

## WebKit layoutTestController Emulator

This document will help you set up the WebKit layoutTestController Emulator on Mozilla Firefox 2 and Mozilla Firefox 3.

### Setup

1. If you already have the WebKit framework checked out, skip to step 4
2. Installing tools
  - a. Mac: Install Subversion client (<http://homepage.mac.com/hiirem/svkbuidls.html>)
  - b. Windows: Install Cygwin. Refer to step 3 of <http://webkit.org/building/tools.html>. You do not need to install Visual Studio.
3. Getting the layout tests
  - a. Use svn to check out the layout tests from <http://svn.webkit.org/repository/webkit/trunk/LayoutTests/http/tests/security>
4. Setting up the environment for testing
  - a. Start an HTTP server on ports 8000 and 8080 and an HTTPS server on port 8443 such that <http://127.0.0.1:8000/security> and <https://127.0.0.1:8443/security> point into the security folder you just checked out (See Appendix)
  - b. Create a new directory to store your new Firefox profile
  - c. Start Firefox with the -profile command line option (pointing it to the new profile you just created), go to Cross-Browser Security Testing homepage at <http://crypto.stanford.edu/websec/cross-testing>, and install browser extension

### Manual testing

1. Start Firefox with the -profile command line option
2. Navigate to <http://127.0.0.1:8000/security/<test>>, where <test> specifies the test you want to run. Note that you must use 127.0.0.1, not localhost
3. After each page loads, if dump is successful, <test>-actual.txt will be dumped in the layout-test-results directory under the OS temp directory (/tmp for Mac/Linux, or wherever %TEMP% is set for Windows)

### Automated testing

1. Download the script from Cross-Browser Security Testing homepage
2. Windows: Open Cygwin.
3. Run the script with the following 3 parameters:
  - a. Path to the Firefox executable
  - b. Directory where the tests reside
  - c. Directory where your Firefox profile (with the layoutTestController emulator active) resides
4. After script finishes executing, check the layout-test-results under the OS temp directory for the results of the tests.

## Appendix

### Starting the HTTP and HTTPS Servers

This appendix will help you set up Apache HTTP server for running the security regression tests. Note: This document was based on Apache HTTP Server 2.2.9. If you get a different version, your instructions may differ. Check the page for your version at <http://httpd.apache.org/docs/> for help.

1. If you already have Apache HTTP Server with SSL support, skip to step 5.
2. Go to <http://httpd.apache.org/download.cgi> and download the latest version of Apache HTTP server for your operating system.  
Windows users: If you download the binary, make sure you get the installer that includes OpenSSL.
3. If you downloaded the source, go to <http://httpd.apache.org/docs/>, open the version corresponding to the one you downloaded, and compile and configure the server using the instructions in the reference manual.
4. Install the server.
5. Open the `httpd.conf` file (typically in the `conf` directory), and make the following changes:
  - a. Find the `Listen` parameter. Typically, a default install will create either the line `Listen 80` or the line `Listen 8080`. Modify the line so that it contains

```
Listen 8000
Listen 8080
```
  - b. Find the line `LoadModule ssl_module modules/mod_ssl.so` and make sure that it is uncommented (no `#` prefixing the line)
  - c. Find the line `Include conf/extra/httpd-ssl.conf` and make sure that it is uncommented (no `#` prefixing the line)
  - d. Find the `DocumentRoot` and point it to the directory ONE ABOVE where you have the security tests checked out. For example, if you have the tests checked out at `/tmp/layout-tests/security`, you should point `DocumentRoot` to `/tmp/layout-tests`. Alternatively, you can copy the `security` directory to the current `DocumentRoot`, which defaults to `<Apache>/htdocs`, where `<Apache>` is the install path of Apache HTTP Server.
6. Create a self-signed SSL certificate.
  - a. Use the instructions at <http://www.openssl.org/docs/HOWTO/keys.txt> to generate an RSA key.
  - b. Use the instructions at <http://www.openssl.org/docs/HOWTO/certificates.txt> to generate a certificate for your RSA key.
7. Open the `httpd-ssl.conf` file (typically in the `conf/extra` directory), and make the following changes:
  - a. Find the `Listen` parameter. Typically, a default install will create the line `Listen 443`. Change it to read `Listen 8443`.
  - b. Find the `SSLCertificateFile` parameter and point it to the certificate you just created.
  - c. Find the `SSLCertificateKeyFile` parameter and point it to the RSA key you just created.
8. Start the Apache server.