WatchingHttpHeaders

When debugging problems with your HTTP server, access to the raw HTTP request and response headers (and sometimes the entire request and response) can be invaluable. Here we list various tools that can help you see, at minimum, the HTTP response headers sent by the server, and sometimes also request headers and body content.

- livehttpheaders for Mozilla Firefox
- firebug for Mozilla Firefox
- Microsoft Fiddler HTTP Debugger
- WireShark network protocol analyser
- Eavesdrop for Mac OS X

Shell

Various HTTP tools that may be available at the unix prompt:

```
wget -S --spider URL
lynx -head -dump URL
curl -I URL
HEAD URL
GET -de URL
w3m -dump_head URL
siege -g URL
```

Manually constructing requests

Using any standard telnet client, you can manually interact with an HTTP server and see the headers.

```
telnet server.example.com 80
HEAD /dir/page.html HTTP/1.1
Host: server.example.com
```

Press enter twice at the end.

Tracing headers over SSL

The `openssl` command can be used to open an SSL connection over which normal HTTP requests can be entered.

```
openssl s_client -connect secure.example.com:443
.. lots and lots of output ..
HEAD / HTTP/1.1
Host: secure.example.com
```

Press enter twice at the end.

Alternatively, ssldump and `wireshark` can use the private key file to decrypt live or recorded SSL traffic.