

CONFIGURING BURP SUITE AND FIREFOX FOR KALI LINUX

by Dwayne Brock

8-21-2025

The following is a brief guide for setting up Burp Suite for use on the Mozilla Firefox browser, on the Kali Linux operating system. Such setup is necessary before any exercises or practice with Burp Suite using online sites may actually be performed.

This guide was created with the assistance of Google Gemini in connection with a google search.

Setting up Burp Suite on Kali Linux :

Burp Suite is a web application security testing tool, and Kali Linux comes with it pre-installed. To effectively use Burp Suite, especially for intercepting HTTPS traffic, you'll need to configure it and your browser (like Firefox) to work together. [1, 2, 3]

Here's a step-by-step guide to setting up Burp Suite on Kali Linux:

1. Launching Burp Suite • Open the applications menu in Kali Linux.

- Navigate to "Web Application Analysis".
- Click on "Burp Suite" to launch the application.
- When prompted to create a project, choose "Temporary project" (for Community Edition users).
- Click "Next," then "Start Burp" using the default settings. [4, 5]

2. Configure Firefox (or preferred browser) To intercept web traffic.

Your browser needs to be configured to use Burp Suite as a proxy.

According to *InfoSec Write-ups* (<https://infosecwriteups.com/how-to-setup-burpsuite-on-linux-350d17780fdb>) and *CloudSpinx* (<https://cloudspinx.com/understanding-and-using-burp-suite-on-kali-linux/>), Firefox is a commonly used and recommended browser due to its ease of configuration.

- Open Burp Suite and go to the "Proxy" tab.
- Click on the "Options" sub-tab.
- Verify that the Proxy Listener is running on 127.0.0.1:8080.
- Open Firefox and go to Preferences > Network Settings > Settings.
- Choose "Manual proxy configuration".
- Set the HTTP Proxy to 127.0.0.1 and the Port to 8080.
- Crucially, select "Use this proxy server for all protocols" (or manually configure HTTPS).
- Click "OK" to save the changes. [3, 8, 9]

3. Install Burp Suite's CA certificate.

To intercept HTTPS traffic, install Burp Suite's CA certificate in your browser.

In Burp Suite, export the CA certificate in DER format. Then, in Firefox, go to *Preferences > Privacy & Security > Certificates > View Certificates > Authorities > Import*. Select the exported certificate, trust it to identify websites, and restart Firefox. [3, 10, 11]

4. Verify interception Open Burp Suite, go to the "Proxy" tab, and ensure "Intercept is on". Navigate to a website in your browser, and you should see the requests in Burp Suite. [3]
This setup allows you to intercept web traffic. Burp Suite has additional features like Intruder, Repeater, and Scanner. Always obtain consent before testing web applications you don't own. [9, 12, 13, 14, 15]

Online References Used:

- [1] <https://www.linkedin.com/pulse/how-use-burp-suite-kali-linux-step-by-step-geznf>
- [2] <https://www.kali.org/tools/burpsuite/>
- [3] <https://www.linkedin.com/pulse/how-use-burp-suite-kali-linux-step-by-step-geznf>
- [4] <https://thenewstack.io/pentest-your-web-apps-with-burp-suite-on-kali-linux/>
- [5] <https://www.examcollection.com/blog/how-to-legally-install-and-use-burp-suite-for-free-on-kali-linux/>
- [6] <https://cloudspinx.com/understanding-and-using-burp-suite-on-kali-linux/>
- [7] <https://infosecwriteups.com/how-to-setup-burpsuite-on-linux-350d17780fdb>
- [8] <https://www.youtube.com/watch?v=nsxlnRqKYJA>
- [9] <https://linuxconfig.org/learn-burp-suite-on-kali-linux-part-1>
- [10] <https://www.youtube.com/watch?v=CI4RFklwUw0>
- [11] <https://www.youtube.com/watch?v=nsxlnRqKYJA>
- [12] <https://www.linkedin.com/pulse/how-use-burp-suite-kali-linux-step-by-step-geznf>
- [13] <https://medium.com/@trixiahorner/burp-suite-made-easy-a-step-by-step-tutorial-part-1-of-2-451695ce84b1>
- [14] <https://www.linkedin.com/pulse/how-use-burp-suite-kali-linux-step-by-step-geznf>
- [15] <https://www.cybrary.it/blog/how-to-use-burpsuite-pro-for-free-on-kali-linux>