University of Dayton
Department of Computer Science

CPS 475/575
Secure Application Development

Lecture 15 – Cookies and Sessions in Web Application Development with PHP

Phu Phung
3/3/2020

Agenda

- Cookies and Sessions
- Session in PHP
- Lab 5: Secure Web Application Development in PHP with Cookies and Sessions

HTTP Review

uses TCP:

- client initiates TCP connection (creates socket) to server, port 80
- server accepts TCP connection from client
- HTTP messages (application-layer protocol messages) exchanged between browser (HTTP client) and Web server (HTTP server)
- TCP connection closed

HTTP is "stateless"

- server maintains no information about past client requests

We need protocols that can maintain "state" between client-server

Revisit: Cookies and JavaScript

- Cookies are data stored in browsers to allow the web servers “remember” the user
  - Cookies can be set by
    - Web servers (through HTTP Response)
    - JavaScript code
  - Cookies can be accessed by
    - Web Browsers
      - Store cookies in local files
      - Send to web servers through HTTP Request
    - JavaScript code
      - Cookies are protected by Same-Origin Policy
        - » Only JavaScript code in the same origin can access the cookies

Server-side Generated cookies

many Web sites use cookies

four components:

1) cookie header line of HTTP *response* message
2) cookie header line in next HTTP *request* message
3) cookie file kept on user's host, managed by user's browser
4) back-end database at Web site

example:

- Susan always access Internet from PC
- visits specific e-commerce site for first time
- when initial HTTP requests arrives at site, site creates:
  - unique ID
  - entry in backend database for ID