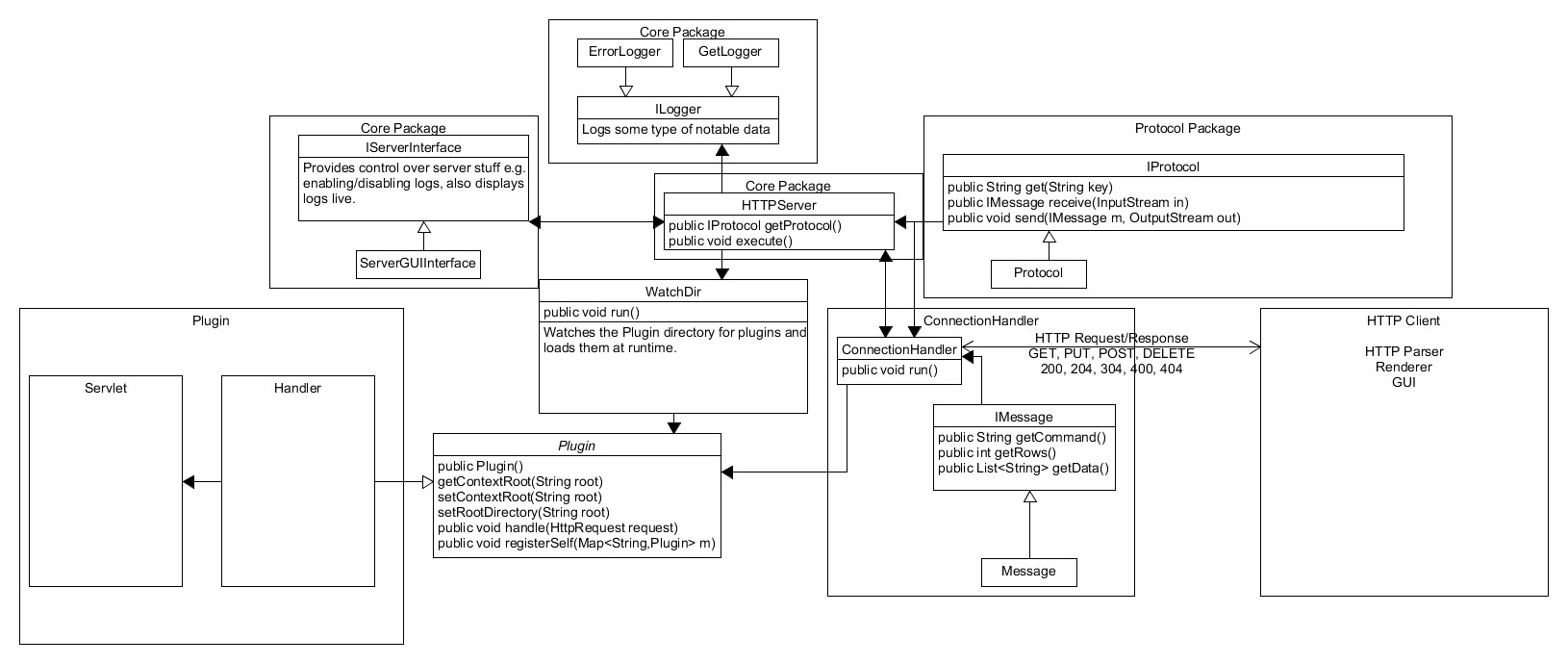
|  |
| --- |
| Rose-Hulman Institute of Technology |
| Simple Web Server |
| CSSE477 |

|  |
| --- |
| Gregory Bollivar and L.E. Davey  11-2-2015 |

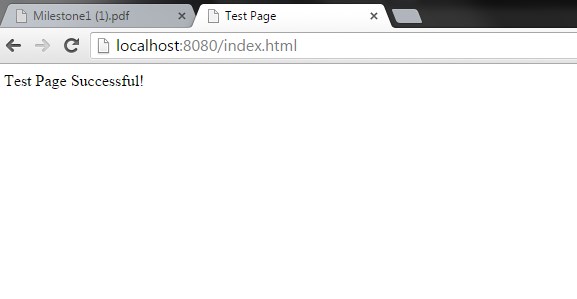
1.)    
Changes to the diagram have occured

2.) About the “detailed diagram” we believe that a.) our detailed diagram is very much the same as the diagram above, b.) it has not changed significantly.

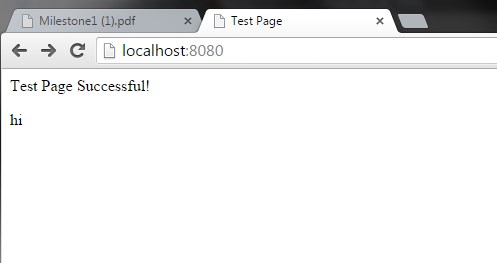
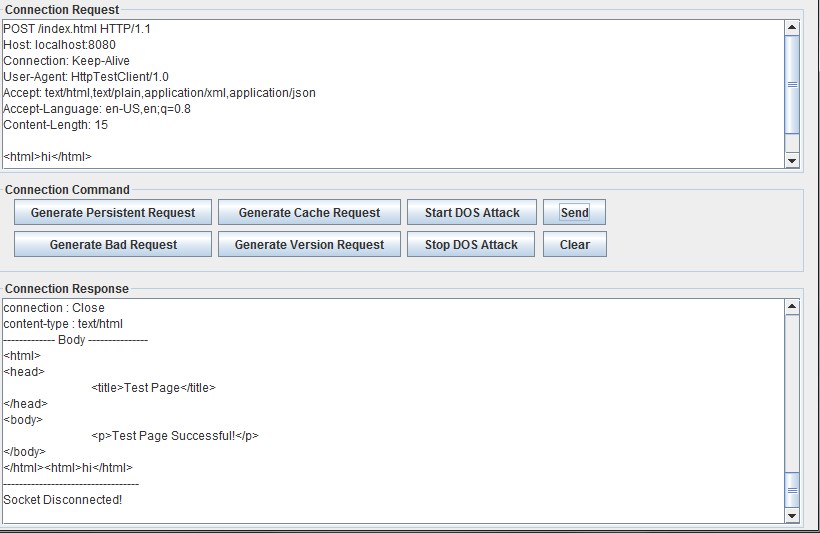
3.) Patterns: Delegating to an interface, Strategy, WatchDir, no additional patterns

4.) Improvements: Our counting, improve client to generate dummy post/put/delete, we increased the security of the system, we restricted access to the plugins folder, added logging, throttled high using clients and attempted to prevent threadbombs.

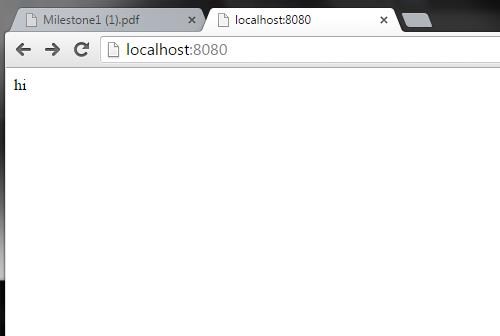
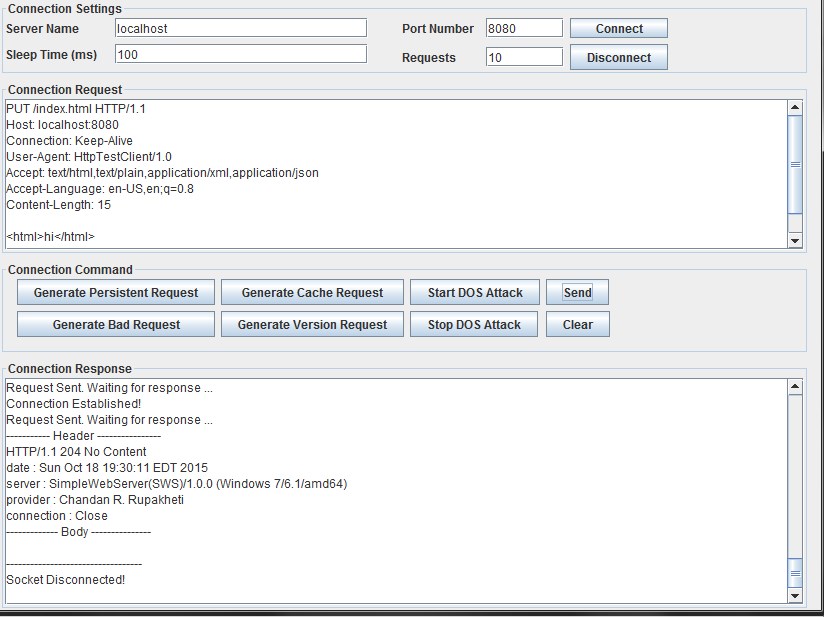
5.) GET:



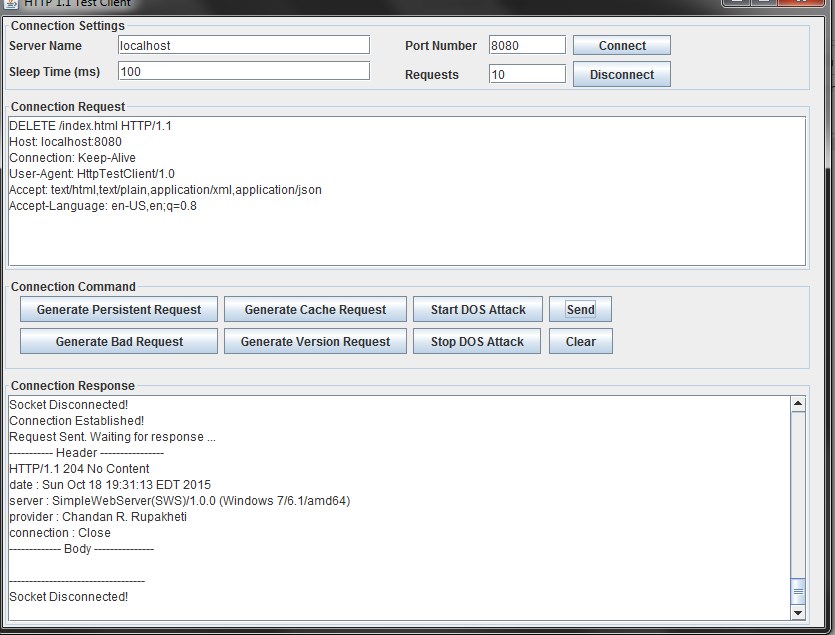
POST:

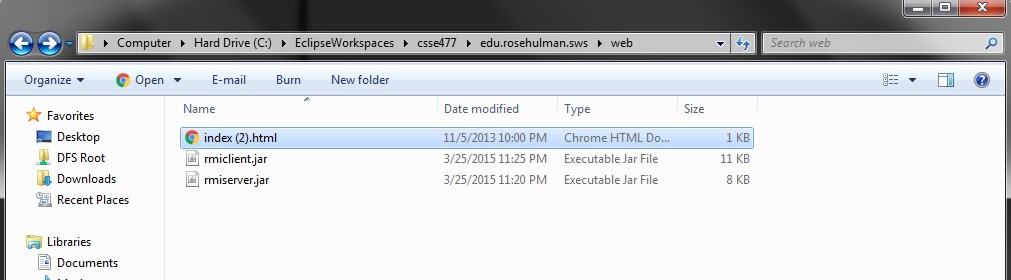
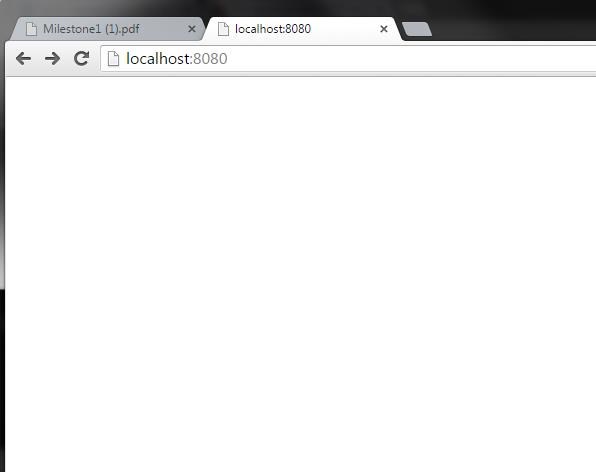


PUT:



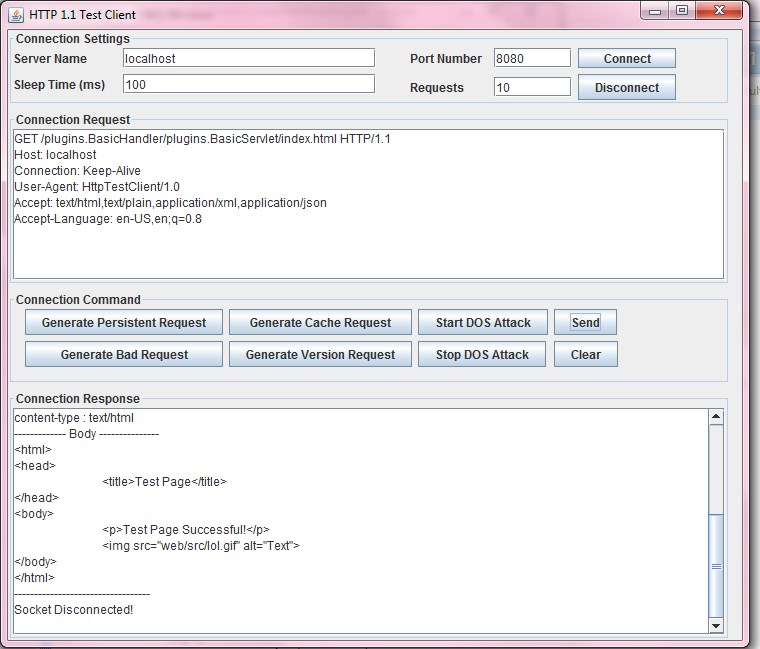
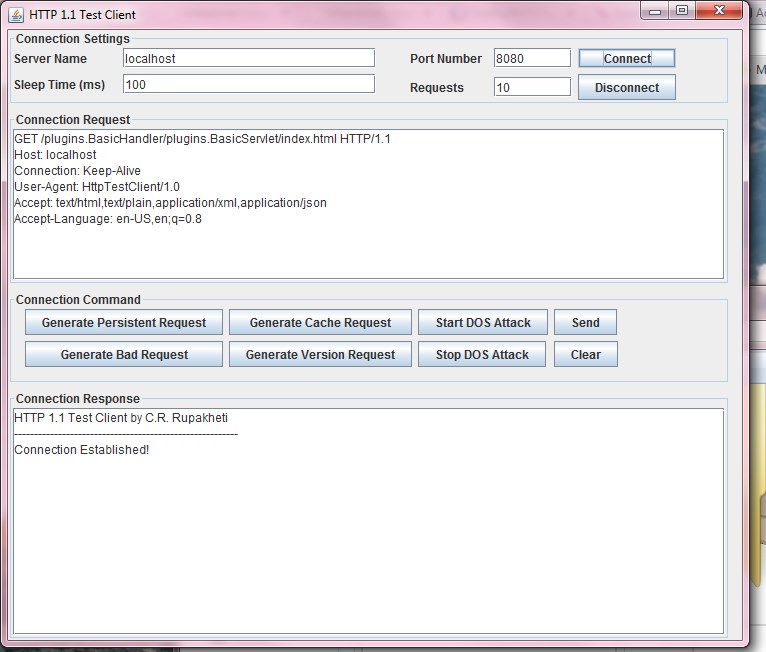
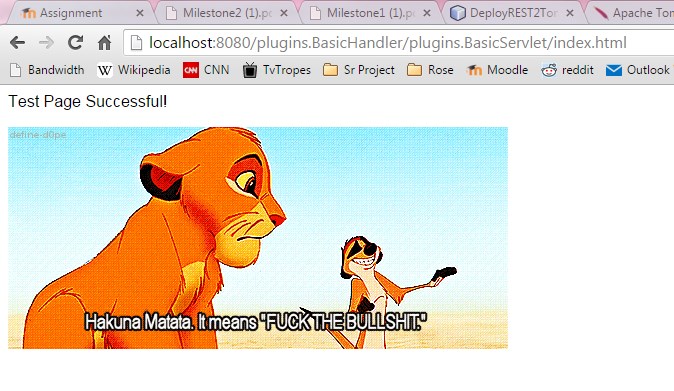
DELETE:



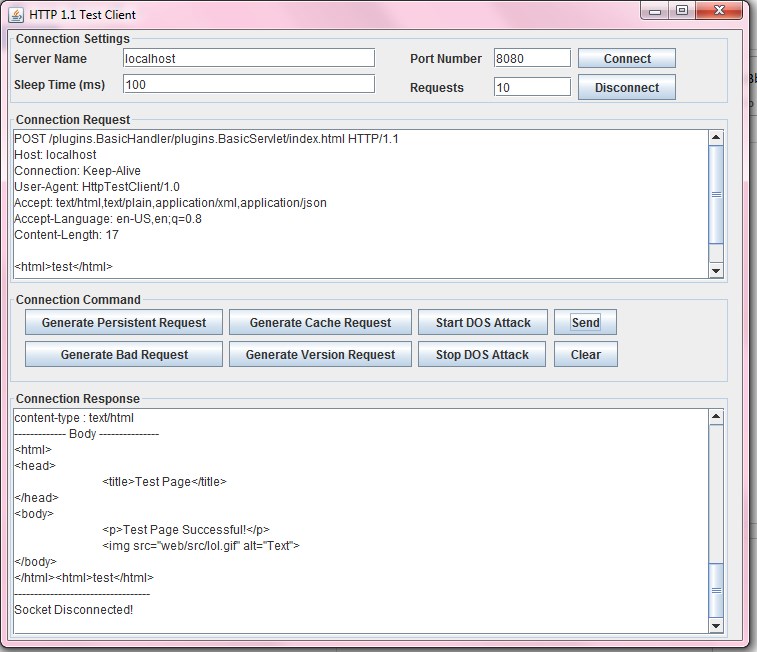
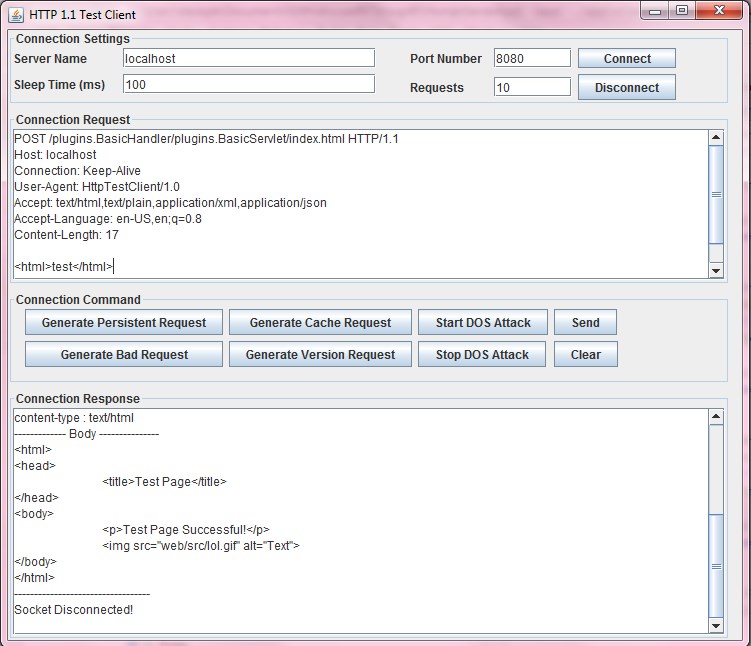


Original GPPD Handler:

GET:



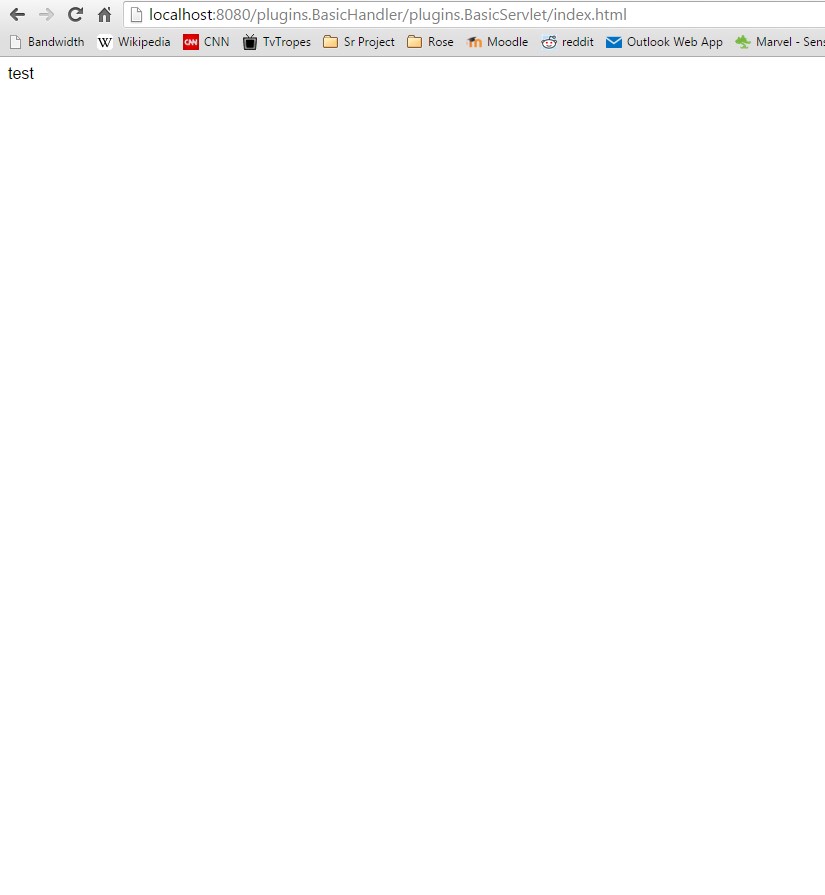
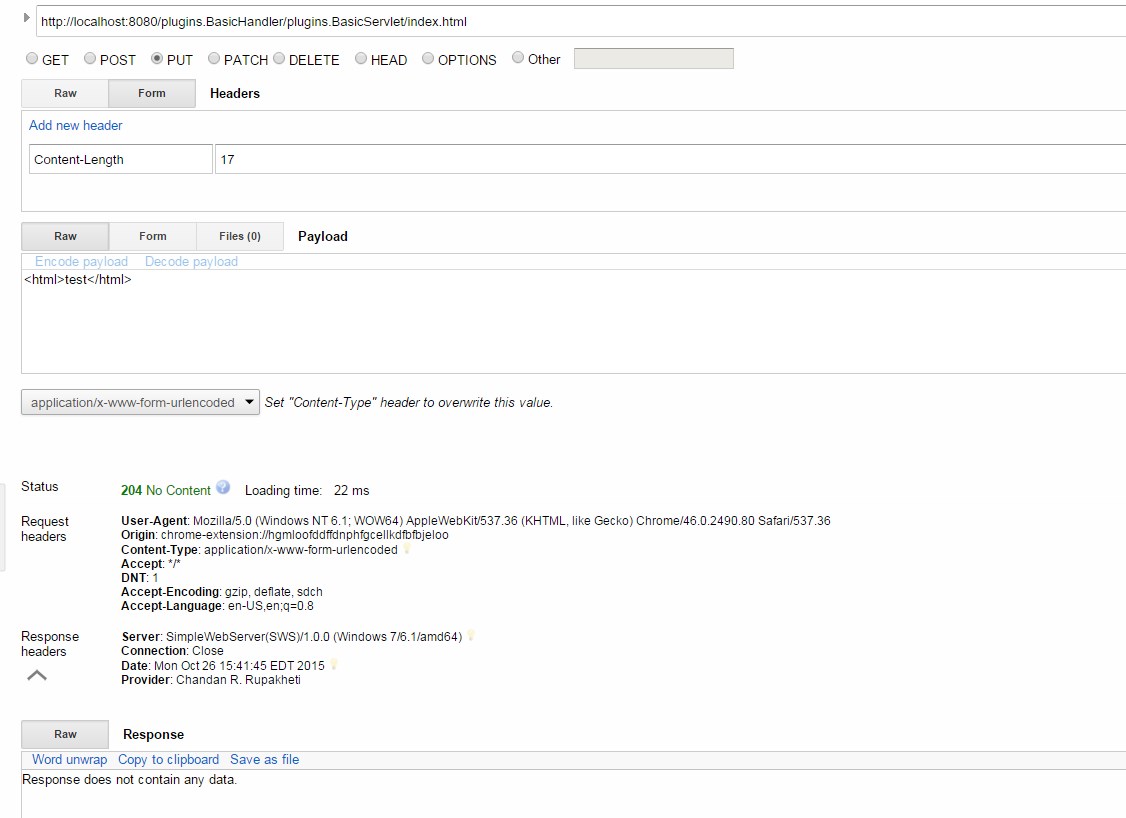
POST



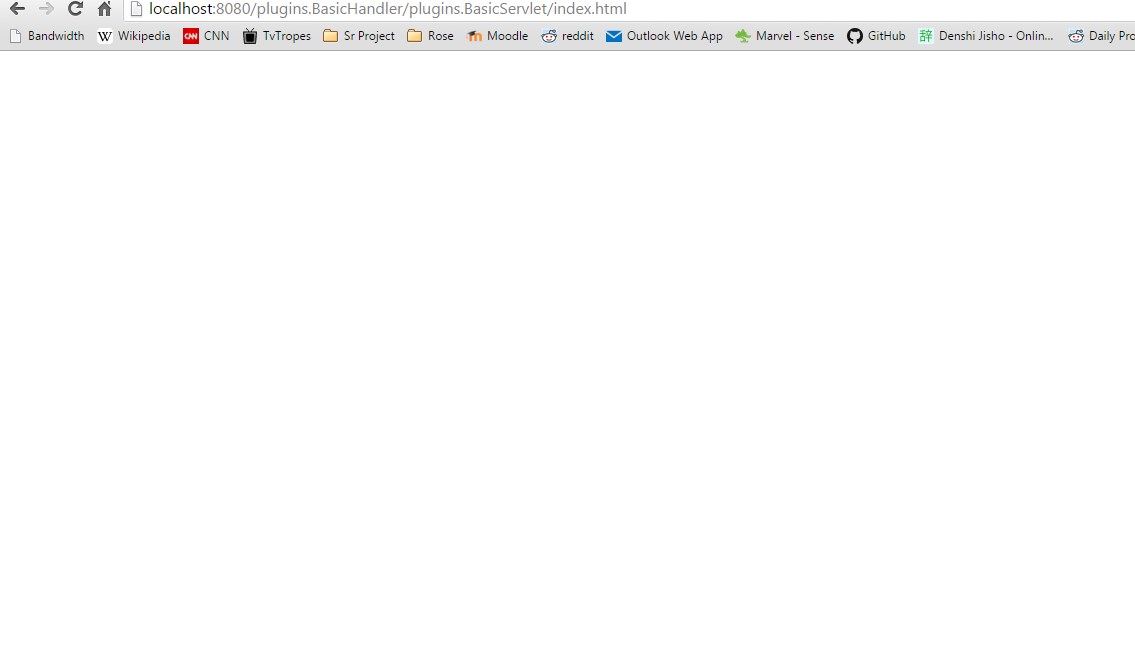
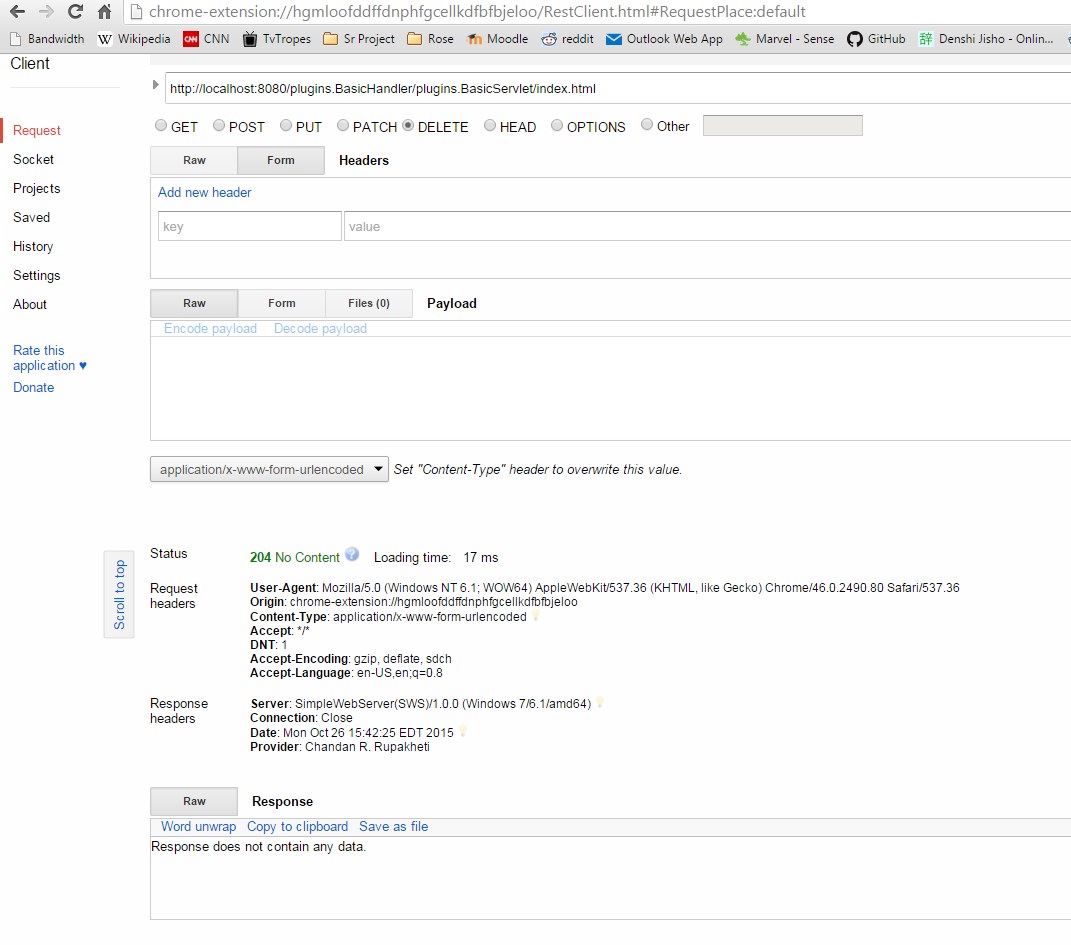
Demonstration of change in browser. Received via GET call.



PUT



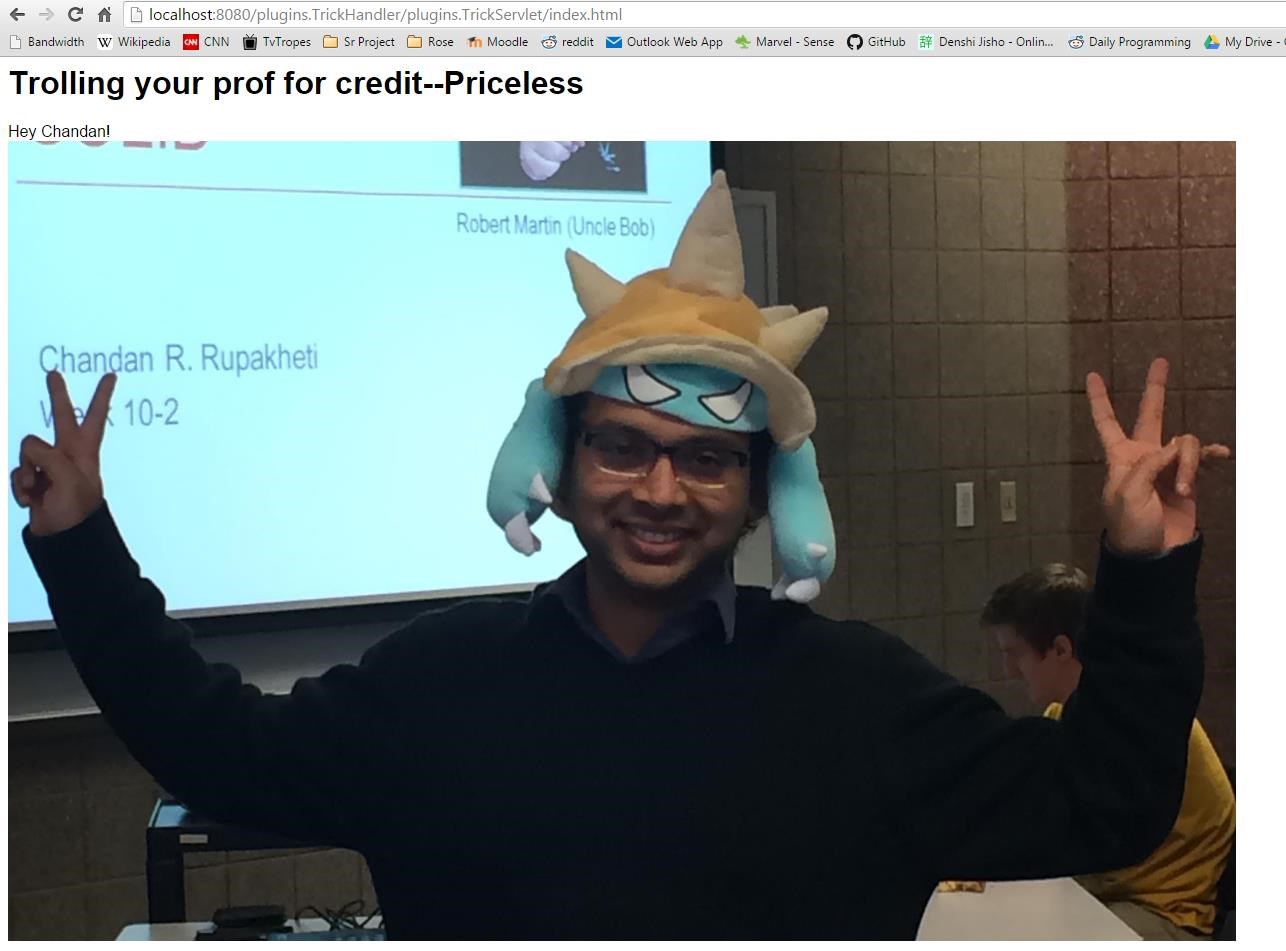
DELETE



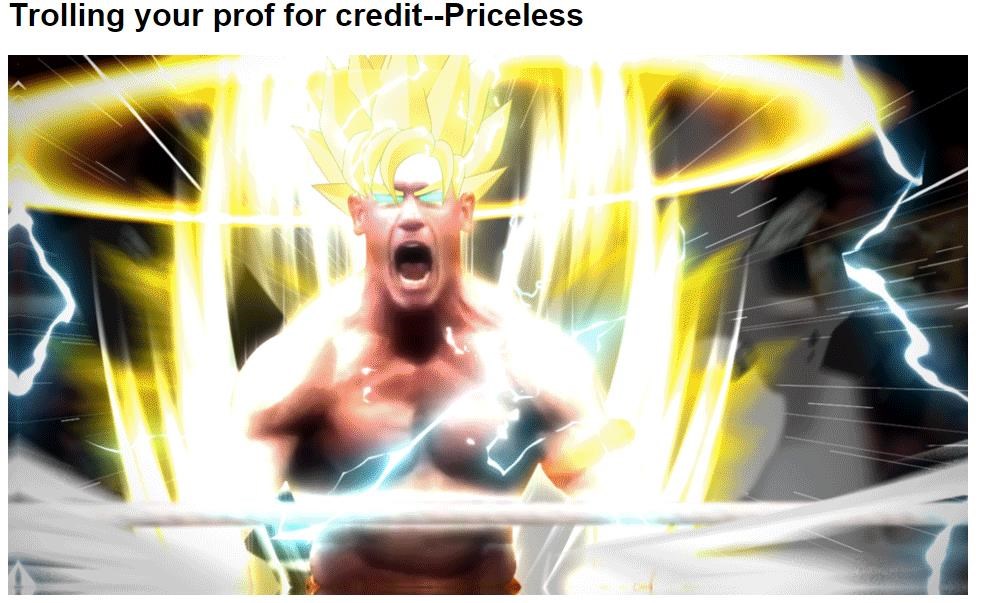
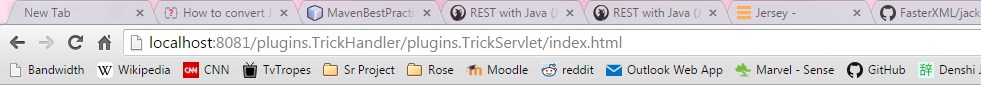
Trick Handler:

This handler redirects the user to one of 5 random webpages no matter what they ask for in a GET request.

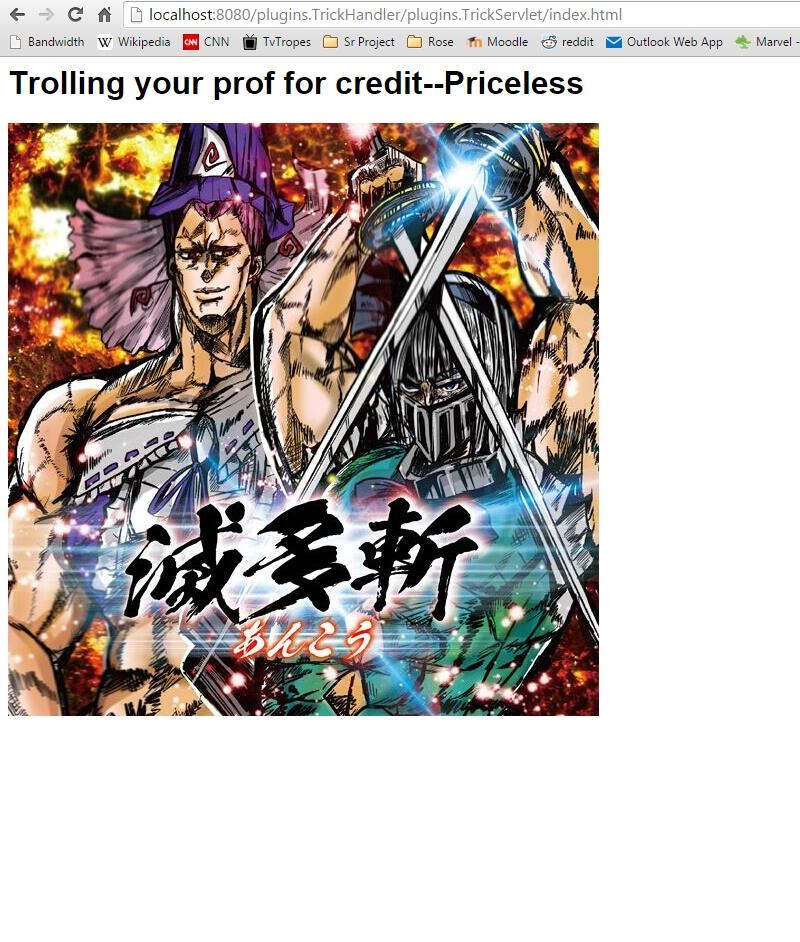
Page #1:



Page #2:

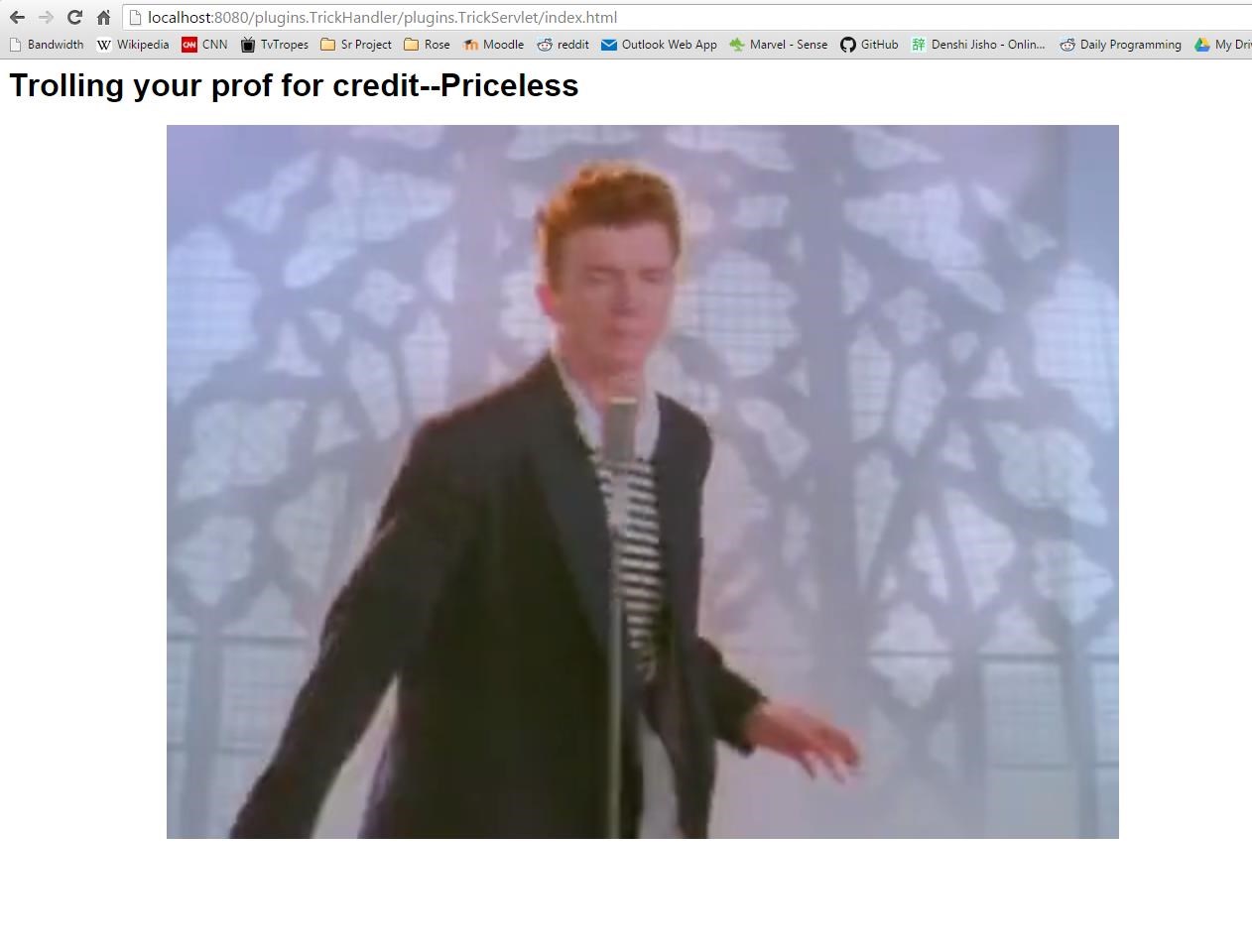
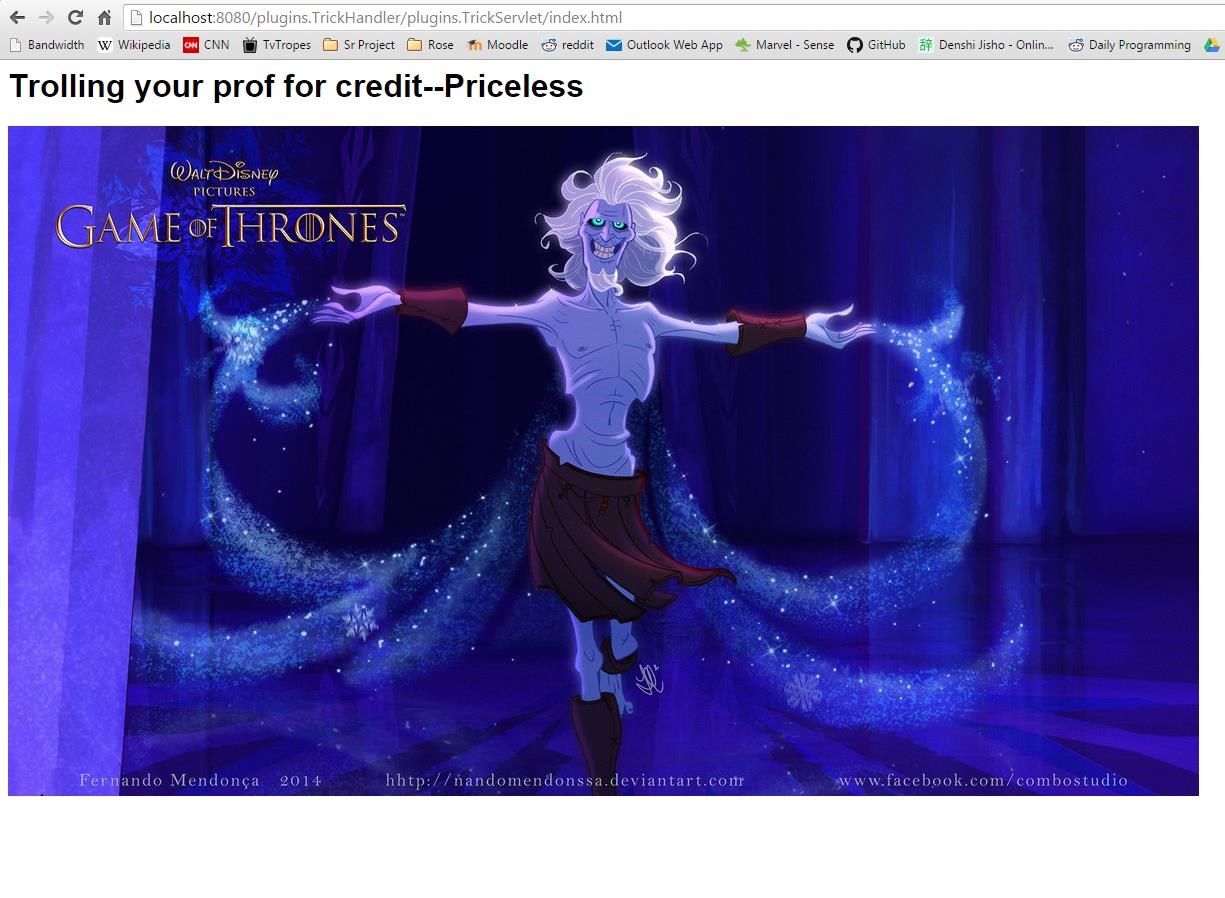


Page #3:

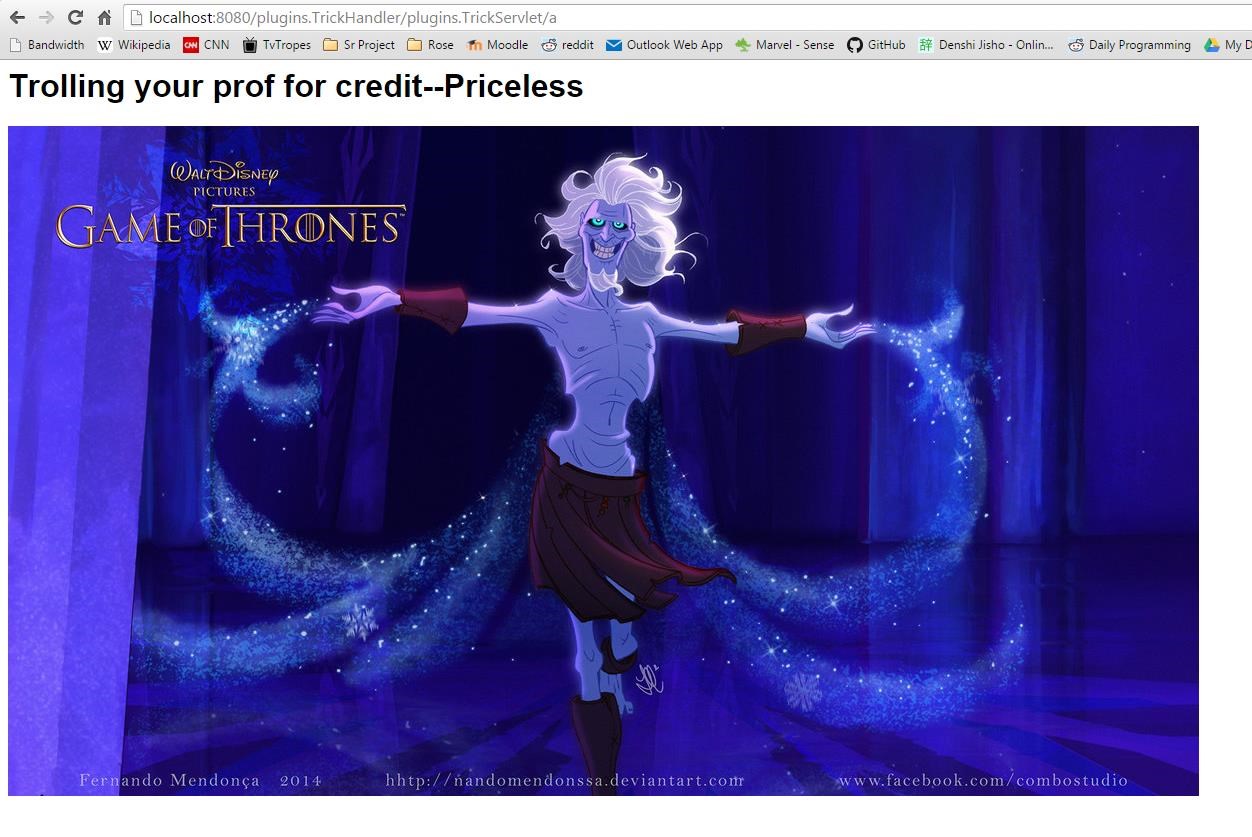


Page #4:

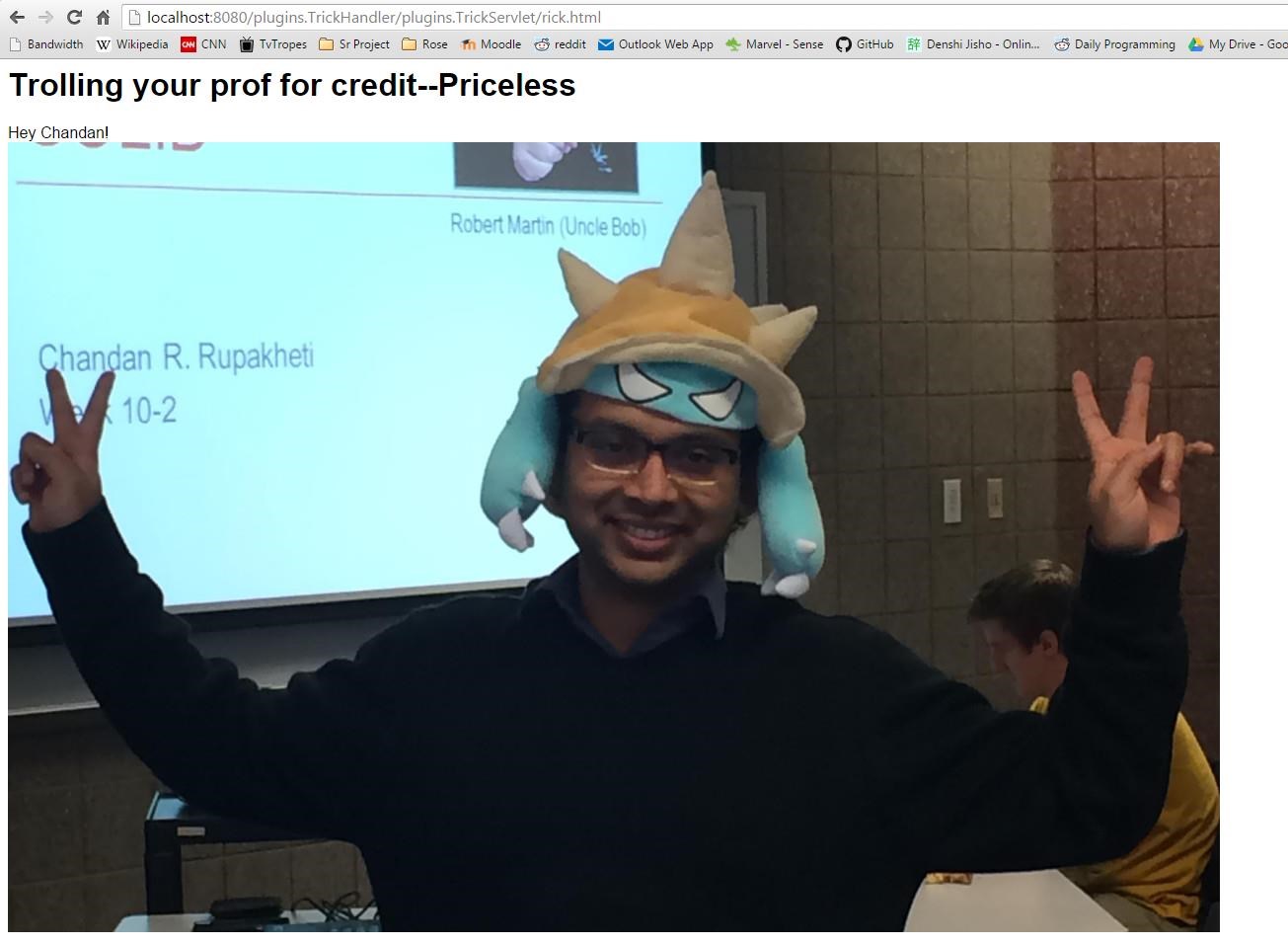
Page #5:



Notice that the URIs are the same for each one. But it doesn’t have to be “index.html”:



Funny thing even if you request the html that it redirects you to, you may not get that html:



4. Feature listing and assignment:

Assignment: Shared-Room Solo Programming for most of it (except for threadbomb prevention which was pair programmed.)

Features:

Malicious Plugin and fix for plugin injection –LE

Portion of logging—LE

Other part of logging—Greg

Throttling—Greg

Threadbomb prevention—Both

Change History:

All red and underlined text is changed.

# Architecture Evaluation and Improvements

## Availability:

Name: DOSing

A1.1 The concrete scenario description showing Source, Stimulus, Environment, Artifact,

Response, Reponse Measure

A1.2 We pointed our DOSing attempts at http://<ip-address>:8080/plugins.BasicHandler/plugins.BasicServlet/web/src/Untitled.gif. We used this because the .gif file was easy to test: it should take approximately 1.2 seconds to run through. Our base line number was 1.48 seconds (accounts for reaction time)

A1.3 When DOSing was performed the time to finish the gif jumped to 5.06s.

A1.4 We set it up to send no data if the client’s IP address has send 50 requests in the past 5 minutes. This was done by creating a ThrottleService class. We also logged the IP address of any throttled users.

A1.5 When throttling was applied, and DOSing was performed the gif load time was 1.54s, well within the margin of error. Additionally the DOSer’s IP address was logged so that we can know who is throttled in case of issues.

Name: Unexplained Shutdown

A2.1

A2.2 L.E. caused a shutdown in server and then Greg had to fix it without asking her how she broke it.

A2.3 It took 6m 35s for Greg to figure out the cause and restart the server from its broken state.

A2.4 We set the server up to log any error messages and any requests from users.

A2.5 When logging was implemented, Greg could see that L.E. had called the Malicious Plugin (see S1) and he was able to restart the server in 3m 9s.

## Security:

Name: MaliciousPlugin

S1.1

S1.2 We wrote a plugin that would force the computer into sleep, we then used a PUT request to deploy the plugin.

S1.3 Number of malicious plugins that can be added: infinite

S1.4 We set the server up to prohibit any requests of any kind that wanted access to the plugins folder and returned a 403 Forbidden response.

S1.5 After we prohibited access to the plugins folder, the number of malicious plugins that can be added:

S2: See A1

## Performance:

Name: ThreadBomb

P1.1

P1.2 L.E. ran multiple DOSing clients against Greg

P1.3 When L.E. ran multiple DOSing clients against Greg, his thread count reached 223 and slowed down the server immensely.

P1.4 We discovered that a threadbomb was actually not a problem. Therefore we didn’t implement anything. If it were a problem, we planned to implement a system whereby by closing inactive connections, we would reduce the thread count.

P1.5 See P1.4

P2: See A1