Dept of Computer Science
Ahmadu Bello University

WEB APPLICATION ENGINEERING II

Lecture #5

Umar Ibrahim Enesi

Dept of Computer Science
Ahmadu Bello University

Objectives

- Gain understanding of how Cookies and Sessions Work
- Understand the limitations of Sessions and Cookies
- Understand how to handle Session and Cookies in PHP

Dept of Computer Science
Ahmadu Bello University

HTTP State Management Mechanism

- HTTP is a stateless protocol.
- A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests – each requests are mutually exclusive.
- Right from the early days of web there is no mechanism for relating one interaction with another.
- Cookies and Session provide a means to achieve that.

Dept of Computer Science
Ahmadu Bello University

Cookies

- The idea of cookies was introduced by the creator of Netscape Navigator to remedy this apparent limitation.
- With cookies, the effort of managing state is left to the developer.
- Note that even with the present of cookies in requests/reponses, as far as HTTP is concerned, they are all still separate and unrelated.

Dept of Computer Science
Ahmadu Bello University

What are Cookies?

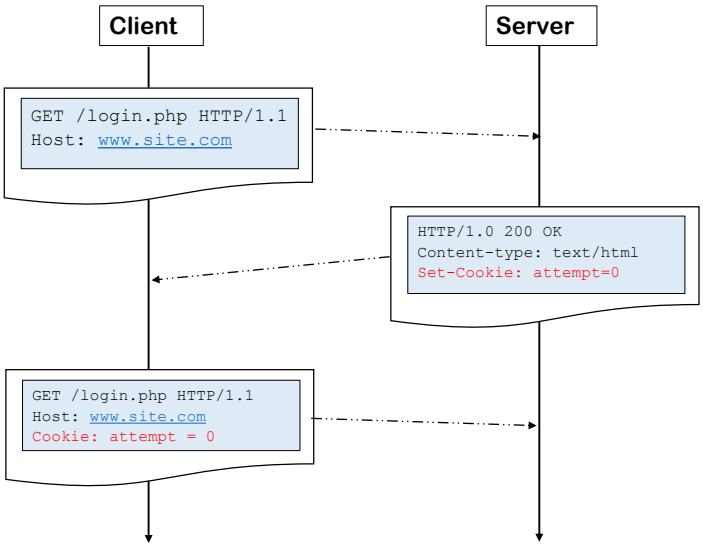
- Cookies are bits of text information stored on the client machine and sent with the HTTP request to or response from the Web site for which they were created.
- A web page (using javascript) or server instructs a browser to store information as cookie.
- When the user-agent makes subsequent requests to the server, cookies information are included.
- Note that access to cookies is controlled by same origin policy - cookies can only be accessed from the domain in which it is associated with.

Dept of Computer Science
Ahmadu Bello University

Cookies Header Fields

- HTTP provides header fields for attaching cookies in header section of request and response messages.
- Using the `Set-Cookie` header field, an HTTP server can pass name/value pairs and associated metadata (attributes) to a browser.
- A browser can also pass cookies to the server by using `Cookie` header field of HTTP request.

Dept of Computer Science
Ahmadu Bello University



Dept of Computer Science
Ahmadu Bello University

Cookie Attributes (metadata)

- Cookies may be set with the following attributes:
  - name=value (*This is the only required attribute*)
  - Expiration date in seconds.(`Max-Age`)
  - The path for which this cookie is valid (`Path`)
  - The domain this cookie is valid for (`Domain`)
  - Need for secure connection (`Secure`)
  - Versioning (`Version`)
  - Commenting (`Comment`)

Dept of Computer Science
Ahmadu Bello University

Types of Cookies

- Session cookie – an in-memory cookie (expiry date is usually set to 0)
- Persistent cookie – cookie with explicit expiry date greater than 0
- HttpOnly cookie – only accessible via HTTP(S). Not accessible by JS
- Third-Party (tracking) cookie – Cookie from external site other than that of displayed web page.

Note that cookies may exhibit more than one of the above type.

- E.g. a cookie may be persistent and tracking cookie at the same time

Dept of Computer Science
Ahmadu Bello University

Manipulating Cookies with PHP

- PHP supports HTTP Cookies.
- To set cookie use `setcookie()` function.
- `setcookie()` must be called BEFORE any output is sent to the browser.
- See PHP documentation manual for full description of usage.
- To access cookies sent from browsers use `$_COOKIE` super global array.
- To delete/expire a cookie, use `setcookie()` and pass in date of the past as the `expire` argument.

Dept of Computer Science
Ahmadu Bello University

Limitations of Cookie

- Browsers might :
  - allow limited size in byte per cookie.
  - restrict the number of cookies per domain.
  - restrict the total number of cookies.
  - be configured to disable cookie support.
- Cookie settings in browsers can be tinkered by the user, therefore not to be trusted.

All of the above make the idea of cookie an unreliable way of managing state of web application. So usage should be with caution.

Dept of Computer Science
Ahmadu Bello University

Typical use of Cookies

- To customize pages. E.g. theme, default page, search results etc.
- To monitor target users' interest for use in advertisement.
- To enable sticky form and "*Remember me*" feature of login forms

Dept of Computer Science
Ahmadu Bello University

SESSION

- Session is another mechanism for managing state of interaction.
- Usually managed at the server end.
- More reliable, less applications than cookies.
- Initiated and manipulated by the server but terminated by the client or the server.

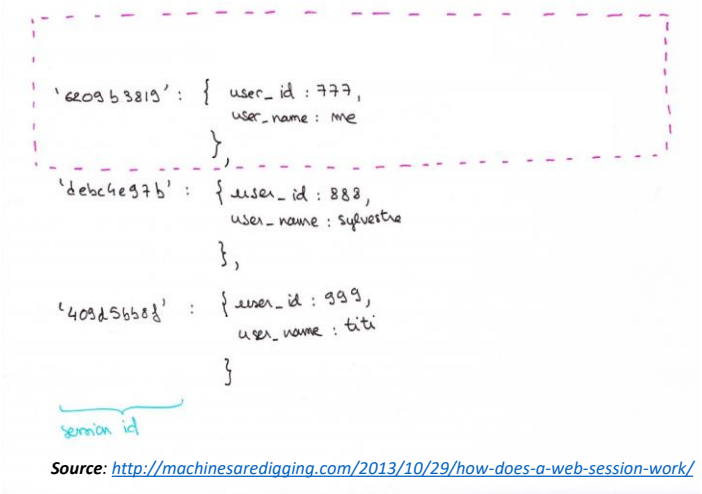
Dept of Computer Science
Ahmadu Bello University

How Sessions Work

- Typically, server handles requests from multiple clients.
- Hence the need to distinguish one client from the other.
- For each client, the server generates a unique id (SESSION ID).
- Each client stores its own session id as cookie (specifically session cookie) or propagated in URL.
- The server on the other hand, maintains a key-value pair data structure where the keys are the available session ids while the value is array of name-value pairs of information specific to the session id.

Dept of Computer Science
Ahmadu Bello University

How Sessions Work



Source: *http://machinesaredigging.com/2013/10/29/how-does-a-web-session-work/*

Dept of Computer Science
Ahmadu Bello University

PHP Session Workflow

- When a session is started by a script, PHP will either retrieve an existing session using the ID passed (usually from a session cookie) or if no session is passed it will create a new session (and set a session cookie)
- If a session has already been started, PHP will extract all data (if any) related to the session id into a super global array called `$_SESSION`.
- During the execution of the script, `$_SESSION` may be manipulated (or even destroyed).
- When the script finish executing the new/modified content in `$_SESSION` (if any) will be sent for storage.

Dept of Computer Science
Ahmadu Bello University

Handling Session in PHP

- Sessions can be started manually using the `session_start()` function. Must be called before outputting to browser.
- Session data can be set or retrieved using `$_SESSION` superglobal associative array.
- Individual session values can be destroyed by unsetting the corresponding element in the `$_SESSION` array.
- To destroy session data, use `session_destroy()`.
- The above does not destroy the Session Id. Use `setcookie()` to achieve that.

Dept of Computer Science
Ahmadu Bello University

Key Point

- HTTP from initial design is stateless.
- Cookies and Sessions are used to remedy this limitations.
- Cookies can be created, manipulated and destroyed both in the client and server.
- Sessions can be created and manipulated by the server but can be destroyed by both the client and the server.
- Sessions tend to be more secured than Cookies.
- Sessions may rely on Cookie functionality or URL propagation.

Reference

- PHP Documentation Manual
- Murach PHP and MySQL
- https://tools.ietf.org/html/rfc6265#section-6.1
- https://www.nczonline.net/blog/2009/05/05/http-cookies-explained/
- https://en.wikipedia.org/wiki/Session_(computer_science)
- http://machinesaredigging.com/2013/10/29/how-does-a-web-session-work/