Senior Project - Apollo

A Tool for Testing the Security of Web Applications

Senior Project: 2001-2002

Jason Hitchings, Philip Piwonka, Andrew Roths, Erik Sipila and Brian Sipsey

IBM Corporation
Boulder, CO

The job of ethical hackers is to expose security holes in a network before a malicious hacker exploits them. In order to do their job, ethical hackers rely on a variety of tools. IBM's Security Assessment Department, specifically the Ethical Hacking Division, wanted a tool to assist them while testing the security of web servers. The purpose of the tool is to allow a user to manipulate the data that is transmitted between a browser and a web server. To carry this out, the tool functions as a proxy and intercepts all data prior to transmission.

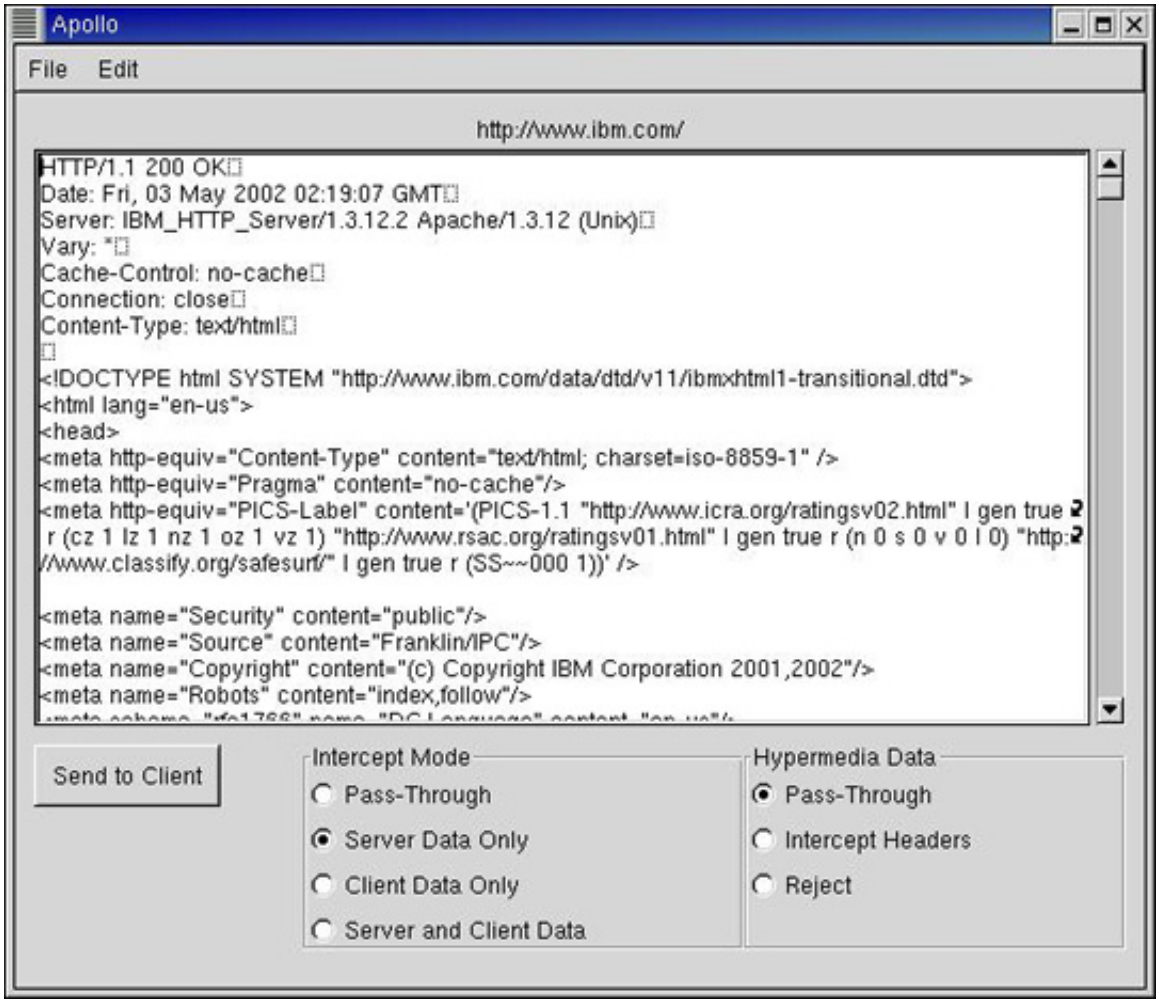
This project is a Linux-based tool that allows a user to intercept and modify hypertext in real-time. The tool has two primary functions:

1. When a browser requests a page while Apollo is enabled, Apollo will intercept the request, displaying the text of the request to the user. The user will then be allowed to either alter the request or simply pass it unaltered on to the web site.
2. Once the web site has received a request from Apollo, the remote server will send the requested data back, which Apollo will also intercept. Before the data is forwarded on to the user's web browser, Apollo will give the user the opportunity to manipulate the data.

To a browser, Apollo appears to be a server, as it receives requests from the browser. To a web server, Apollo is seen as the client, for it requests and receives data. This capability allows the user to compromise a web site's security by means such as:

- Changing a JavaScript Boolean value to give the appearance that a user has correctly entered a login and password
- Modifying hidden HTML tags
- Changing or disabling redirects
- Modifying CGI requests

The project was developed in C++ and GTK in a Red Hat Linux environment.



Graphical User Interface

```
Apollo

    MAIN MENU
  E - Edit Data
    P - Passthrough Data
    O - Options
    Q - Quit

    INTERCEPT MODE
    Passthrough
    Server
    Client
    Both

    HYPERMEDIA
    Passthrough
    Intercept Headers
    Reject

Current Intercept  Mode: Passthrough
Current Hypermedia Mode: Passthrough
--------------------------------------------------------------------------------
```

Terminal User Interface

Department of Computer Science
College of Engineering and Applied Science
University of Colorado Boulder
Boulder, CO 80309-0430 USA

Questions/Comments?
Send email to
Bruce.Sanders@Colorado.EDU

Engineering Center Office Tower
ECOT 717
+1-303-492-7514
FAX +1-303-492-2844