

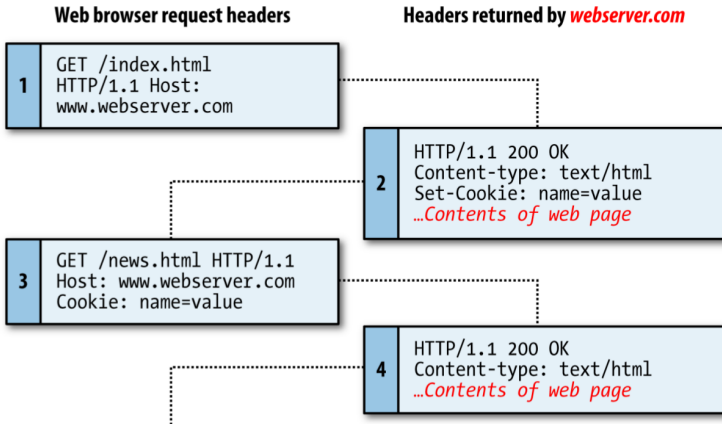
Cookies, Sessions, and Authentication

CSC 242, Web Programming

HTTP Cookies

- HTTP is a stateless protocol
- HTTP cookies are a way to store stateful information between separate HTTP requests
- An HTTP cookie is an item of data that the server sends to the client and the client stores that data to send in future requests
- The data in a cookie can only be read from the issuing domain

HTTP Cookie Headers



Setting a Cookie with PHP

- The setcookie function:

```
setcookie(name, value, expire, path, domain,  
          secure, httponly)
```

- `name`: The name of the cookie
 - `value`: The value of the cookie; can contain up to 4KB of data
 - `expire`: (Optional) The Unix timestamp for the expiration date
 - `path`: (Optional) The path to the cookie on the server
 - `domain`: (Optional) The domain of the cookie
 - `secure`: (Optional) Whether the cookie must be sent over a secure connection
 - `httponly`: (Optional) Whether the cookie must use the HTTP protocol
- Note: a cookie must be set before any HTML has been output

Accessing a Cookie with PHP

- The cookie is placed in the `$_COOKIE` array
- Example: accessing a cookie with the name `username`

```
$username = $_COOKIE['username']
```

Destroying a Cookie with PHP

- To destroy a cookie, the `setcookie` function must be called with an expiration date set in the past
- All of the other parameter values that were used when initially setting the cookie must be the same

PHP Sessions

- A PHP session is a mechanism to store stateful information on the server
- PHP sessions enable variable storage so that the variables can be used from multiple PHP scripts

Starting a PHP Session

- A session must be started before any HTML has been output
- The `session_start` function starts a session
- To save and access session variables, assign them to the `$_SESSION` array

```
<?php
// start the session
session_start();

// store a session variable
$_SESSION['username'] = "Alice";
?>
```


Ending a PHP Session

- The `session_unset` function deletes the session variables
- The `session_destroy` function destroys the session

```
<?php
// start the session to access the
// session data
session_start();

// remove the session variables
session_unset();

// destroy the session
session_destroy();
?>
```

HTTP Basic Access Authentication

- HTTP Basic authentication is a method for enforcing access controls for web resources
- When an unauthenticated client tries to access the resource, the server sets the 401 status code and the HTTP header:
`WWW-Authenticate: Basic realm="Restricted"`
- The client can authenticate by setting the HTTP header:
`Authorization: Basic [encoded credentials]`

HTTP Authentication in PHP

- The username and password from a client's Authorization header are placed in the `$_SERVER` array
- The username: `$_SERVER['PHP_AUTH_USER']`
- The password: `$_SERVER['PHP_AUTH_PW']`