

# Lecture 6 – Cookies & Sessions

## Web Application Development

January 29, 2015

Jeffrey L. Eppinger  
Professor of the Practice  
School of Computer Science

# Lecture Schedule – 1<sup>st</sup> Half

(subject to change)

- |                       |                       |
|-----------------------|-----------------------|
| #1 Intro              | #9 Django Templates   |
| #2 HTML & CSS         | #10 Images            |
| #3 JavaScript & DOM   | #11 AJAX              |
| #4 CSS Frameworks     | #12 jQuery            |
| #5 HTTP & Django      | #13 Databases         |
| #6 Cookies & Sessions | #14 Cloud Deployment  |
| #7 Django Models      | #15 SSL               |
| #8 Transactions       | #16 Project Proposals |

# Agenda

→ Course Administration

Questions for You

Hidden Fields

Cookies

Sessions

Sample Final Exam Questions

# Super Bowl Office Hours

Sunday office hours have been moved to the following times:

- Shannon: 1pm to 3pm
- Divya: 3pm to 5pm
- (Same location: WEH 5120)

# Updated Late Policy

- ✓ HW due on Mondays at 11:59pm
- ✓ No penalty if turned in by Wednesday at 11:59pm
  - But late days are tracked and will delay your signup for project demo
- Penalty if turned in by Thursday at 11:59pm
  - And late days are tracked and will delay your demo signup
  - No need to notify us in advance
- If you want to turn it in after Thursday, you must see the professor after any lecture
  - Late days & penalties apply
  - Please don't request additional time via e-mail
  - Additional time will not be granted if your HW has already been graded

# Agenda

- ✓ Course Administration
  - Questions for You
    - Hidden Fields
    - Cookies
    - Sessions
    - Sample Final Exam Questions

# Question for You

- Can You Anonymously Use CMU's Network?
- Do You?

# Question for You

- Should I have given you a “to do list” example in Django?



# Here It Is!

- Shared “to do list” example:  
<http://real.wv.cs.cmu.edu:8000/shared>

# Question for You

- What is XSS?

# Cross-Site Scripting

- Attacker injects scripts into a site's data that other users will see
- Example:
  - Put HTML or JavaScript into a shared to do list!

# Question for You

- What is CSRF?

# Cross-Site Request Forgery

- A web page that tricks user into submitting a request elsewhere
  - Request runs with user's identity
- Website A generates a page that contains a link website B
  - User happens to already be logged into website B
  - Link requests website B make some changes to user's account
- Example of Website A attack on GitHub (doesn't work)
  - Page 1: In webapp class? Tell us your GitHub ID and win a free prize!
  - Page 2: Click [here](#) for your prize
  - What's [here](#)?

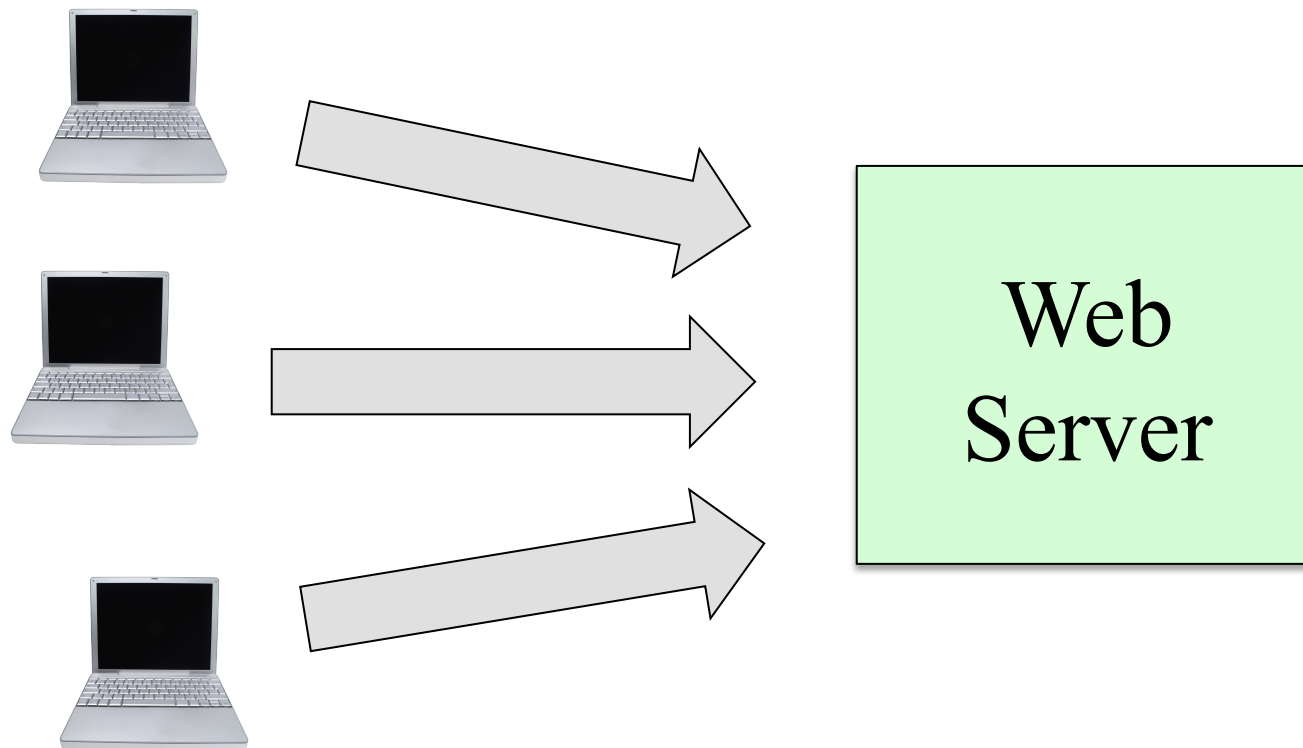
```
<a href="https://github.com/CMU-Web-App-Development/[id].git?action=delete">
  here
</a>
```

# Agenda

- ✓ Course Administration
- ✓ Questions for You
  - Hidden Fields
  - Cookies
  - Sessions
  - Sample Final Exam Questions

# Server's Problem

- How to tell which browser a request comes from?



# Hidden Fields In HTML

- Maintain data correlated with a page
  - They are embedded in the page
  - Especially helpful with context changes with back button
- It's a type of field that you can put in an HTML form

```
<input type="hidden" name="fname" value="Joe"/>
```
- This field not displayed, but its value is returned as a parameter on the subsequent request
- Is this secure?



# Example

- Hidden Field Example
  - <http://real.wv.cs.cmu.edu:8000/hidden>

# Agenda

- ✓ Course Administration

- ✓ Questions for You

- ✓ Hidden Fields

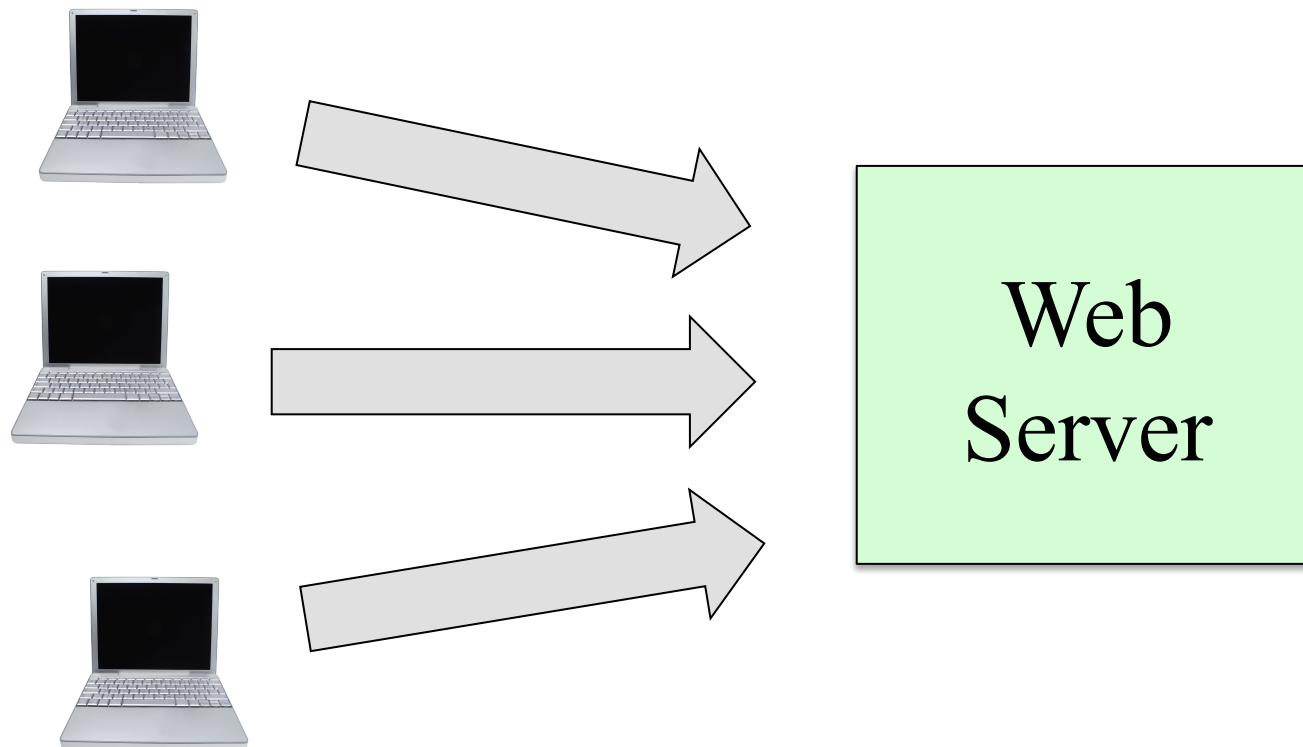
- Cookies

- Sessions

- Sample Final Exam Questions

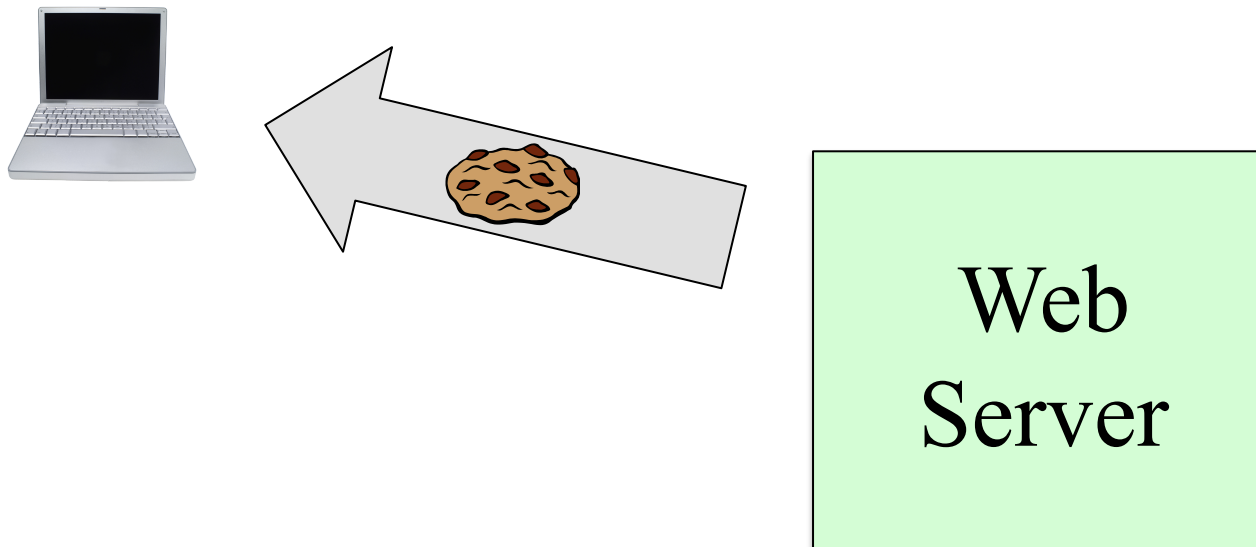
# Server's Problem

- How to tell which browser a request comes from?



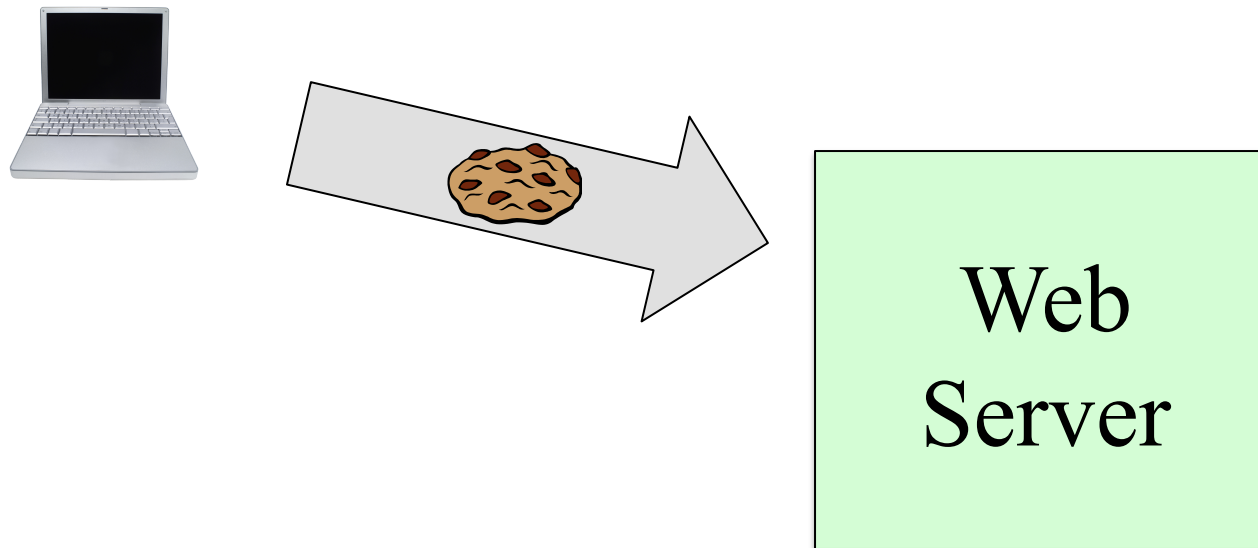
# Server Sends a Cookie

- Server sends cookies to browser in HTTP Response
- Cookies are server generated data
  - Typically identify user (or browser), preferences, etc



# Browser Sends Back Cookies

- Browser does not “understand” the cookie data
- Browser sends cookies back in subsequent requests
  - Server will now know “who” is making the request

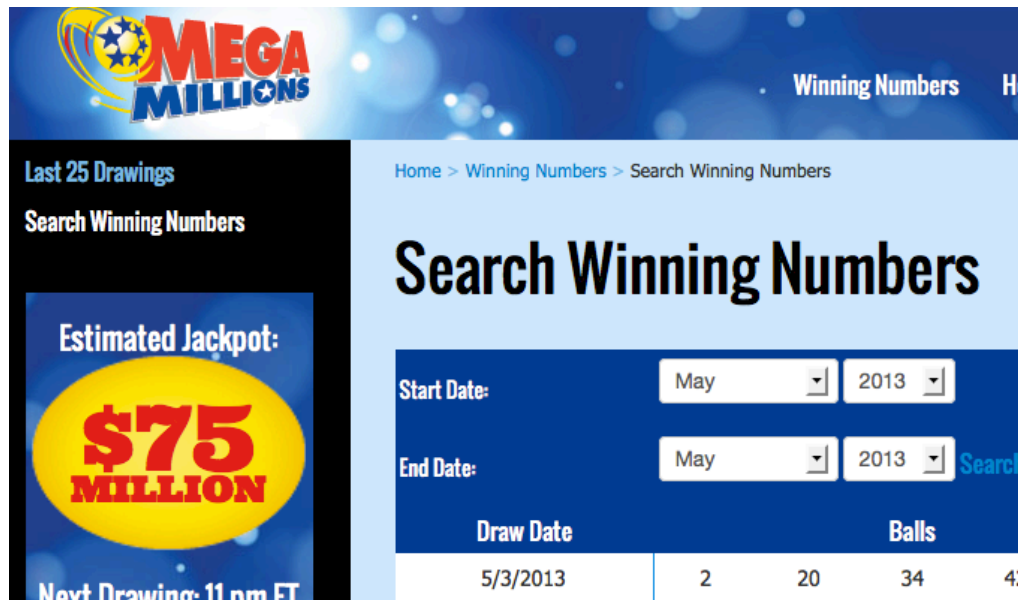


# Cookies in General



- Term dates back to the 1970s
  - Magic cookie, magic number, ticket, token
- Short packet of data
- Not interpreted by the recipient
- Recipient can use the data when talking to sender
  - an identifier
  - a ticket
  - a capability
- Typically, they are hard to forge

# Lottery Ticket



**MEGA MILLIONS**

Winning Numbers

Home > Winning Numbers > Search Winning Numbers

## Search Winning Numbers

Start Date: May 2013

End Date: May 2013 [Search](#)

Draw Date	Balls	Mega Ball	Megaplier	Details
5/3/2013	2 20 34 42 54	39	2	<a href="#">Details</a>

Estimated Jackpot: **\$75 MILLION**

Next Drawing: 11 pm ET



www.palottery.com

Thu Cash 5 Jackpot \$325,000. Sat Powerball Jkpt \$191 Mil. Annuity. Fri Mega Millions \$126 Mil. Annuity. Thu Match 6 Jackpot \$750,000.

Surprise! A Double Draw was held Wed. for Quinto Night. A total of 84 winners received \$37,350 for the 2 draws. Numbers at palottery.com

Term: 994464 bdfcb8b5  
5231-00000700067840-46 May 02, 2013 09:43

\$1.00 - 1 Draw  
Fri 03-May-2013  
Megaplier No

**MEGA MILLIONS**

A. 01 06 21 49 52 Megaball: 35 QP

www.palottery.com

Benefits Older Pennsylvanians. Every Day.

# HTTP Cookie *Headers*



- Sending a cookie in an HTTP Response

**Set-Cookie: name=value**

**Set-Cookie: name=value; <attributes>**

- Sending back a cookie in an HTTP Request

**Cookie: name=value; name=value**



# HTTP Cookie *Attributes*




Attributes are optional

- Expires – Sets max lifetime of cookie (date & time)
- Max-Age – Sets max lifetime of cookie (seconds)
- Domain – To which hosts to send cookie back
- Path – For which URLs to send cookie back
- Secure – Only send cookie on secure connections
- HttpOnly – Don't expose cookie to scripts

# HTTP Cookie Terminology

- Session Cookie – Deleted on browser close
- Persistent Cookie – Stored until expiration date
- Third-party Cookie – Cookies from other sites
  - Often used for tracking
  - You can configure your browser to reject these

# Cookies don't always taste good

- Cookies can only contain a little data
  - Up to 4kb 
- Cookies can be modified by the user
  - Sometimes we don't care
    - E.g., cookie data can specify user preferences
  - Usually we care
    - E.g., cookie data specify which user is logged in
    - Cookie data are long random strings or hashes
    - Very difficult for user guess or compute
- Cookies might not be accepted by the browser
  - You can configure your browser not to accept cookies

# Simple Example of Cookie Data

- Securely keep track of which user is logged in
- Cookie data is a long number with three parts
  1. Large random number
  2. System time (in seconds or milliseconds)
  3. Sequence number since server startup
- Use this number as a database access key
  - Database is stored on server (memory or disk)



# Lets Look at Some Cookies

- Firefox: Tools => Web Developer => Network
- Chrome: View => Tools => Developer Tools



# Agenda

- ✓ Course Administration
- ✓ Questions for You
- ✓ Hidden Fields
- ✓ Cookies
- Sessions
- Sample Final Exam Questions

# Sessions

- Maintain data correlated with browser session
- Cookies are typically used to implement sessions
  - A session id is stored in the cookie
    - It's big and ugly
  - Maintains a list of (name,object) pairs in the server
  - In Django, it's `request.session`
  - Access it like a Python dictionary

# Example

- Private To Do List
  - <http://real.wv.cs.cmu.edu:8000/private>



# Question for You

- Is private to do list vulnerable to CSRF?
- If so, how would you prevent that?

# Question for You

- What if the browser doesn't accept cookies?

# URL Rewriting

- If the browser doesn't accept cookies, the session id is embedded (appended to?) each URL in the HTML response
- When the rewritten URL is accessed, the server extracts the embedded session id
- Negatives of this technique:
  - Each URL in the HTML response must embed session id with

# Agenda

- ✓ Course Administration
- ✓ Questions for You
- ✓ Hidden Fields
- ✓ Cookies
- ✓ Sessions
- Sample Final Exam Questions

# Sample Final Exam Question

- When to use hidden-fields, cookies, or sessions?
  - Login
  - Redirect
  - Shopping cart
  - Editing Records
- We'll come back to each of these in future lectures

# Hidden Fields

- Maintain data correlated with a page
  - They are embedded in the page
  - Especially helpful with context changes with back button
- Not good for login or shopping cart
- Possibly for redirect
- Perfect for editing or deleting records

# Sessions

- Maintain data correlated with browser session
  - Usually implemented using cookies that have a short life-time – like not stored on the disk
- Transcends pages
- Good for login
  - Especially for “typical” security requirement
    - Close your browser or sit idle and you log in again
- Good for shopping cart
- Bad for editing/deleting records

# Cookies

- Maintain data correlated with the client machine
  - Usually cookies have long lifetimes that span browser sessions
- Transcend browser sessions (and pages)
- Good for login
  - If you want “remember me” function on machine
  - Especially for storing hashed credentials
- Bad for editing/deleting records



# Agenda

- ✓ Course Administration
- ✓ Questions for You
- ✓ Hidden Fields
- ✓ Cookies
- ✓ Sessions
- Sample Final Exam Questions