Burp Suite

https://portswigger.net/burp

Written by BB King || linkedin.com/in/bbhacking
Reviewed by Chris Traynor || ridgebackinfosec.com

Burp Suite is an intercepting HTTP proxy that can also scan a web-based service for vulnerabilities. A tool like this is indispensable for testing web applications. Burp Suite is written in Java and comes bundled with a JVM, so it works on any operating system you're likely to use. It comes in a free Community version and a paid-for Professional version. Pro offers more automation and more powerful filters, but Community is enough for CTFs and a good chunk of penetration testing too.

*The "**proxy**" part means that it acts as a pass-through system for network traffic between an HTTP client and an HTTP server. Requests from the client pass through Burp Suite—which usually runs on the same host as the client—before hitting the network, and responses from the server pass through Burp Suite before going to the browser (or any other user agent).*

*The "**intercepting**" part means that it allows you to hold on to a request (or a response) and inspect or modify it before releasing it on its way.*

*The "**suite**" part means it does a whole lot more than just intercept HTTP traffic. Burp Suite is made up of a half-dozen or so built-in tools and also supports extensions, of which more than 300 are available for one-click installation via the BApp Store in the Extensions tab.*

Getting Started

The first thing to do with Burp Suite is to just look at some HTTP traffic and see what you can learn by reading what you see. To do this:

- » *Go to the "Proxy" tab*
- » *Open the "Intercept" sub-tab*
- » *Click "Open browser"*

This will launch an embedded Chromium-based browser that is pre-configured to use Burp Suite as its proxy.

In that browser, visit https://example.com/ then come back to Burp Suite and click on the HTTP History tab of the Proxy. Among a few other requests your browser does on its own, you'll see a "Host" of "https://example.com" and a "Method" of "GET" and a "URL" of "/". When you select that row, you'll see the HTTP request and response in the panes below.

Right-click on any request and choose "Send to Repeater" then send the request again from within Repeater. Now modify the request in some way and send it again to see how the server handles different inputs. Start deleting headers until you get an error or a timeout, then try to figure out what caused the difference.

Right Click on Everything

A lot of Burp Suite's functionality is in the context menus, so it pays to right-click on everything. You may be surprised at what you find.

Now, on to the tools in the Suite...

Proxy

The Proxy History shows all of the traffic that has gone through Burp Suite so far.

- Click on any heading here to sort by that heading. Click again to sort in reverse. Click a third time to go back to unsorted.
- Click and drag the column headings to put them in a different order.
- Scroll all the way to the right to see all the columns and understand what they're showing you.
- Click on the dark bar above the headings to see the filters available. Better filtering is one of the key benefits of Burp Pro over Community.
- Right-click on any request you see here and choose "Send to Repeater" (or any other tool) and see what you can do with it in that other tool.
- The Inspector shows you information about the request, including parsed out versions of any headers, parameters, and cookies. It also shows you any text you have selected (and its length in decimal and hex) and allows you to decode selections right there.
- The Inspector shows up next to the request and response panes in other tools too.
- Click the WebSockets history tab under the Proxy tab to see if your application uses Web Sockets. Look at the traffic here and send it to Repeater to mess with it.

Repeater

Repeater allows you to edit and re-send any HTTP request or Web Socket message.

- Always send a baseline request from Repeater before you make any changes. This lets you know how the server responds to an unmodified request so you can compare that to other responses later.
- Double-click on any tab and you can give it a new name.
- Click on the plus next to the tabs and you can create a new "tab group" for when you have a lot of activity in Repeater and need to organize it better.
- Copy a URL from anywhere to your clipboard. In any Repeater request window, right-click and choose "paste URL as request" to get a default request for that URL.

FURTHER LEARNING

Check out these BHIS resources to learn more:

https://youtu.be/Gb7OQm5-Xdw

https://youtu.be/lyJihH8FYkI

https://youtu.be/xKudsnN3gkE

https://www.youtube.com/playlist?list=PL-4fu-TjKox5c3x0Z2IDjQCX8zdWl6VfhN

Intruder

Intruder lets you send many requests based on one baseline request, iterating over variables you choose in locations you define.

- Send a request to Intruder by right-clicking on it in any other tool.
- Define "insertion points" by highlighting the text you want to replace and clicking the "Add" button.
- Clear insertion points by clicking the "Clear" button. If you have something selected when you do this, only the selected insertion points will be cleared.
- Click on the question mark next to the attack type at the top (by default, it is "Sniper attack") to learn about the attack options. Don't try to memorize them—that will come with time.
- Use Payload Processing rules to modify your payloads before sending the request.
- For example, you might use "Encode as base64" if you suspect the application requires base64-encoded input in some location. This allows you to feed Intruder the values as cleartext but have them sent encoded. This lets you more easily observe what's going on.
- Intruder applies URL-encoding by default for payloads that include certain characters. Look at that list: you don't always want it to encode those characters.

Extensions

Burp Extensions are as much a part of Burp Suite as Repeater is. The list here contains more than 300 extensions. Look here for things that address whatever you're dealing with. Working with JWTs? Search for "JWT". Looking at authorization issues? Search for "Authorization".

- Sort the list of extensions by Rating to find what others get value from.
- Sort it by Popularity to find what's used often.
- Sort it by Last Updated to find new or updated extensions.
- Plan to spend some time here to find extensions that work well for you.

Learn

The Learn tab offers guides to using Burp Suite. Maybe more importantly, it has a link to Portswigger's Web Security Academy, a free resource for learning more about web app vulnerabilities and how to test for them.

- You can hide the Learn tab by going to Settings > Display and scrolling to the bottom.
- While you're in Settings > Display, you can toggle dark or light mode, too.