



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
 - ▶ ...

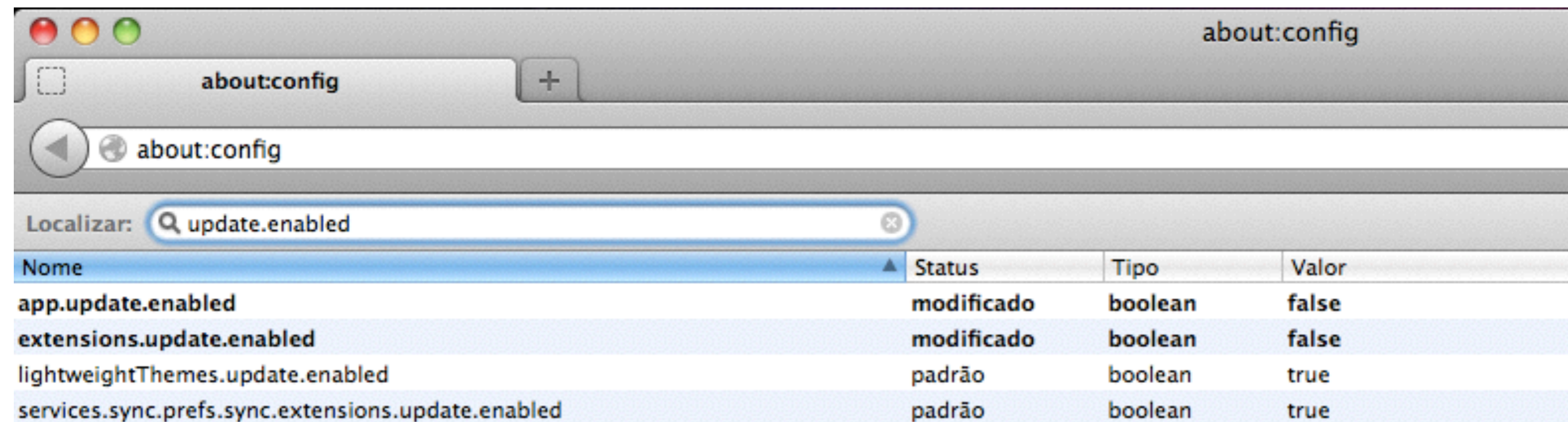
Se preparando para o ZAP

- ▶ 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.

Limpendo o Firefox

- ▶ Desabilite as extensões que fazem conexão com a internet

Desative os updates de extensões



The image shows a browser window with the address bar set to 'about:config'. A search bar labeled 'Localizar:' contains the text 'update.enabled'. Below the search bar, a table displays the search results for configuration preferences related to updates.

Nome	Status	Tipo	Valor
app.update.enabled	modificado	boolean	false
extensions.update.enabled	modificado	boolean	false
lightweightThemes.update.enabled	padrão	boolean	true
services.sync.prefs.sync.extensions.update.enabled	padrão	boolean	true

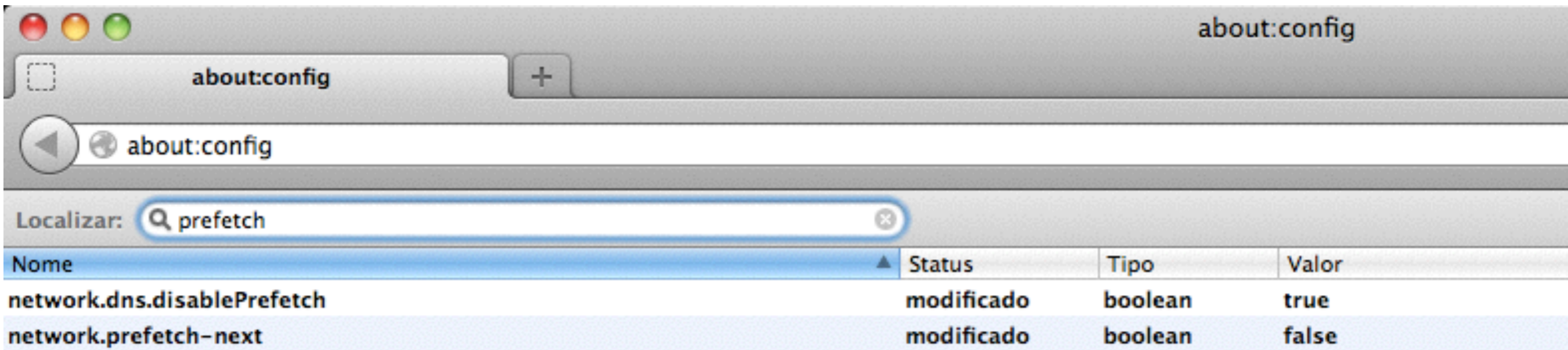
Desative o Pipelining



The image shows a browser window with the address bar containing 'about:config'. A search bar labeled 'Localizar:' contains the text 'pipe'. Below the search bar is a table of configuration settings. The table has four columns: 'Nome', 'Status', 'Tipo', and 'Valor'. Two rows are highlighted with a black border: 'network.http.pipelining' and 'network.http.pipelining.ssl', both with a status of 'modificado' and a value of 'true'.

Nome	Status	Tipo	Valor
gfx.prefer-mesa-llvmpipe	padrão	boolean	false
network.http.pipelining	modificado	boolean	true
network.http.pipelining.abtest	padrão	boolean	false
network.http.pipelining.aggressive	padrão	boolean	false
network.http.pipelining.max-optimistic-requests	padrão	número i...	4
network.http.pipelining.maxrequests	padrão	número i...	32
network.http.pipelining.maxsize	padrão	número i...	300000
network.http.pipelining.read-timeout	padrão	número i...	30000
network.http.pipelining.reschedule-on-timeout	padrão	boolean	true
network.http.pipelining.reschedule-timeout	padrão	número i...	1500
network.http.pipelining.ssl	modificado	boolean	true
network.http.proxy.pipelining	padrão	boolean	false

Desative o Pre-fetching



The image shows a screenshot of a web browser's 'about:config' page. The search bar contains the text 'prefetch'. Below the search bar, a table lists the search results. The table has four columns: 'Nome', 'Status', 'Tipo', and 'Valor'. Two entries are visible: 'network.dns.disablePrefetch' with status 'modificado' and value 'true', and 'network.prefetch-next' with status 'modificado' and value 'false'.

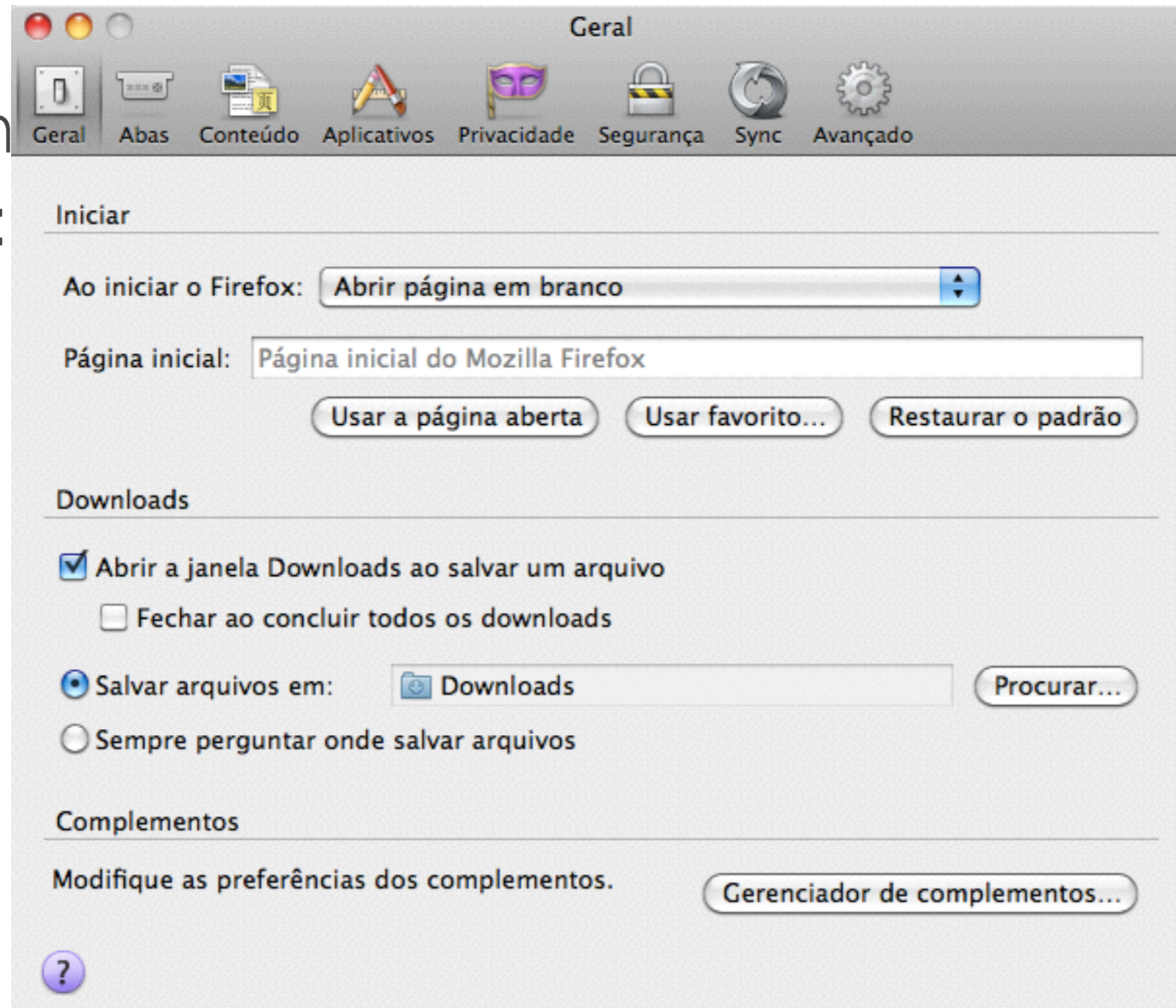
Nome	Status	Tipo	Valor
network.dns.disablePrefetch	modificado	boolean	true
network.prefetch-next	modificado	boolean	false

Apague os favoritos

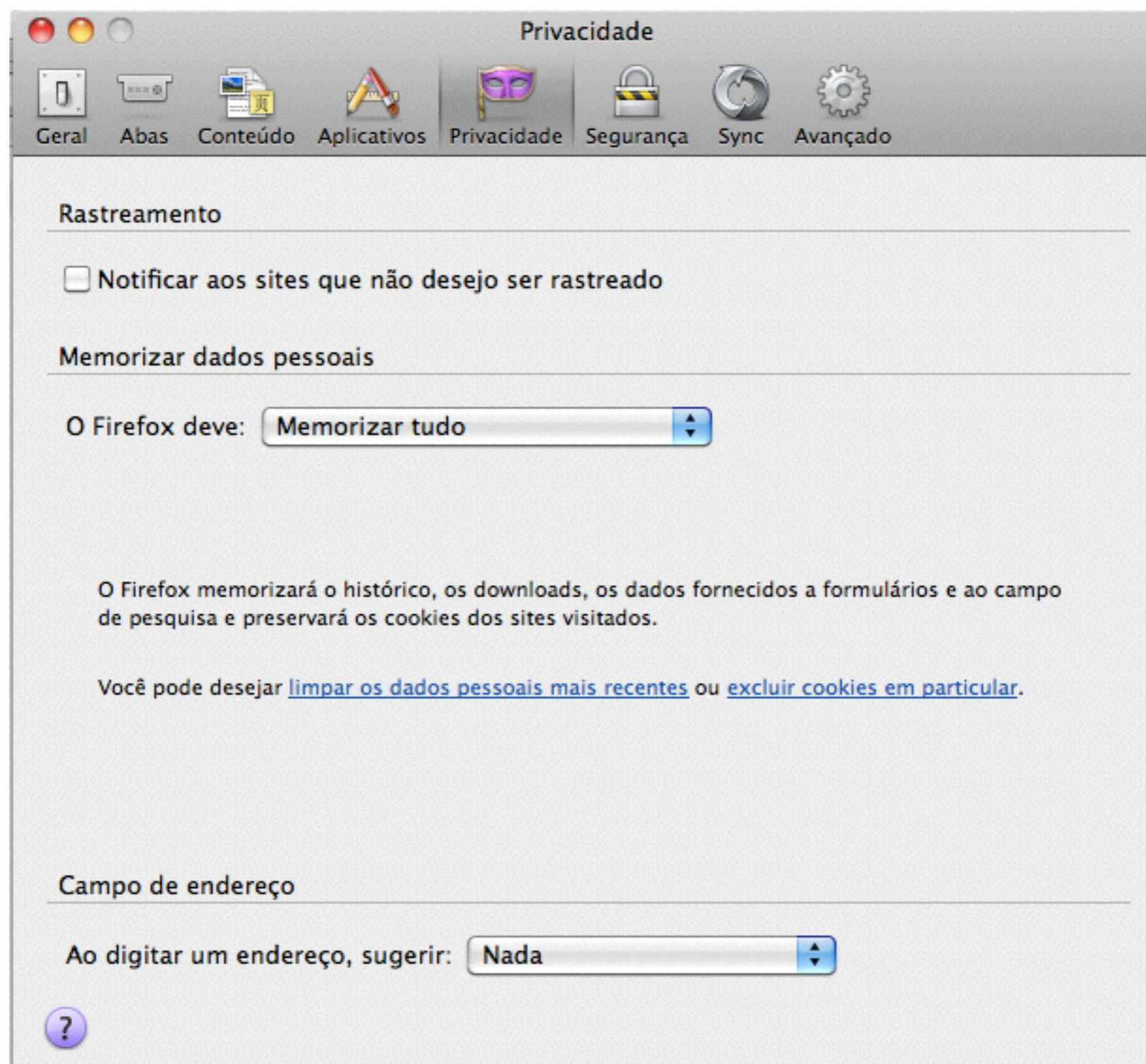
Mude a home page

- ▶ Vá em
about:

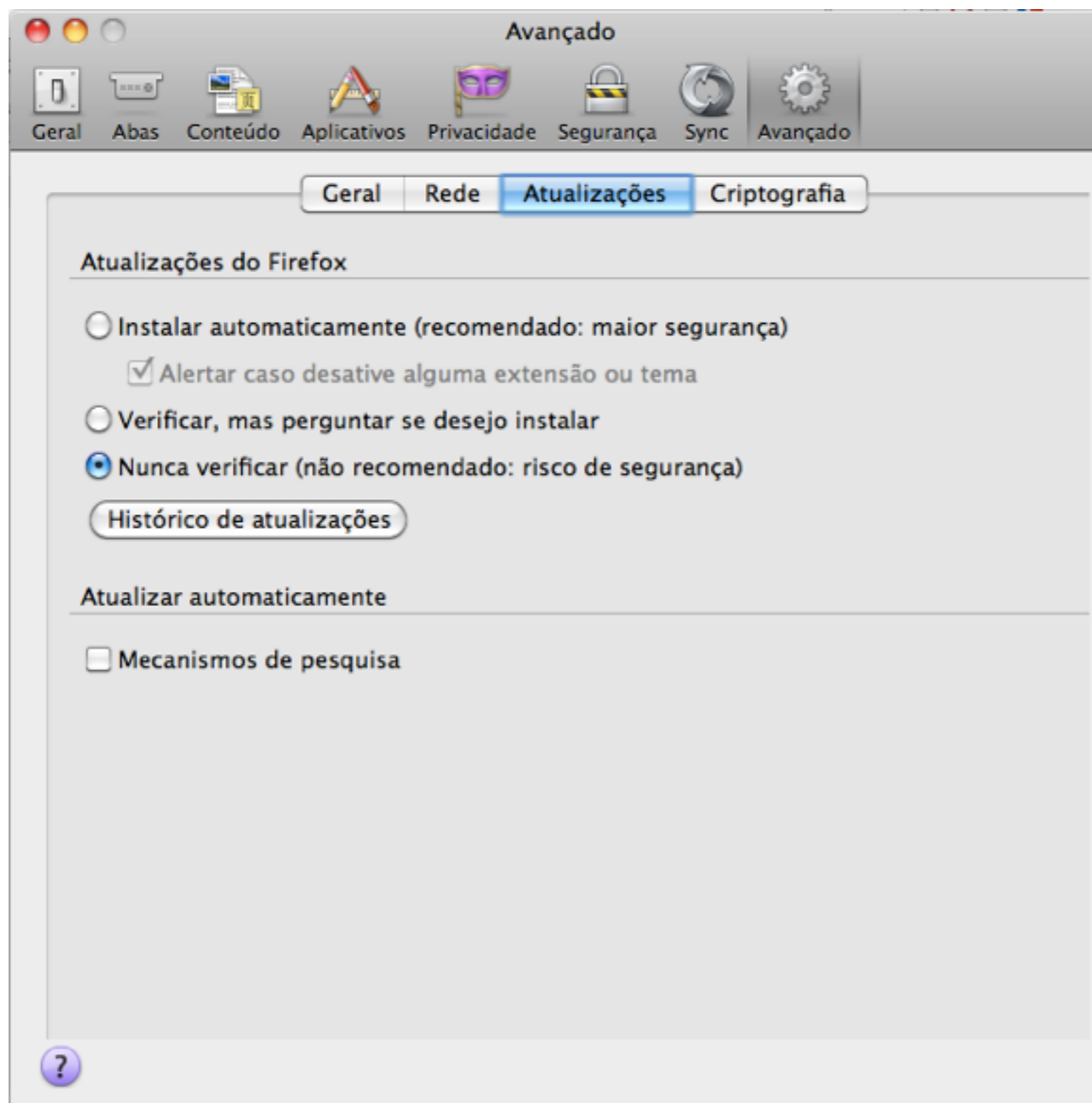
e como:



Desative as sugestões de página



Desative os updates



Ha

- ▶ Vá i
- rod
- ▶ Vá i



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>