

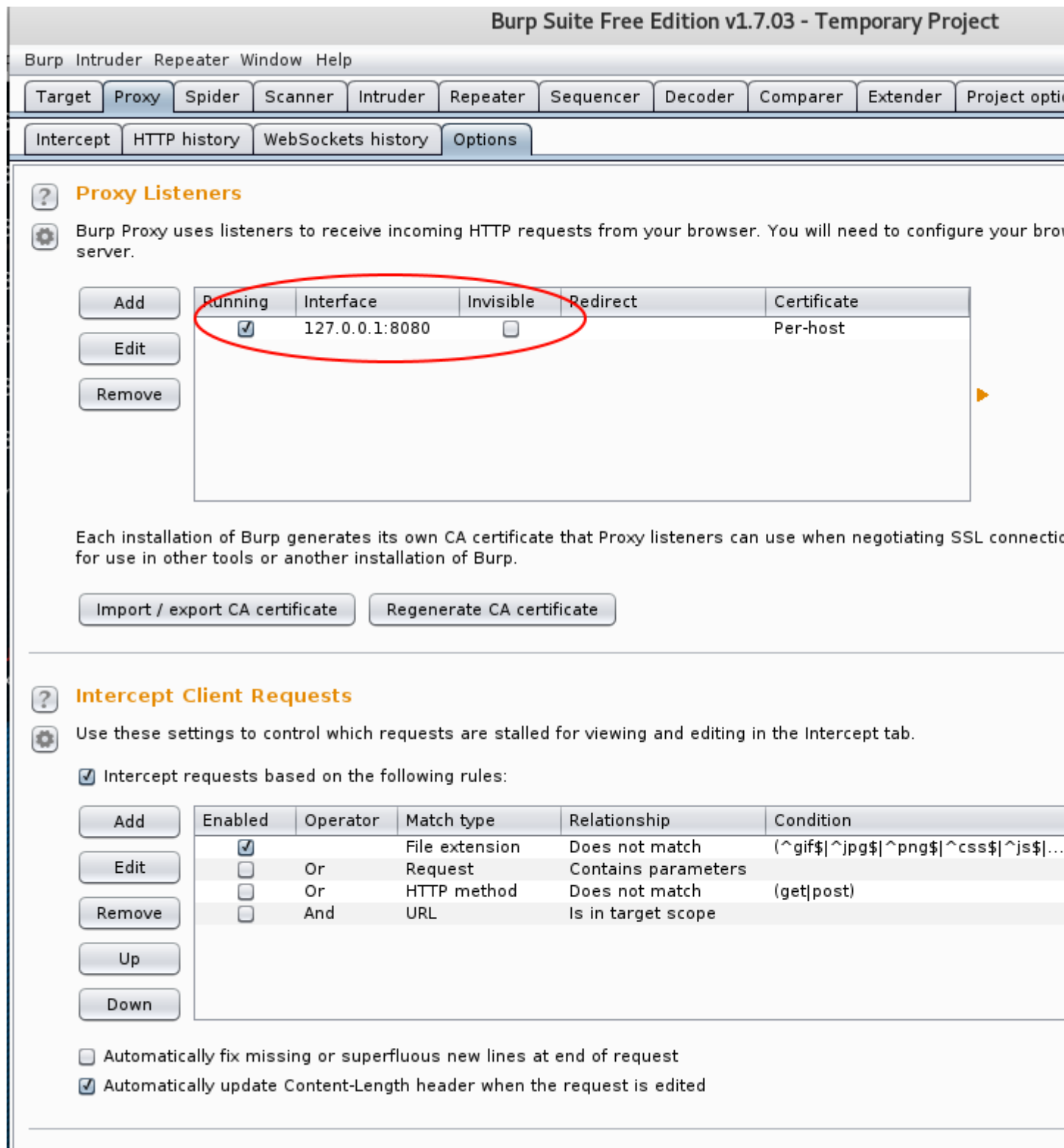
Burp Suite est un outil permettant de réaliser des tests de sécurité d'application web. Celui-ci peut vous servir si vous souhaitez altérer des requêtes à la volée pour tester diverses vulnérabilités. C'est un outil populaire, qui mérite donc au moins un petit tutoriel.

Pour le lancer :

Menu « **Applications -> Applications Web -> BurpSuite** »

Vous pouvez utiliser les paramètres par défaut lors du lancement.

Rendez-vous dans « **Proxy -> Options** » et vérifiez qu'il y ait un listener actif :



The screenshot shows the 'Burp Suite Free Edition v1.7.03 - Temporary Project' window. The 'Proxy' tab is selected, and the 'Options' sub-tab is active. The 'Proxy Listeners' section is visible, showing a table with one listener configuration. A red circle highlights the 'Running' checkbox (checked), the 'Interface' (127.0.0.1:8080), and the 'Invisible' checkbox (unchecked). Below the table, there are buttons for 'Add', 'Edit', and 'Remove'. The 'Intercept Client Requests' section is also visible, showing a table with rules for intercepting requests. The 'Enabled' checkbox is checked, and the rules are: 'File extension' (Does not match, (^gif\$|^jpg\$|^png\$|^css\$|^js\$|...)), 'Request' (Contains parameters), 'HTTP method' (Does not match, (get|post)), and 'URL' (Is in target scope). There are also buttons for 'Add', 'Edit', 'Remove', 'Up', and 'Down' for the rules table. At the bottom, there are checkboxes for 'Automatically fix missing or superfluous new lines at end of request' (unchecked) and 'Automatically update Content-Length header when the request is edited' (checked).

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options

Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use the proxy server.

Add Edit Remove

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections for use in other tools or another installation of Burp.

Import / export CA certificate Regenerate CA certificate

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☒ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$...
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

Add Edit Remove Up Down

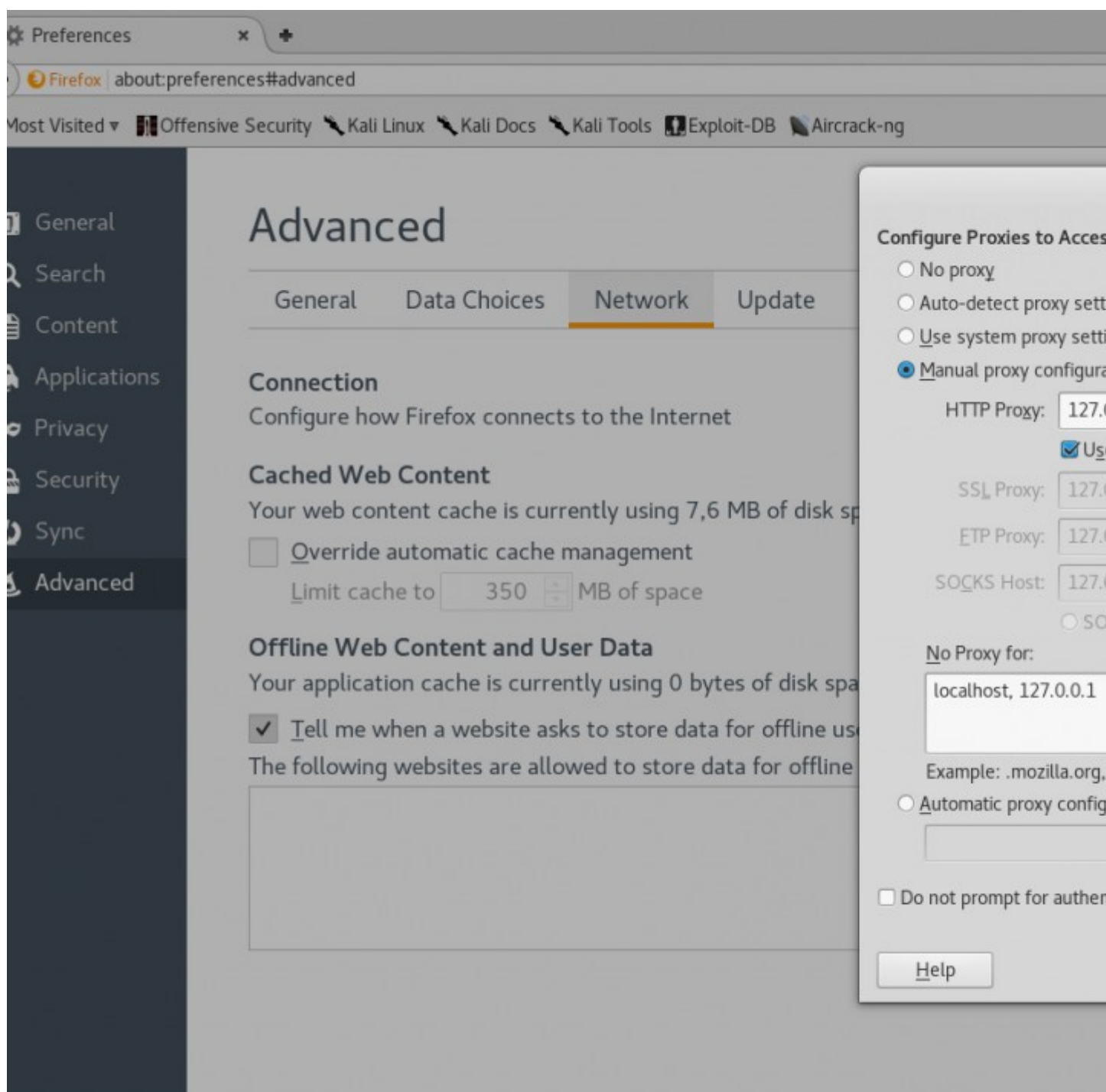
☐ Automatically fix missing or superfluous new lines at end of request

☒ Automatically update Content-Length header when the request is edited

Vous pouvez ensuite utiliser Firefox (dans Kali) pour le configurer avec BurpSuite :

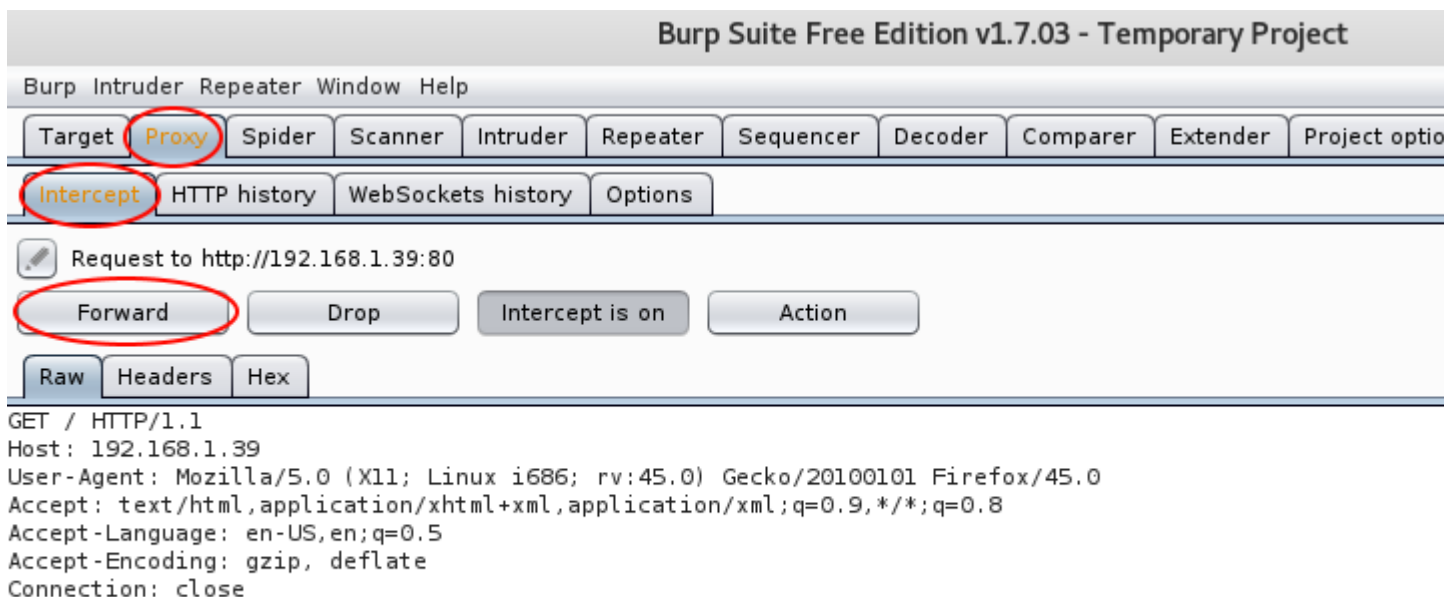
Tapez « **about:preferences** » dans la barre d'adresses.

Sélectionnez l'onglet « **Advanced** » puis « **Network** » et cliquez sur « Settings » puis entrez l'adresse IP locale et le port donnés dans BurpSuite :

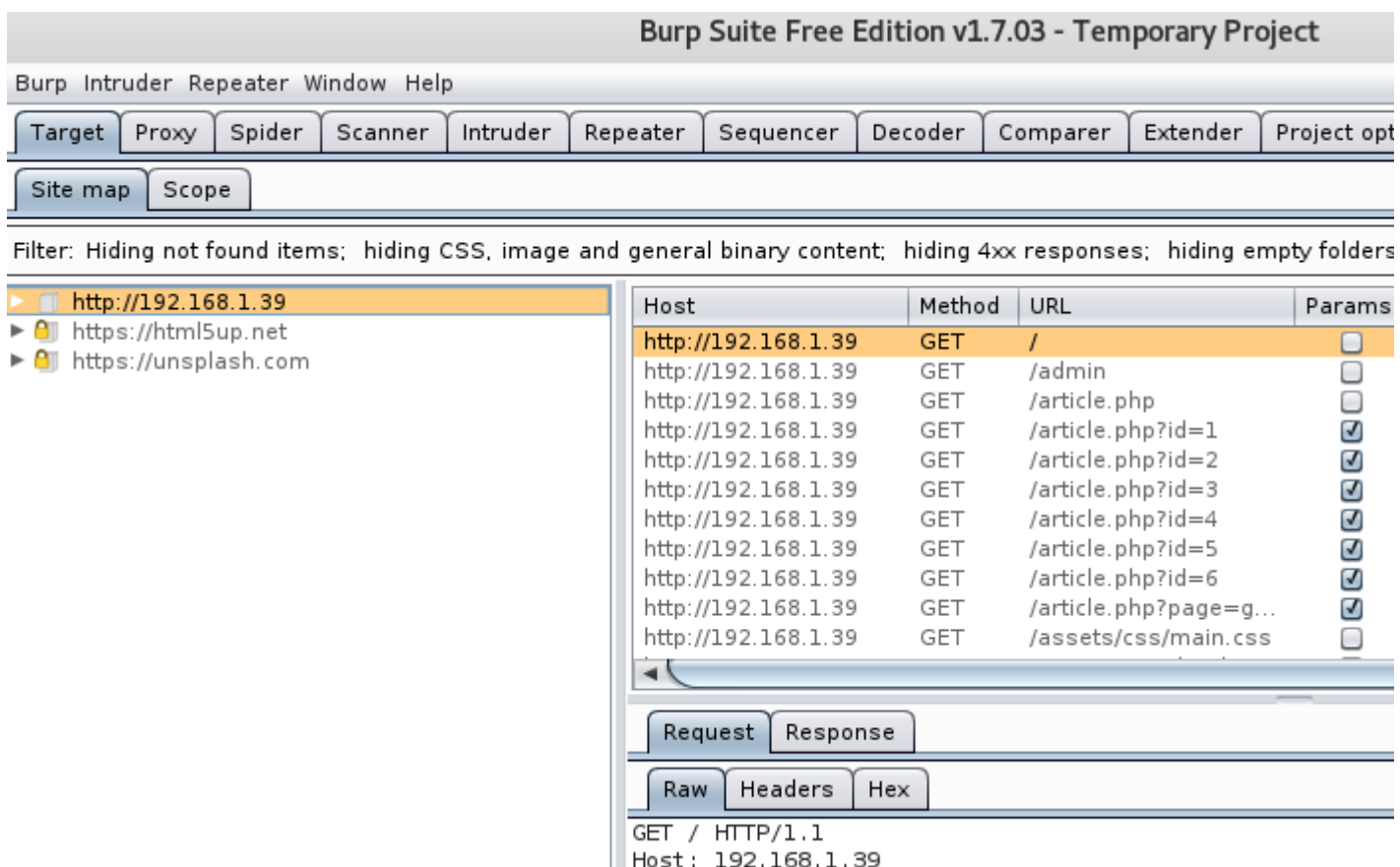


Vous pouvez ensuite visiter des sites web dans Firefox, par exemple un site vulnérable en local (de mon cas, « VulneWeb » hébergé sous Windows 7).

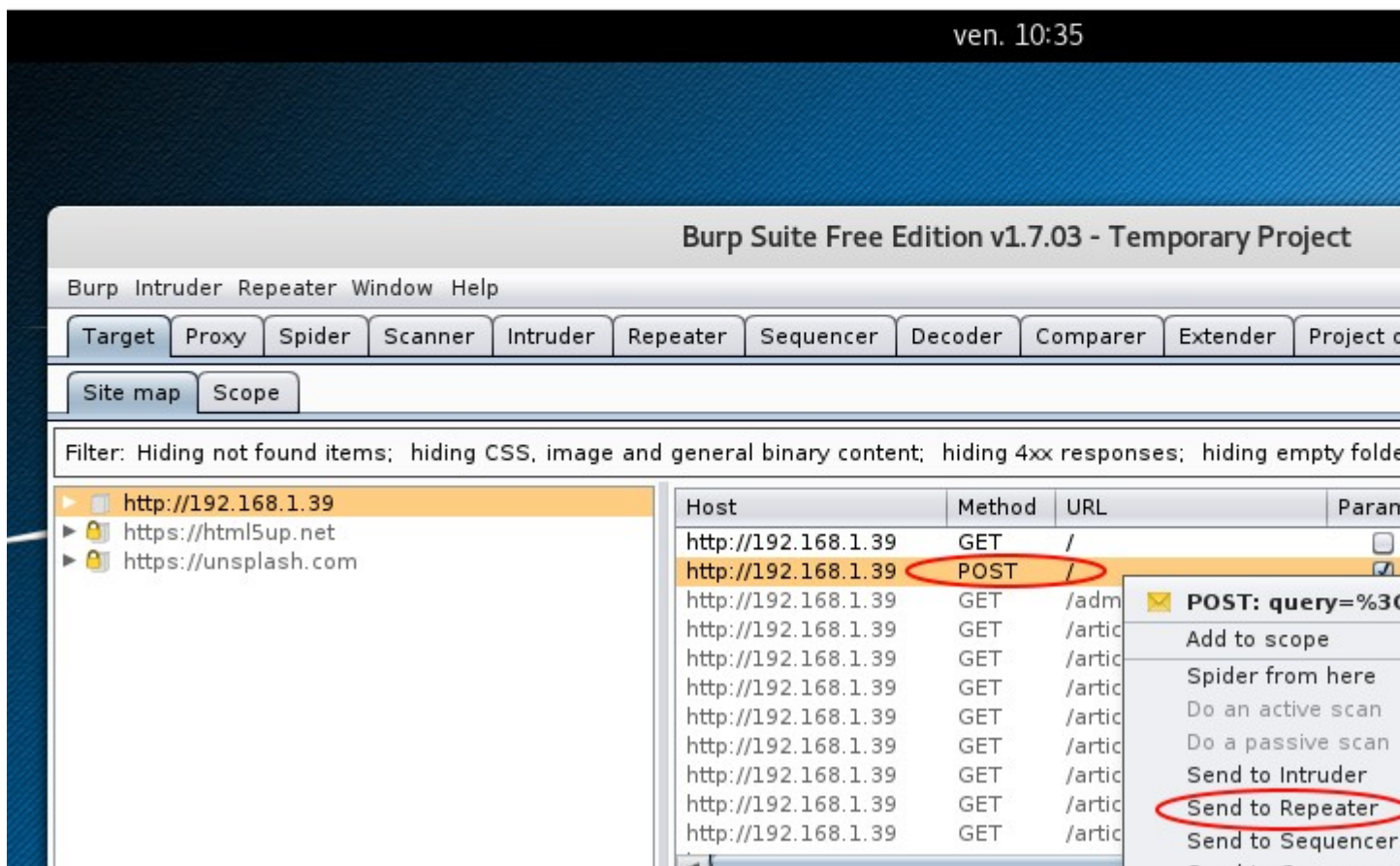
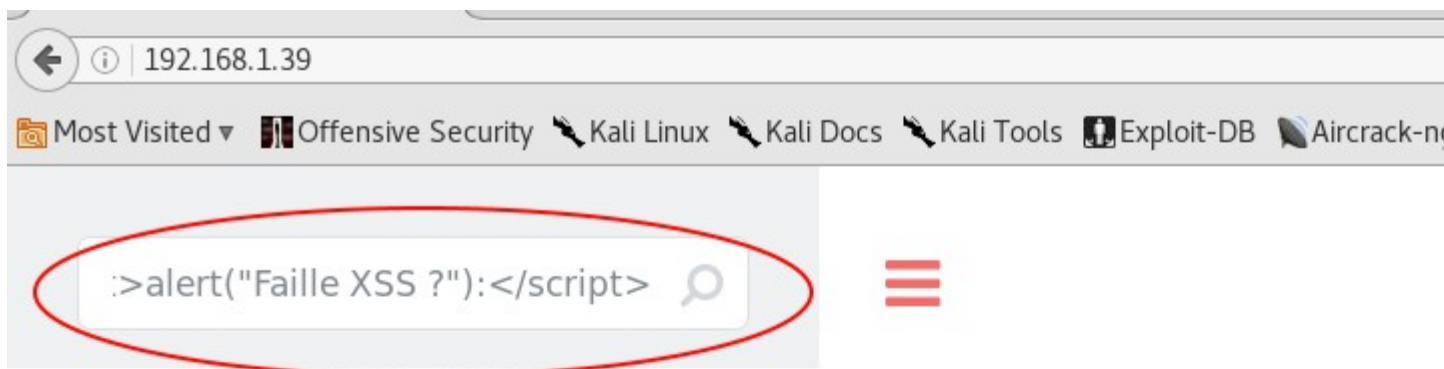
L'onglet « **Proxy** » s'allumera ainsi que l'onglet « **Intercept** ». Vous pouvez cliquer sur le bouton « **Forward** » pour continuer les requêtes.



L'onglet « Target » et le sous-onglet « Sitemap » seront dès lors actifs et enregistreront les sites web visités :



Pour tester une faille XSS par exemple, vous pouvez la tester manuellement dans le site web, puis la laisser passer à travers le proxy puis cliquer sur la requête et l'envoyer dans le répéteur :



De là, vous pourrez rejouer la requête en changement notamment son contenu :

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

TargetProxySpiderScannerIntruderRepeaterSequencerDecoderComparerExtenderProject options

1 × ...

GoCancel<|v>>|v>

Request

RawParamsHeadersHex

POST request to /

Type	Name	Value
Body	query	%3Cscript%3Ealert%28%22Fajlle+XSS

AddRemoveUp

Response

RawHeadersHex

HTTP/1.1 200 OK
Date: Fri, 17 Mar 2017 14:00:00 GMT
Server: Apache/2.4.23 (Ubuntu)
X-Powered-By: PHP/5.6.33-1ubuntu0.16.04+deb8u8
Content-Length: 4746
Connection: close
Content-Type: text/html

Vous avez accès au tutoriel pour tester le Top 10 OWASP des failles web via le lien suivant :
<https://support.portswigger.net/customer/en/portal/articles/1969845-using-burp-to-test-for-the-owasp-top-ten>