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

Starting ratigan

You start ratigan just as you start any jar:

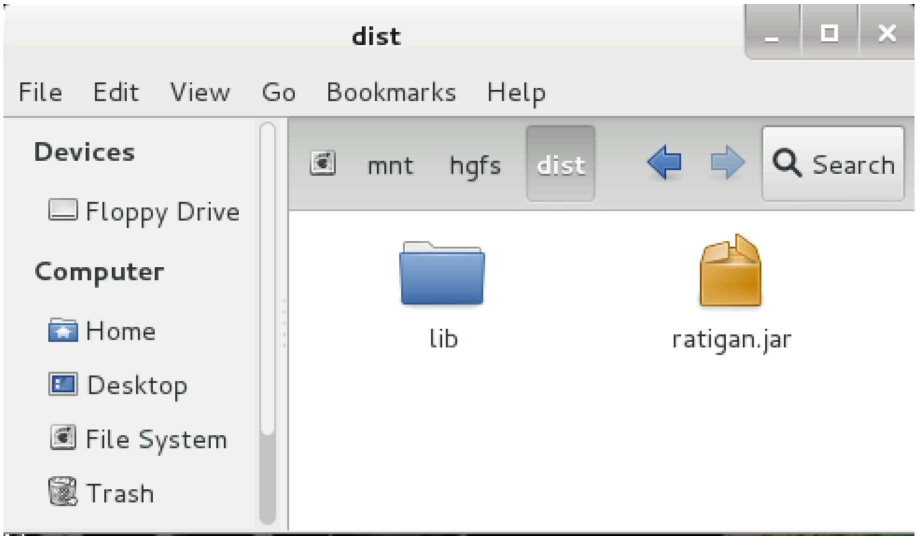
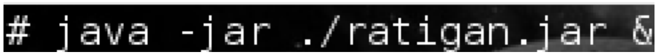


Figure 1 – GUI: Double-click the ratigan.jar file

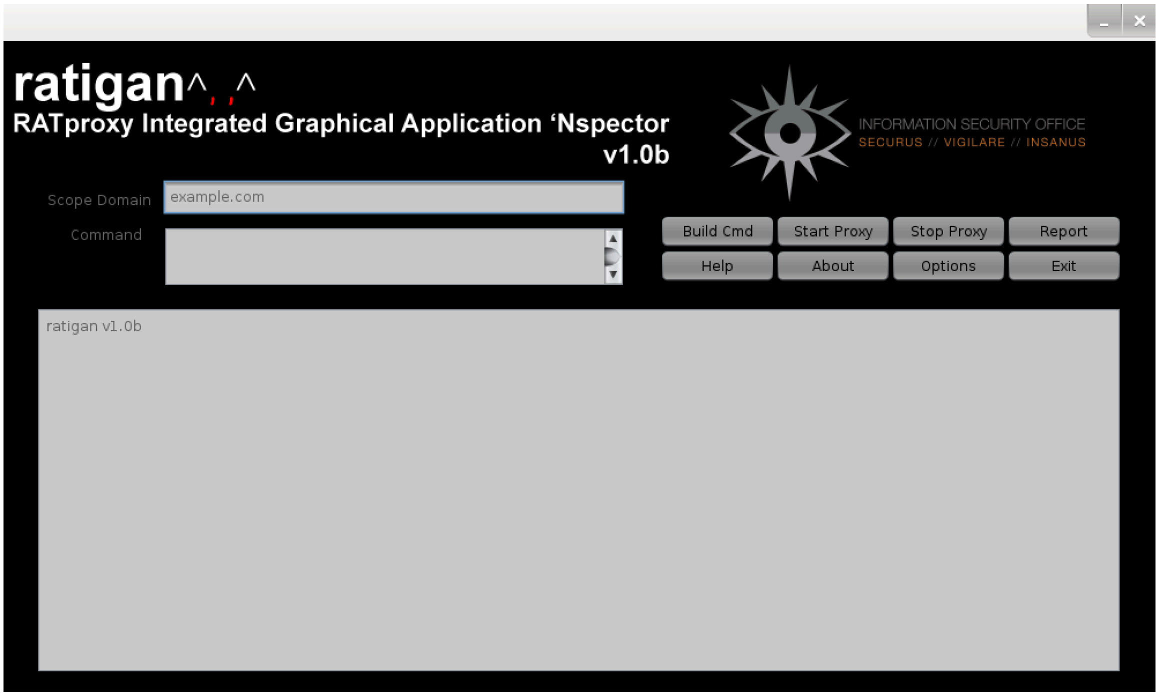


```
# java -jar ./ratigan.jar &
```

Figure 2 – Console: Type this command

Using ratigan

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


ratigan^,,^
RATproxy Integrated Graphical Application 'Nspector
v1.0b
INFORMATION SECURITY OFFICE
SECURUS // VIGILARE // INSANUS
Build Cmd
Start Proxy
Stop Proxy
Report
Help
About
Options
Exit

Scope Domain: example.com

Command:

```
ratigan v1.0b
```

Figure 3 - The ratigan interface

Set the Target

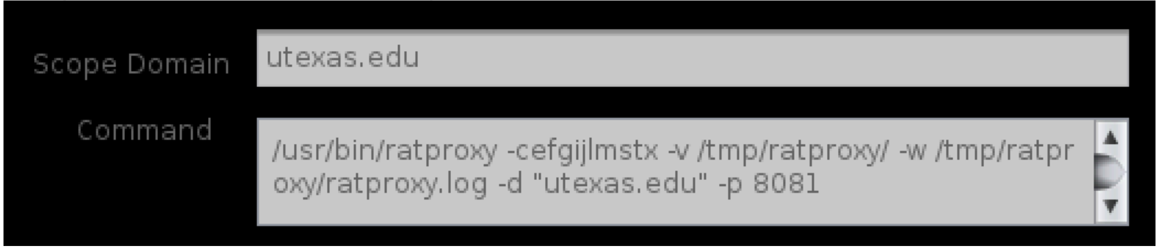
Enter the target URL into the "Scope Domain" box. It's okay to use an IP address. You can also use an address that's a level or two up from your target application. This is useful if your application makes calls to other directories on your server.

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.



Scope Domain: utexas.edu

Command:

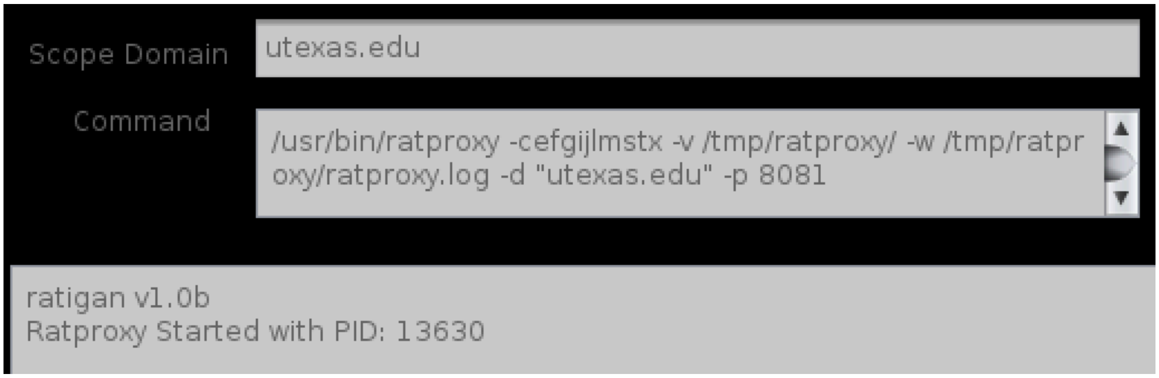
```
/usr/bin/ratproxy -cefgijlmstx -v /tmp/ratproxy/ -w /tmp/ratpr
oxy/ratproxy.log -d "utexas.edu" -p 8081
```

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.



Scope Domain: utexas.edu

Command:

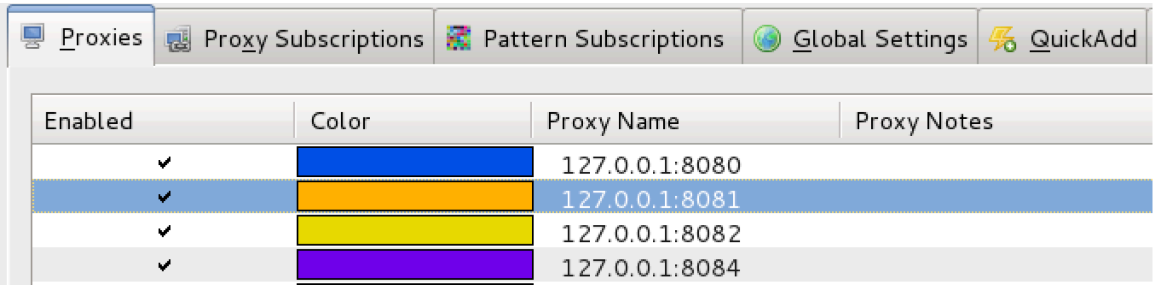
```
/usr/bin/ratproxy -cefgijlmstx -v /tmp/ratproxy/ -w /tmp/ratpr
oxy/ratproxy.log -d "utexas.edu" -p 8081
```

```
ratigan v1.0b
Ratproxy Started with PID: 13630
```

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.



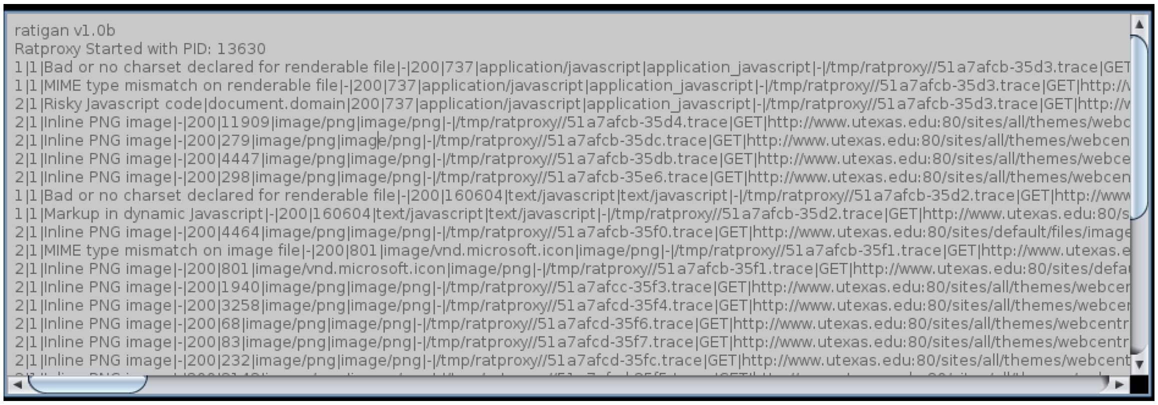
Enabled	Color	Proxy Name	Proxy Notes
✓	🟦	127.0.0.1:8080	
✓	🟧	127.0.0.1:8081	
✓	🟨	127.0.0.1:8082	
✓	🟪	127.0.0.1:8084	

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.



```
ratigan v1.0b
Ratproxy Started with PID: 13630
1|1|Bad or no charset declared for renderable file|-|200|737|application/javascript|application_javascript|-|/tmp/ratproxy//51a7afcb-35d3.trace|GET
1|1|MIME type mismatch on renderable file|-|200|737|application/javascript|application_javascript|-|/tmp/ratproxy//51a7afcb-35d3.trace|GET|http://\
2|1|Risky Javascript code|document.domain|200|737|application/javascript|application_javascript|-|/tmp/ratproxy//51a7afcb-35d3.trace|GET|http://w
2|1|Inline PNG image|-|200|11909|image/png|image/png|-|/tmp/ratproxy//51a7afcb-35d4.trace|GET|http://www.utexas.edu:80/sites/all/themes/webc
2|1|Inline PNG image|-|200|279|image/png|image/png|-|/tmp/ratproxy//51a7afcb-35dc.trace|GET|http://www.utexas.edu:80/sites/all/themes/webcen
2|1|Inline PNG image|-|200|4447|image/png|image/png|-|/tmp/ratproxy//51a7afcb-35db.trace|GET|http://www.utexas.edu:80/sites/all/themes/webce
2|1|Inline PNG image|-|200|298|image/png|image/png|-|/tmp/ratproxy//51a7afcb-35e6.trace|GET|http://www.utexas.edu:80/sites/all/themes/webcen
1|1|Bad or no charset declared for renderable file|-|200|160604|text/javascript|text/javascript|-|/tmp/ratproxy//51a7afcb-35d2.trace|GET|http://www
1|1|Markup in dynamic Javascript|-|200|160604|text/javascript|text/javascript|-|/tmp/ratproxy//51a7afcb-35d2.trace|GET|http://www.utexas.edu:80/s
2|1|Inline PNG image|-|200|4464|image/png|image/png|-|/tmp/ratproxy//51a7afcb-35f0.trace|GET|http://www.utexas.edu:80/sites/default/files/image
2|1|MIME type mismatch on image file|-|200|801|image/vnd.microsoft.icon|image/png|-|/tmp/ratproxy//51a7afcb-35f1.trace|GET|http://www.utexas.e
2|1|Inline PNG image|-|200|801|image/vnd.microsoft.icon|image/png|-|/tmp/ratproxy//51a7afcb-35f1.trace|GET|http://www.utexas.edu:80/sites/defa
2|1|Inline PNG image|-|200|1940|image/png|image/png|-|/tmp/ratproxy//51a7afcc-35f3.trace|GET|http://www.utexas.edu:80/sites/all/themes/webcer
2|1|Inline PNG image|-|200|3258|image/png|image/png|-|/tmp/ratproxy//51a7afcd-35f4.trace|GET|http://www.utexas.edu:80/sites/all/themes/webcer
2|1|Inline PNG image|-|200|68|image/png|image/png|-|/tmp/ratproxy//51a7afcd-35f6.trace|GET|http://www.utexas.edu:80/sites/all/themes/webcentr
2|1|Inline PNG image|-|200|83|image/png|image/png|-|/tmp/ratproxy//51a7afcd-35f7.trace|GET|http://www.utexas.edu:80/sites/all/themes/webcentr
2|1|Inline PNG image|-|200|232|image/png|image/png|-|/tmp/ratproxy//51a7afcd-35fc.trace|GET|http://www.utexas.edu:80/sites/all/themes/webcent
```

Figure 7 - Ratproxy output displayed in Output box

Generate a Report

When you click the **Report** button, ratigan will perform several actions behind-the-scenes:

- Stop any running Ratproxy processes
- Determine if a report file already exists
  - YES – Open report in default browser
  - NO – Generate a report and change **Report** button to say "**View**."

The file checking ensures that ratigan will not overwrite a previously created report. The default location for the report file is /tmp/ratproxy/ratproxy-report.htm.

Exit ratigan

Simply click Exit, and ratigan will quit.