The Evil Tester's Guide to HTTP Proxies

A Tutorial for TestNet May 2013

Alan Richardson
@eviltester
www.eviltester.com
www.compendiumdev.co.uk
www.seleniumsimplified.com

slides: http://unow.be/at/gtn_tute

Logistics

- 09:30
- xx:xx half hour break
- 13:00

Only 3 hours!

1st Hour: Theory & Modern Browsers

- 20 mins Intro, basic theory
- 5 Mins 'Modern Browsers
- 5 Mins Demo
- 15 minutes browser exercise
- 15 minutes debrief

2nd Hour: BurpSuite

- 10 mins Introduction to proxies
- 20 mins BurpSuite overview
- 15 minutes BurpSuite Exercise
- 15 minutes BurpSuite debrief and questions

3rd Hour: Fiddler & End Notes

- 15 mins fiddler overview
- 15 minute Exercise
- 15 minute debrief and questions
- 10 minute end notes
- 5 minutes Q&A

Blurb: Evil Tester guide - HTTP proxies

I test a lot of web applications. I use proxy servers to interrogate and manipulate web traffic. So in this tutorial I want to introduce you to the basics of proxy servers, using BurpSuite and Fiddler.

We will cover and go beyond the obvious interrogation and manipulation traffic and also look at how to use autoresponders, custom rules and traffic generators. The different capabilities of the tools and how to use them in combination.

And as a bonus we will look at the new features in modern browsers that help you achieve some of the proxy benefits out of the box, for those moments when you have to test unarmed.

As well as the tools I want to cover the thought processes and models that help you get the best from the tools because "Form can follow features" and "Terrain can inform technique".

Technical Web Testing: A Model

The MORIM Loop

- Model
- Observe
- Reflect
- Interrogate
- Manipulate

The MORIM Loop - Model

- *Model*
  - Build a layered model of the application functionality, flows, technology usage, etc.

- *Observe*
- *Reflect*
- *Interrogate*
- *Manipulate*

The MORIM Loop - Observe

- *Model*
- *Observe*
  - At every layer, what can you see?
  - Can you increase the depth of observation.
  - Do you understand what you see?
  - What else could you observe?

- *Reflect*
- *Interrogate*
- *Manipulate*

The MORIM Loop - Reflect

- *Model*
- *Observe*
- *Reflect*
  - Expand the model,
  - Intent - for deliberate action
  - Analyse the observations
  - What does that imply?
  - How? Risks? What else? When?
- *Interrogate*
- *Manipulate*

The MORIM Loop - Interrogate

- *Model*
- *Observe*
- *Reflect*
- *Interrogate*
  - Deep dive into observed data
  - Breakpoint
  - Correlate data changes with state
  - etc.

- *Manipulate*

The MORIM Loop - Manipulate

- *Model*
- *Observe*
- *Reflect*
- *Interrogate*
- *Manipulate*
  - Edit the data
  - Change the state
  - Edit the communication
  - Change the environment context
    e.g. speed, memory, etc.

The MORIM Loop - Utilisation

- Repeat
- Transpose - do the events in any order
- Learn
- Deliberately decide what to try next
- Do it - take advantage of what happens

During all the exercises; Consider:

Observation

- What are you observing. What are you not observing. What do you want to observe? Why?

Interrogation

- What do you want to see in more detail? How can you do that? Why?

Manipulation

- What do you want to amend? How could you? Why?

Our Basic Web Technology Knowledge

High Level Generic Architecture

Browser

- client side state
- Cookie Management
- Local Storage
- HTML rendering
- JavaScript Execution
- etc.

Traffic

<-HTTP->

- forms
- XML
- JSON
- etc.

Server

- Web Server
- App Server
- Database

- server side state

Introduction to Modern Browsers

Modern Browsers

- Dev Tools
- Observe Network Traffic
- Interrogate & Manipulate
  - DOM
  - Data - cookies, local storage
- Differing capabilities between browsers

"Don't get hung up on 'I need to test on BrowserX' - use them all, even while you focus on BrowserX"

Quick Demo of Modern Browser

- Interrogate Dom?
- Manipulate Dom?
- Observe Cookies?

- Interrogate Cookies?
- Manipulate Cookies?

- Observe Network Traffic?
- Interrogate Traffic?
- Manipulate Traffic?

Augment Browsers

- Out of the box experience continually improves
- Use browser plugins to increase the functionality of the browser even further

Gruyere - Cloud app to test against

A Google App Engine hosted application to learn security testing for common vulnerabilities.

Read the Instructions

- http://google-gruyere.appspot.com/

Create a new instance

- http://google-gruyere.appspot.com/start

For local App Testing

- WebGoat
  - http://code.google.com/p/webgoat/

Or anything from BitNami

bitnami.org

Modern Browser Exercise

1. Decide on a browser: IE, Firefox, Opera, Chrome
2. Find the Dev Tools in the browser
3. Visit http://google-gruyere.appspot.com/start
4. Explore and investigate the Browser capabilities using this app
5. Debrief in 15 mins
   - What "Observe, Interrogate, Manipulate" capabilities did the browser have?
   - What did you want them to have?
   - Other thoughts?

For full control, Use a Proxy...

Introduction to Proxies

slides: http://unow.be/at/gtn_tute

What is an HTTP Proxy?

- Sits between browser and server
- route all requests through the proxy

Browser -> Request -> Proxy -> Server

Browser <- Proxy <- Response <- Server

Https handled by 'man in the middle' certificate use.

Why should a tester care?

- Learn
  - HTTP
  - JSON
  - App Architecture
- Observe & Manipulate Traffic
- Simulate Network Speeds
- Simulate different browsers
- Test new css and js without a release to main site
- Test extreme '4xx', '5xx' conditions

When should you use it?

- Almost all the time

When should you not use it?

- confirm a defect happens without the proxy
- streaming?
- long polling?

A proxy is invasive, and can impact your results. So you need to double check your results without the proxy.

But the value trumps the risk.

How?

Quick Demo

Proxies and their capabilities

Proxies we will cover today

- BurpSuite
- Fiddler

- Capabilites
- Demos
- Exercises

Generic Testing Requirements

Traffic {Request, Response} CRUD

- Create - Generate new requests
- Read - Observe Traffic
  - Requests
  - Responses
- Update -
  - Manipulate Requests & Responses
    - Manually
    - Automatically
  - Replay Requests
- Delete - block requests or responses

Configure Browser to use a Proxy

Configure Browser to use a Proxy

- Chrome, IE all use the System Internet Settings
- Firefox and Opera can maintain proxy settings independently of system settings

Configure Chrome to use a Proxy

- Chrome\Settings search for proxy
- Use the normal system proxy settings
- Chrome Incognito and normal mode share proxy settings

Configure Firefox to use a Proxy

- Firefox\Options
  - Advanced\Network
    - Connection [Settings...]
    - Manual proxy configuration:
    - use value listed in Proxy\Options Listeners
    - ignore the "No Proxy For"
- If you already configured IE or Chrome then you could use System Proxy Settings

Configure Opera to use a Proxy

- Settings\Preferences
  - Advanced\Network
  - [Proxy Servers...]
  - use config from Proxy\Options
- F12 can quickly toggle proxy on off once configured

Configure IE to use a Proxy

- Config \ options
  - Connections
    - Lan settings
      - Use Proxy Server
        - use details from Proxy\Options

You may be asked about proxy certificate (BurpSuite portswigger)

- Adhoc - Add it as an exception
- To remove exception
  - Firefox
    - Options\Advanced\Encryption
    - view certificates
      - servers (PortSwigger)
  - Chrome
    - Settings \ search for manage certificates
  - Opera
    - Preferences
      - Advanced\Security
      - Manage Certificates...
  - IE
    - Config \ Internet Options \ Content [Certificates]

BurpSuite

What is BurpSuite?

- Java based Proxy
- Professional and Free License
  - Pro designed for security professionals
  - Free version usually good enough for testing
- Book: "The Web Application Hacker's Handbook"
- http://portswigger.net/burp/download.html

Basic Features For Testing

- Proxy
- Spider
- Repeater
- Sequencer
- Decoder
- Comparer

How to Install & Run

- Download the .jar file
  - http://portswigger.net/burp/download.html
- Double click or "java -jar burpsuite_free_vx.x.jar"
  - where x.x is the version you downloaded

BurpSuite Basics

- Tabbed GUI
- Proxy\Options
- Configure Browser
- Intercept
- Obeserve with History Tab
- Repeater to replay and manipulate
- Site Map
- Spider
- Decoder
- Intruder - variety of params

Exercise - explore tool and proxy capabilities

- 20 mins explore, 10 mins debrief
- Use BurpSuite on guyere
  - Setup the proxy
  - Config browser to point to browser
  - Choose a site and browse
  - View the Traffic
  - View sitemap
    - visit pages you haven't been that sitemap found
  - Repeat requests
  - Tamper Traffic
  - do any of the pages lend themselves to sequencing?

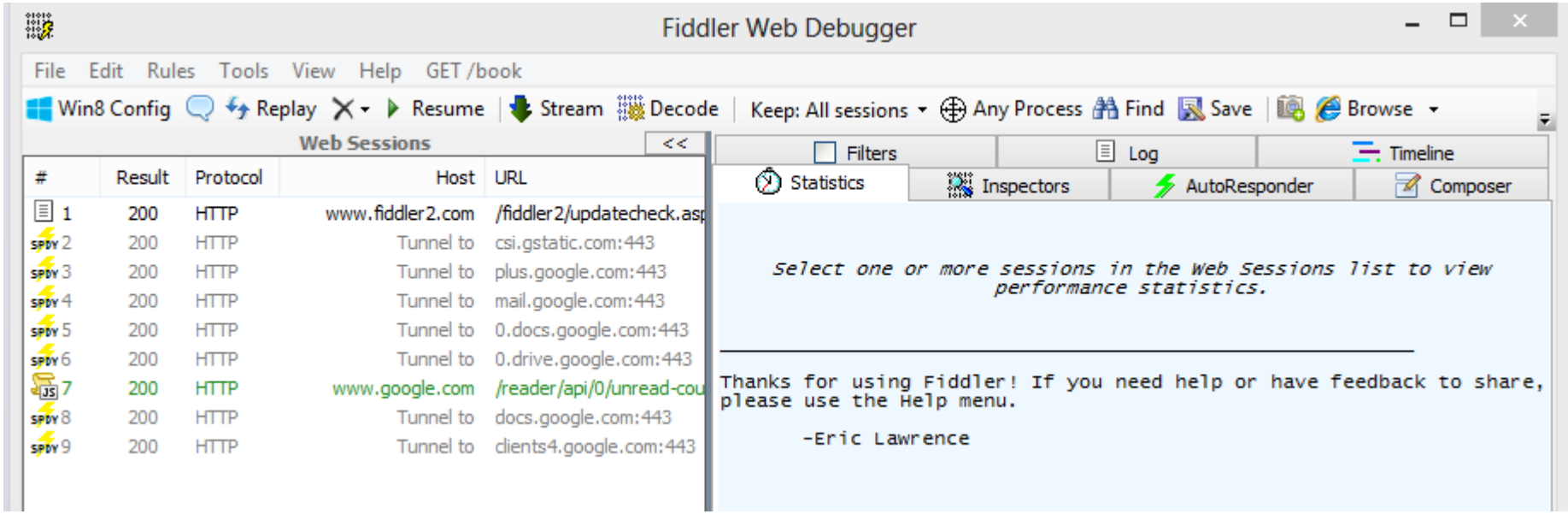
Debrief

- Comments, Questions?

Fiddler

What is Fiddler?

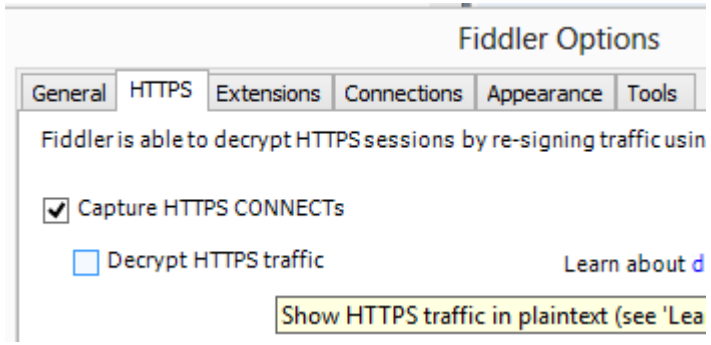
- .net based (v2 & v4)
- http://www.fiddler2.com/
- now owned by Teleric



Obvious Differences

- Automatically hooks into Windows System Proxy
  - IE & Chrome use by default without configuration
  - This makes it good for beginners

- HTTPS decryption off by default
  - Tools \ Fiddler Options
    - HTTPS tab
      - Decrypt HTTPS traffic



Fiddler Extensions

- www.fiddler2.com/fiddler2/extensions.asp
  - Formatters
  - Windows 8 "Metro"
  - Android & iOS Certificate maker
  - Request Differ
  - SAZ Clipboard Util
  - Geo spoofing
  - Rules Editor
  - Privacy Scanner
  - Performance Tester Helper
  - Stress Testing
  - Security Testing - Watcher & Ammonite & X5s
  - Fuzzing - intruder21
  - etc.

Fiddler Basics

- Firefox Hook "Tools \ Monitor with Fiddler"
- WebSessions Pane - History
- Statistics Tab
- Inspectors Tab
- AutoResponder Tab
- Composer Tab
- Filters Tab
- Timeline Tab
- Config Options
- Decode with TextWizard
- Replay
- Export Sessions

Exercise - explore proxy functionality and compare with BurpSuite

- Any new functionality I didn't mention?
- Which is easier?
- Any missing functionality?
- Can you chain proxies?

Psychology of Proxying

Isn't this just Security Testing?

Yes, No?

Opinions?

Observation & Manipulation

Comments on what you observed?

- What didn't you observe?
- What did you want to observe?
- What could you not observe?

Comments on Manipulation?

- What did you manipulate?
- What did you want to manipulate?
- What could you not manipulate?

What makes a difference?

You can manipulate a whole bunch of things, why would you want to manipulate the:

- Header?
- Body?
- Request URI?
- Params?
- Payload?

Inspiration from Form

What can this tool do? == New test ideas!

e.g.

- what does the autoresponder feature let me do?
- What could I use the save as HAR file for?
- etc.

Recommended For Self Study

Videos & Courses

- Evil Tester Videos on Burp on Youtube
  - www.youtube.com/watch?v=ft5MSmf42Kw
  - www.youtube.com/watch?v=JmAk1OVwp-4
- ZAP
  - www.youtube.com/watch?v=QG2RCZHMEkM
  - www.youtube.com/user/psiinon?feature=watch
- Technical Web Testing 101
  - www.udemy.com/technical-web-testing-101
  - Free Udemy Course

Books

- The Web Application Hacker's Handbook
  - www.amazon.com/exec/obidos/ASIN/1118026470
  - www.amazon.co.uk/exec/obidos/ASIN/1118026470

- Debugging with Fiddler by Eric Lawrence
  - www.amazon.com/exec/obidos/ASIN/1475024487
  - www.amazon.co.uk/exec/obidos/ASIN/1475024487

Proxies

- BurpSuite
  - http://www.portswigger.net/burp/
- Fiddler
  - http://www.fiddler2.com/fiddler2/
- zaproxy (Zed Attack Proxy)
  - http://code.google.com/p/zaproxy/
  - https://twitter.com/zaproxy

Apps to test against

- http://google-gruyere.appspot.com/part1
  - http://google-gruyere.appspot.com/start
- https://hack.me/
- http://demo.testfire.net/
- WebGoat
  - http://code.google.com/p/webgoat/

- Lists of Apps to Test Against
  - http://blog.taddong.com/2011/10/hacking-vulnerable-web-applications.html

Q & A

Alan Richardson is an Independent Test Consultant based in the UK. He offers training and consultancy in Selenium WebDriver, exploratory and technical web testing.

- uk.linkedin.com/in/eviltester

Contact Alan for training and consultancy tailored to your needs:
alan@compendiumdev.co.uk

Blogs and Websites

- SeleniumSimplified.com
- EvilTester.com
- Testing Papers and Tools
  - CompendiumDev.co.uk

Twitter: @eviltester

Online Training Courses

- Technical Web Testing 101
  - Unow.be/at/udemy101
- Intro to Selenium
  - Unow.be/at/udemystart
- Selenium 2 WebDriver API
  - Unow.be/at/udemyapi

Videos

youtube.com/user/EviltesterVideos

Books

Selenium Simplified

Unow.be/rc/selsimp