Testing Web Apps Using ratigan

INFORMATION SECURITY OFFICE
SECURUS // VIGILARE // INSANUS

Joshua Harper GCFE GCFA PI GSEC
Network Security Analyst
UT Austin

Prerequisites

ratigan is a graphical interface and command-builder for Ratproxy. It relies on the stock Ratproxy binaries and scripts to do the actual assessment and reporting work. In order to get the most out of ratigan, please ensure that the following prerequisites are met:

- Ratproxy installed in /usr/bin.
- Java
- A browser that can be set to route traffic through the proxy. We recommend the browser plugin FoxyProxy

Installing ratigan

ratigan is hosted on GitHub. Create and navigate to the folder where you want to install it, and then type following command:

```
git clone https://github.com/JonValt/ratigan.git
```

Starting ratigan

You start ratigan just as you start any jar:

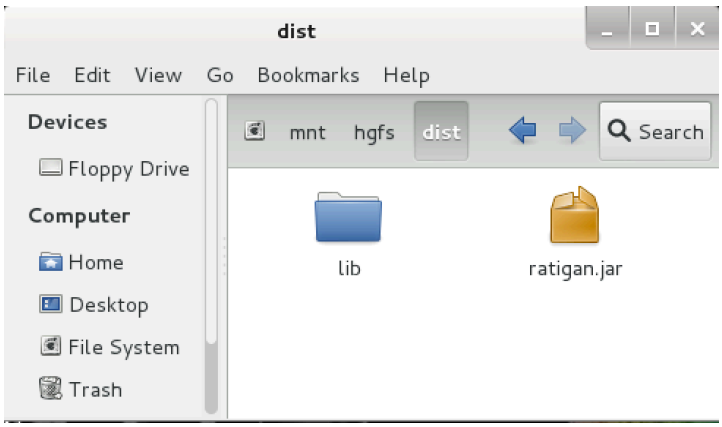

Figure 1 – GUI: Double-click the ratigan.jar file

```
# java -jar ./ratigan.jar &
```

Figure 2 – Console: Type this command

Using ratigan

This is the ratigan interface, where you'll do most of your work:

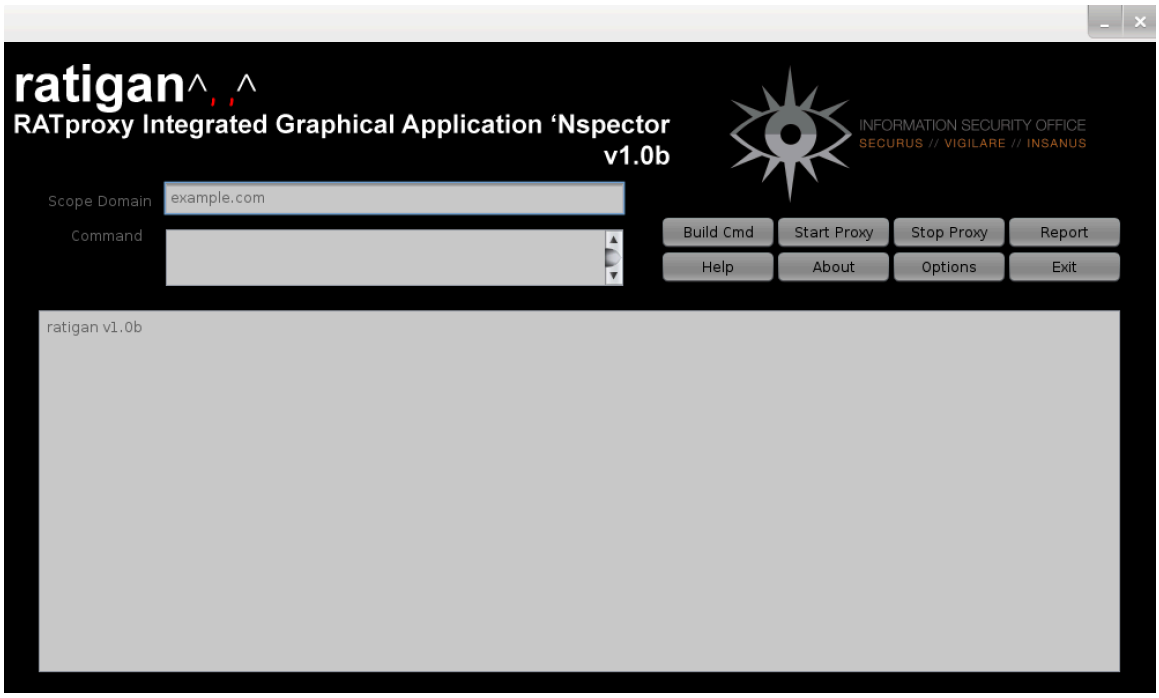

Figure 3 - The ratigan interface

Set the Target

Enter the target URL into the "Scope Domain" box. It's okay to use an IP address. You can also use an address that's a level or two up from your target application. This is useful if your application makes calls to other directories on your server.

Build the Command

Click the **Build Cmd** button. Creating and executing a command in ratigan are purposely two separate steps. This enables you to verify the command before it is run and make any necessary changes.

Verify or Modify the Command

The Command box is now filled with the command generated by your Scope Domain and other options.

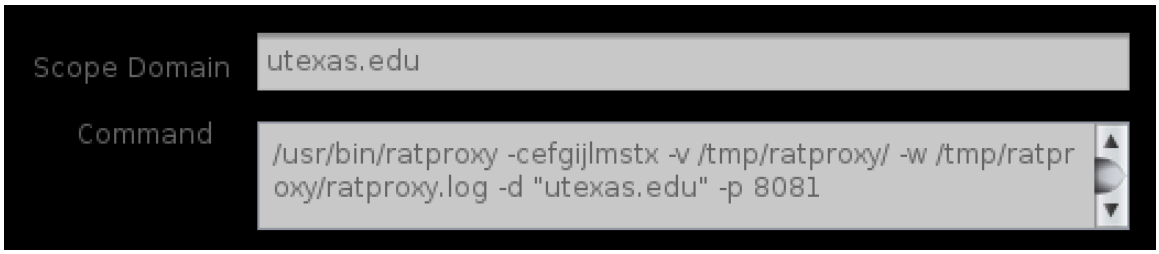

Figure 4 - Generated command displayed in window

This can be edited manually, so if you have a grip on what the various options mean, simply modify them here.

Start Ratproxy

Click **Start Proxy**. If Ratproxy was started successfully, a notification will appear in the Output window. It is now listening for traffic on the selected port.

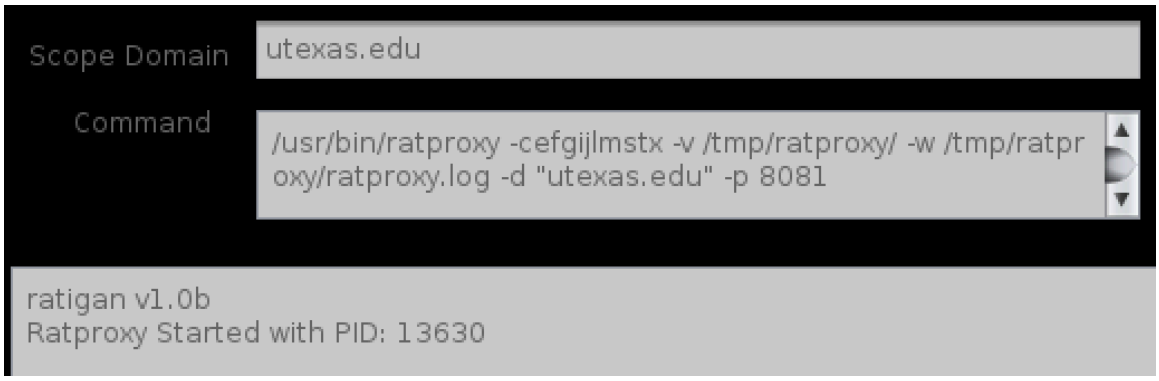

Figure 5 - Ratproxy assigned PID 13630

Configure the Browser

Direct all traffic through Ratproxy, which is now listening on 127.0.0.1 on the selected port.

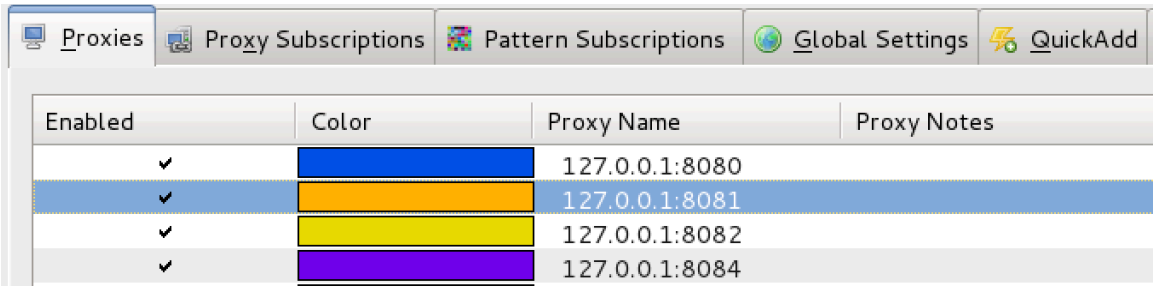

Figure 6 - FoxyProxy configured for port 8081

Test the WebApp

Use your web application in the normal fashion. Note: If you're using https, you will have to override certificate errors. This is because Ratproxy is intercepting, decrypting, and (depending on your settings) manipulating the traffic.

As you use your application, the output from Ratproxy will be displayed in the Output box.

Figure 7 - Ratproxy output displayed in Output box

Generate a Report

When you click the **Report** button, ratigan will generate a report and open it with your default browser.

ⓘ Due to the way Ratproxy works, ratigan must stop all Ratproxy processes before generating a report. When you start the proxy again, Ratproxy will automatically delete the data file that is used for generating reports. Therefore, if you start another project, you will lose your ability to create a report from the previous session.

Exit ratigan

Simply click Exit, and ratigan will quit.