Cookies

Cookies

- HTTP is stateless
- To "remember" a user we use cookies
  - In a response header, we can give the user information as a cookie
    - All subsequent requests will contain these cookies in a header
- Since cookies work through headers: ASCII only

Cookie Headers

- Set-Cookie
  - Use this header in your response to tell a client to set a cookie
- Cookie
  - The client will send all Cookies with each request using this header

Set-Cookie

- The Set-Cookie header is used by servers to tell the client to set a cookie
- Cookies are sent as key-value pairs

- Syntax:
  - <key>=<value>

- Example:
  - Set-Cookie: id=X6kAwpgW29M
  - Set-Cookie: visits=4

Cookie

- Header used by clients to deliver all cookies that have been set

- Syntax [Same as Set-Cookie]:
  - <key>=<value>
  - Multiple cookies separated by ;

- Example:
  - Cookie: id=X6kAwpgW29M; visits=4

Client-Side Cookies

- The client can also set and change their cookies
  - Do not trust the value stored in a cookie
- If a cookie is important for security
  - Verify its validity

- Client can read/set cookies with JavaScript
  - So can attackers!

- Access cookies with "document.cookie"

Cookie Hijacking

- Cookies are often used for authentication
  - Set a cookie at logon to remember that the user is authenticated
  - Prevents sending username/password with every request

- What if someone steals your cookies?
  - They can authenticate as you without needing your password
  - They would have to get their JavaScript running in your browser

Directives

- Can add directives when setting a cookie
  - Separate directives with ;
- Expires
  - The exact time when the cookie should be deleted
    - Must be in the format:
      - <day-name>, <day> <month> <year> <hour>:<minute>:<second> GMT
      - Set-Cookie: id=X6kAwpgW29M; Expires: Wed, 12 Feb 2020 13:42:32 GMT
- Max-Age
  - Set the number of second before the cookie expires
  - Set-Cookie: id=X6kAwpgW29M; Max-Age: 3600
- If neither Expires nor Max-Age are set, the cookie will be deleted when the user ends the session

Directives

- Secure
  - Only send this cookie over HTTPS
- HttpOnly
  - Don't let anyone read or set this cookie using JavaScript
  - Prevents hijackers from reading your cookies

- Set-Cookie: id=X6kAwpgW29M; Secure; HttpOnly

Directives

- Path
  - Specify a prefix that the path must match for the cookie to be sent
  - Set-Cookie: id=X6kAwpgW29M; Path: /posts
    - Cookie is only sent when the requested path begins with /posts