BurpSuite

The Swiss army knife of security tools
Glancing Blow
The Tab Functionality

<table>
<thead>
<tr>
<th>Burp</th>
<th>Intruder</th>
<th>Repeater</th>
<th>Window</th>
<th>Help</th>
<th>Target</th>
<th>Proxy</th>
<th>Spider</th>
<th>Scanner</th>
<th>Intruder</th>
<th>Repeater</th>
<th>Sequencer</th>
<th>Decoder</th>
<th>Comparator</th>
<th>Extender</th>
<th>Options</th>
<th>Alerts</th>
</tr>
</thead>
</table>

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders.
Proxy – Where It Starts

• A proxy is a piece of software (it could be hardware)
• It sits between one thing and another and behaves as the middleman
• Example
  – You are at your browser communicating with a web app
  – You decide you want a proxy sitting between your browser and the app
  – So, you start a proxy server running and then you tell your browser to send requests to the proxy
  – The proxy receives requests from the browser and forwards them to the web app
  – When responses come back, the proxy routes them to you
Proxy – Where It Starts

Your Browser → The Proxy Server → The Web App

Matching Ports

This has to be agreed upon
Proxy – Why Would You Do This?

• Because the proxy provides a service you want
  – Encryption of traffic
  – Anti-virus scanning
  – Keeping track of sites visited
  – Stopping you from reaching some sites

  – Giving you control over what goes on
  – Allowing you to see what is going on in the exchange
  – Providing services to make your job easier

• The proxy can make your life much simpler
Getting Burp Suite

• There are two versions
  – Professional, about $300/year
  – Not so professional, free, and missing some cool stuff

• Download it from http://portswigger.net

• It's Java App, so you just download the jar file

• Put it somewhere convenient
  – /home/opt/BurpSuite or C:/opt/BurpSuite or whatever

• To start it, use
  – java -Xmx1024m -jar <path to the jar file>
  – The amount of memory can be lower or larger, but 256m is about the min
How to Proxy with Burp

• Start up Burp Suite
How to Proxy with Burp

- Proxy -> Intercept

You might want to start with Intercept off, so click on it.
How to Proxy with Burp

• Proxy -> Options

This is where your proxy listens. 8080 can be changed. Usually it listens on the system where it is running.

If running isn't checked, check it.
Setting Up Your Browser – Local Burp

• Firefox
  – Tools -> Options (Win) or Edit -> Preferences (Lin)
  – Advanced -> Connection -> Settings
  – Check Manual Proxy Settings

  – Use this proxy server ...

  – Change the port if desired
Setting Up Your Browser – Local Burp

• IE
  – Tools -> Internet Options -> Connections -> LAN Settings
  – Configure Proxy Settings
  – Check Manual Proxy Settings

  – Use this proxy server ...

  – Check this if you want

  – Change the port if desired
Setting Up Your Browser – Local Burp

- Advanced tab, but the default is typically correct
Testing Your Setup

- Chromium and Safari left to the reader
- You are now set up.

- To test it, click on the Proxy -> History tab
- Then go to some URL in your browser
The Setup

Simple form

and response

```
select name, userid from accounts where account='1234'
You are identified as
name userid
Joe B | joe
```
Information in the History Tab

- First, there is a huge amount of information just in the History tab.
### Request Headers

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>/cs476/sql/ HTTP/1.1</td>
</tr>
<tr>
<td>Host</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0</td>
</tr>
<tr>
<td>Accept</td>
<td>text/html,application/xhtml+xml,application/xml;q=0.9,<em>/</em>;q=0.8</td>
</tr>
<tr>
<td>Accept-Language</td>
<td>en-US,en;q=0.5</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>gzip, deflate</td>
</tr>
<tr>
<td>DNT</td>
<td>1</td>
</tr>
<tr>
<td>Referer</td>
<td><a href="http://127.0.0.1/cs476/">http://127.0.0.1/cs476/</a></td>
</tr>
<tr>
<td>Connection</td>
<td>keep-alive</td>
</tr>
</tbody>
</table>

**The request headers**
Anything useful here?

The response
## Response Headers

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP/1.1</td>
<td>200 OK</td>
</tr>
<tr>
<td>Date</td>
<td>Tue, 04 Feb 2014 12:21:18 GMT</td>
</tr>
<tr>
<td>Server</td>
<td>Apache/2.2.25 (Unix) mod_ssl/2.2.25 OpenSSL/1.0.1f DAV/2 PHP/5.5.8</td>
</tr>
<tr>
<td>Last-Modified</td>
<td>Tue, 21 Jan 2014 19:49:34 GMT</td>
</tr>
<tr>
<td>ETag</td>
<td>&quot;b084-de-4f0804eb7ef80&quot;</td>
</tr>
<tr>
<td>Accept-Ranges</td>
<td>bytes</td>
</tr>
<tr>
<td>Content-Length</td>
<td>222</td>
</tr>
<tr>
<td>Keep-Alive</td>
<td>timeout=5, max=100</td>
</tr>
<tr>
<td>Connection</td>
<td>Keep-Alive</td>
</tr>
<tr>
<td>Content-Type</td>
<td>text/html</td>
</tr>
</tbody>
</table>
## Submit Request Params

### Table:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>account</td>
<td>1234</td>
</tr>
</tbody>
</table>

**GET request to /cs476/sqli/submit.php**
Popup Menu Options

- Right-click
- This how you can pass a particular URL to one of the Burp Suite tool.
  - Repeater
  - Spider
  - Active Scan
  - Passive Scan
  - Intruder
A Live Example
Homework 3

- [http://www.hackthissite.org](http://www.hackthissite.org)
- Go there and register
  - The passwords are a pain
  - Start with the basic mission and move on up
  - You should be able to get to through at least 3 of the Realistic Missions
  - We are going to talk about some of this next time
Homework 4

• The topic is BurpSuite