CS 155 April 19, 2005

Web Browser Security

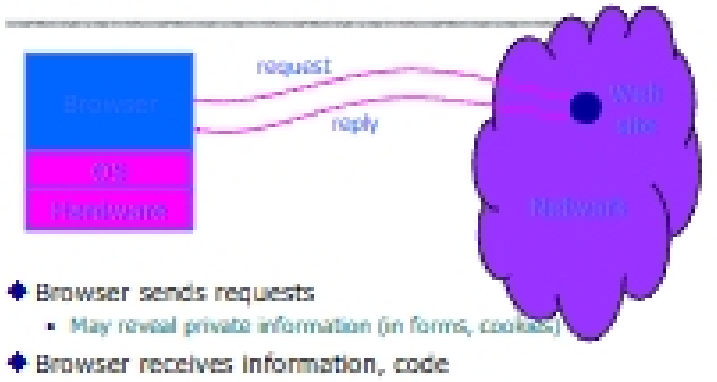
John Mitchell

Course Schedule

- Projects
  - Project 1: Assigned April 7, Due April 21
  - Project 2: Assign April 21, Due May 5
  - Project 3: Assign May 12, Due June 2 *No Late Days*
- Homework
  - HW 1: Assigned April 14, Due April 28
  - HW 2: Assign April 28, Due May 12
  - HW 3: Assign May 19, Due June 2 *No Late Days*

All assign/due dates are Thursdays (see calendar on web)
June 2 is "automatic one week extension from May 26"

Browser and Network



- Browser sends requests
  - May reveal private information (in forms, cookies)
- Browser receives information, code
  - May corrupt state by running unsafe code
- Interaction susceptible to network attacks
  - Consider network security later in the course

INTERNETWEEK.com Tuesday, February 12, 2002

Microsoft Issues New IE Browser Security Patch

By Richard Karpinski

- Microsoft has released a security patch that closes some major holes in its Internet Explorer browser
- The so-called "cumulative patch" fixes six different IE problems ...
- Affected browsers include Internet Explorer 5.01, 5.5 and 6.0.
- Microsoft rated the potential security breaches as "critical."

Feb 2002 patch addresses:

- A buffer overrun associated with an HTML directive ... Hackers could use this breach to run malicious code on a user's system.
- A scripting vulnerability that would let an attacker read files on a user's systems.
- A vulnerability related to the display of file names ... Hackers could ... misrepresent the name of a file ... and trick a user into downloading an unsafe file.
- A vulnerability that would allow a Web page to improperly invoke an application installed on a user's system to open a file on a Web site.
- ... more ...

MS announced 20 vulnerabilities on April 13, 2004 !!!

And then again this year, ...

Windows Security Updates Summary for April 2005

Published: April 12, 2005

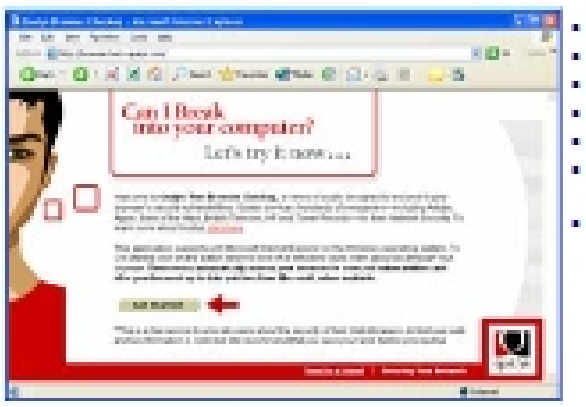
A security issue has been identified that could allow an attacker to compromise a computer running Internet Explorer and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Browser Security Check

http://www.verisign.com/advisor/check.html

What kind of security are they checking?

More informative test site



- Cookie Disclosure
- Clipboard Reading
- Program Execution
- File Execution
- Web Page Spoofing
- Security Zone Spoofing
- Hard Drive Access

http://browsercheck.qualys.com/

Browser security topics

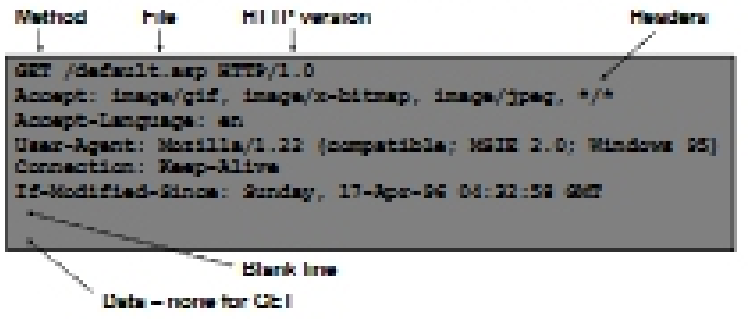
- HTTP review
- Controlling outgoing information
  - Cookies
    - Cookie mechanism, JunkBuster
  - Routing privacy
    - Anonymizer, Crowds
  - Privacy policy – P3P
- Risks from incoming executable code
  - JavaScript
  - ActiveX
  - Plug ins
  - Java

HTTP

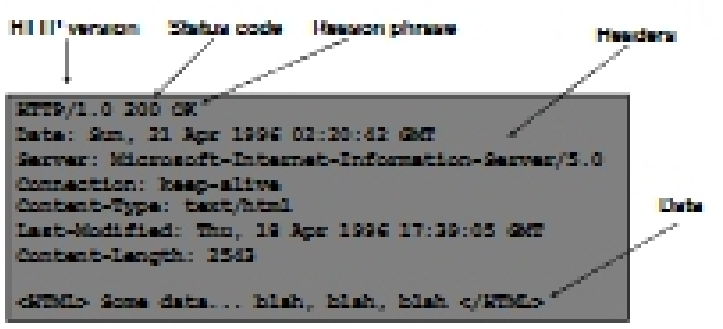
HyperText Transfer Protocol

- Used to request and return data
  - Methods: `GET`, `POST`, `HEAD`, …
- Stateless request/response protocol
  - Each request is independent of previous requests
  - Statelessness has a significant impact on design and implementation of applications
- Evolution
  - HTTP 1.0: simple
  - HTTP 1.1: more complex

HTTP Request



HTTP Response

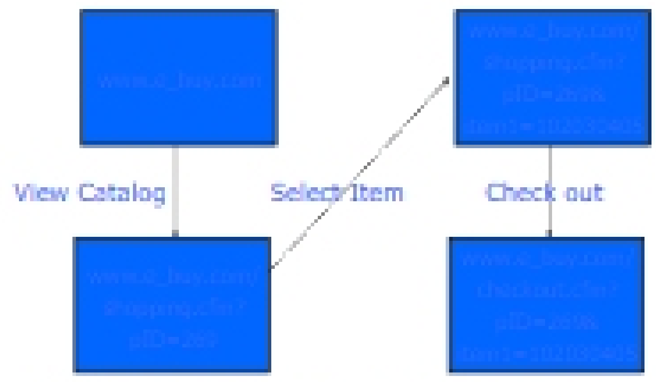


HTTP Server Status Codes

Code	Description
200	OK
201	Created
301	Moved Permanently
302	Moved Temporarily
400	Bad Request – not understood
401	Unauthorized
403	Forbidden – not authorized
404	Not Found
500	Internal Server Error

- Return code 401
  - Used to indicate HTTP authorization
  - HTTP authorization has serious problems!!!

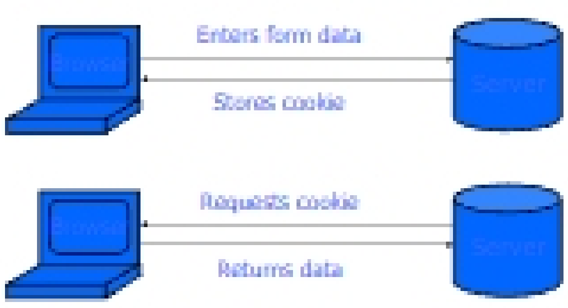
Primitive Browser Session



Store session information in URL; Easily read on network

Store info across sessions?

- Cookies
  - A cookie is a file created by an Internet site to store information on your computer



Http is stateless protocol; cookies add state

Browser Cookie Management

- Cookie Ownership
  - Once a cookie is saved on your computer, only the Web site that created the cookie can read it.
- Variations
  - Temporary cookies
    - Stored until you quit your browser
  - Persistent cookies
    - Remain until deleted or expire
  - Third-party cookies
    - Originates on or sent to another Web site

Third-Party Cookies

- Yahoo! Privacy Center
  - Yahoo! sends most of the advertisements you see
  - However, we also allow … third-party ad servers … to serve advertisements
  - Because your web browser must request these … from the ad network web site, these companies can send their own cookies to your cookie file …
  - **Opting Out of Third-Party Ad Servers**
    - "If you want to prevent a third party ad server from sending and reading cookies on your computer, currently you must visit each ad network's web site individually and opt out (if they offer this capability)."

Example: Mortgage Center

<html> <title>
Mortgage Center
</title> <body>
… http://www.loanweb.com/ad.asp?RLID=0b70at1ep0k9

What's this?