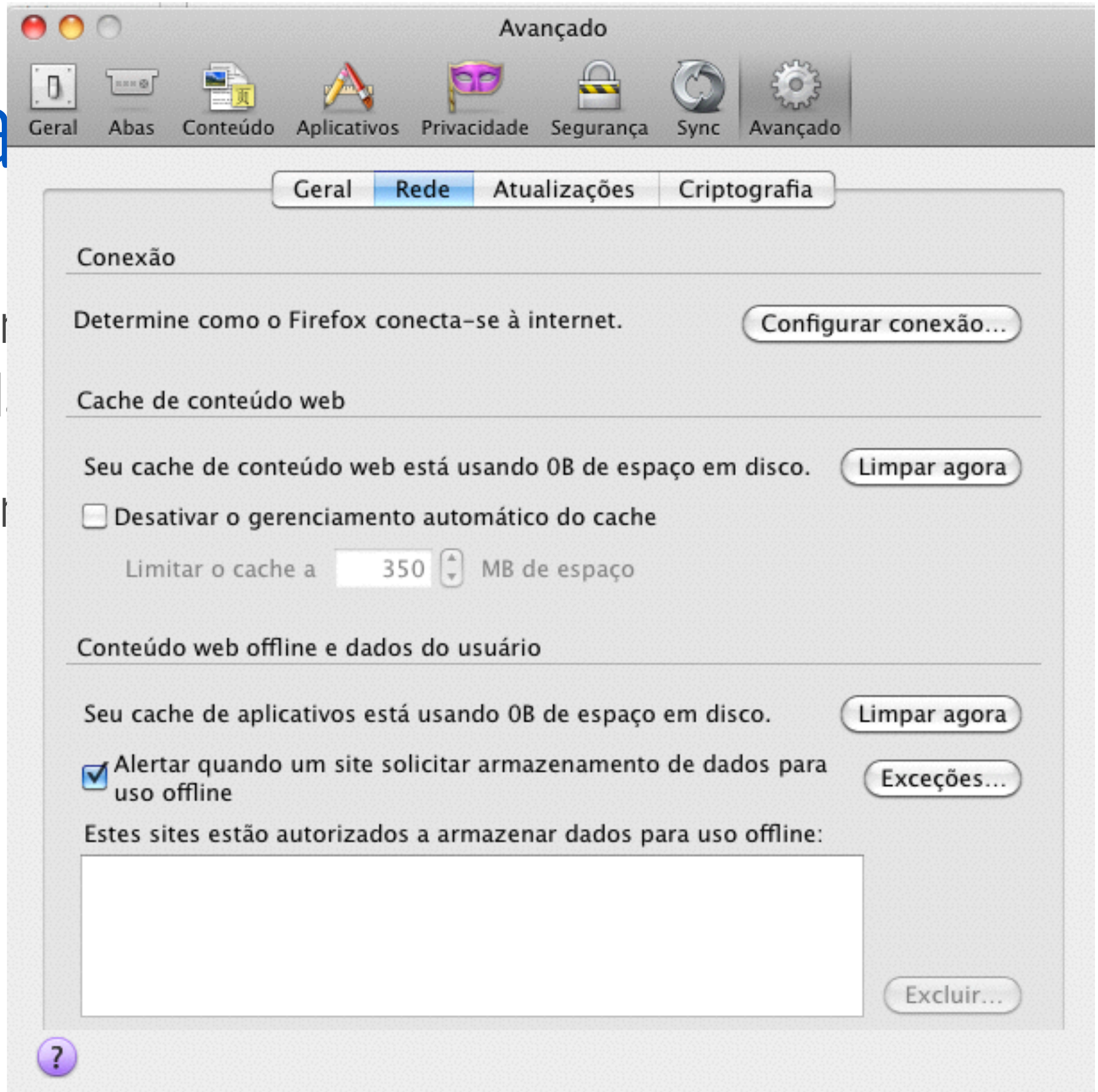


Desative os updates



Ha

- Vá r
  rod
- Vá r



Agora navegue um pouco

Recursos do ZAP

Transformando campos *hidden* em *input*

Spidering

- As vezes a aplicação é muito grande...
- É muito custoso mapear toda a aplicação navegando por ela...

Breakpoints e Reenvio

Breakpoints e Reenvio

- No exemplo podemos modificar os valores que passamos inicialmente.
- Os dados estão sendo validados?

Breakpoints e Reenvio

Decode,Encode...

Fuzz

Fuzz

- Customização de listas:

Força Bruta

- Permite encontrar os recursos da aplicação com o uso de listas. (usa HEAD)

Duvidas?

Execute ZAProxy

Admin configuration

Workspace used /home/ludovicroucoux/Documents/workspace/ZAProxy_Esclave
ZAProxy host localhost (Configured in admin mode)
ZAProxy port 8500 (Configured in admin mode)

Startup

☐ Start ZAProxy in a pre-build step

JDK: InheritFromJob

◉ ZAProxy is installed by Jenkins

Tool to use: ZAProxy_2.4.0

○ ZAProxy is already installed

Avancé...

Setup

Load session:

Target URL: http://demo.testfire.net/

☑ Spider URL

☑ Scan URL

ZAProxy default directory: /home/ludovicroucoux/.ZAP

Choose policy to use: OnlySQLInjection

☑ Generate report

Choose format report: html, xml

Filename for report: ZAPslaveReports/SQLInjectionReport

☑ Save session

Filename for session: ZAPslaveSessions/SQLInjectionSession

Supprimer

https://wiki.jenkins-ci.org/display/JENKINS/ZAProxy+Plugin