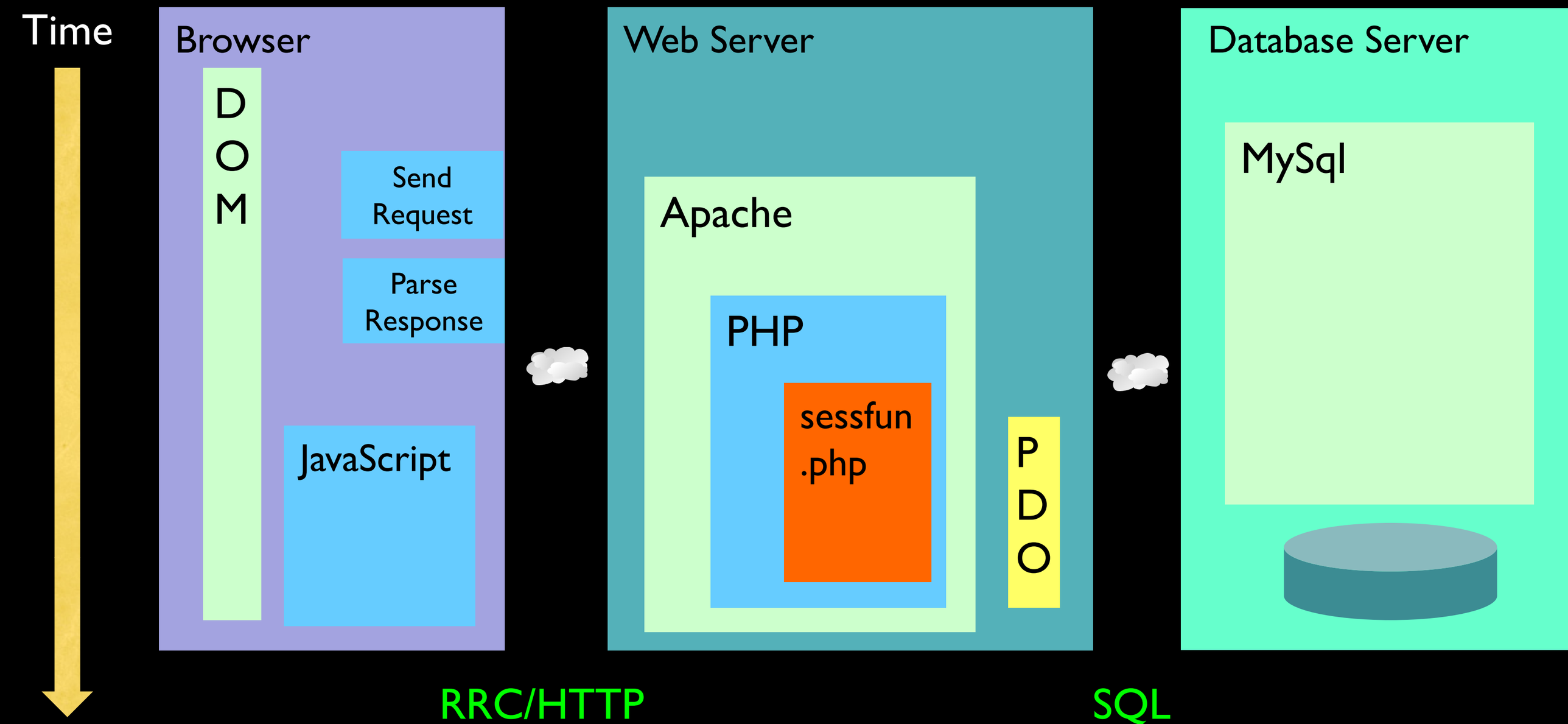
Redirect, Routing, and Authentication

Dr. Charles Severance
www.wa4e.com

http://www.wa4e.com/code/route.zip

CC BY


Time
Browser
DOM
Send Request
Parse Response
JavaScript
Web Server
Apache
PHP
sessfun .php
PDO
Database Server
MySql
RRC/HTTP
SQL

HTTP Status Codes

- http://www.dr-chuck.com/page1.htm - 200 OK
- http://www.wa4e.com/nowhere.htm - 404 Not Found
- http://www.drchuck.com/ - 302 Found / Moved

Also known as “redirect”

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

HTTP Location Header

- If your application has not yet sent any data, it can send a special header as part of the HTTP Response.
- The redirect header includes a URL that the browser is supposed to forward itself to.
- It was originally used for web sites that moved from one URL to another.

http://en.wikipedia.org/wiki/URL_redirection

header

(PHP 4, PHP 5)

header — Send a raw HTTP header

Description

Report a bug

```
void header ( string $string [, bool $replace = true [, int $http_response_code ]] )
```

header() is used to send a raw HTTP header. See the » HTTP/1.1 specification for more information on HTTP headers.

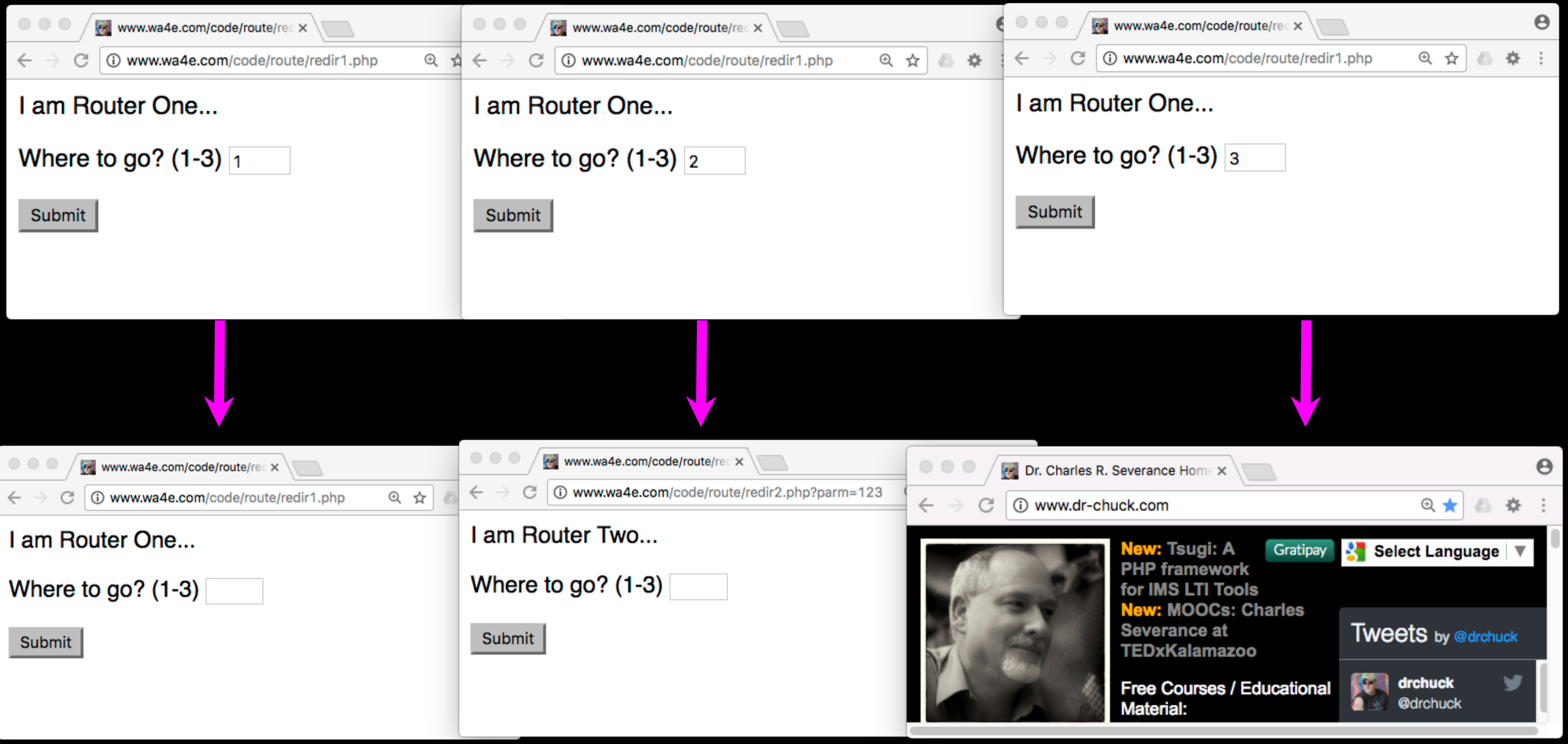
Remember that **header()** must be called before any actual output is sent, either by normal HTML tags, blank lines in a file, or from PHP. It is a very common error to read code with include, or require, functions, or another file access function, and have spaces or empty lines that are output before **header()** is called. The same problem exists when using a single PHP/HTML file.

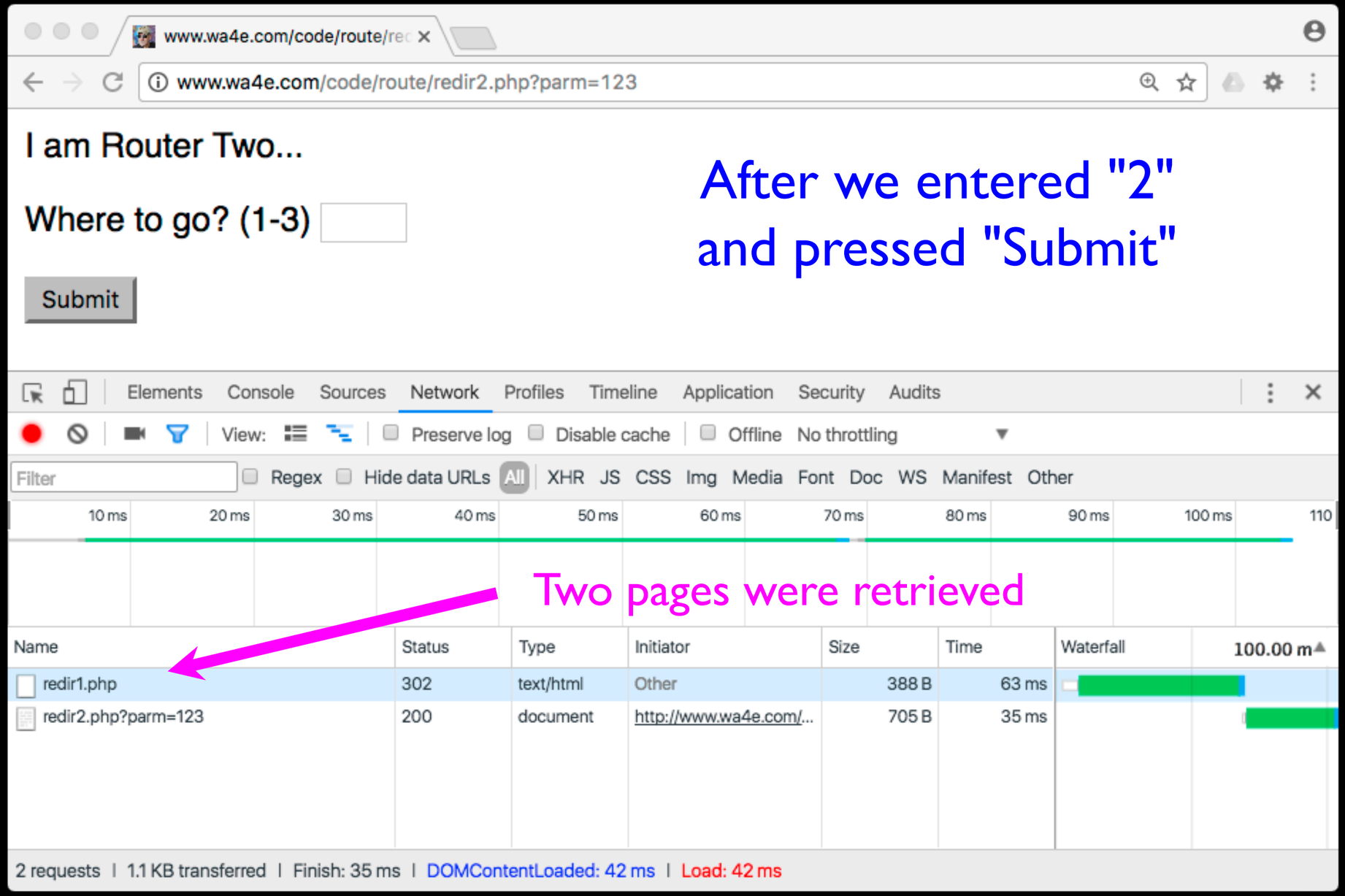
```
<html><= Error
<?php
/* This will give an error. Note the output
 * above, which is before the header() call */
header('Location: http://www.example.com/');
?>
```

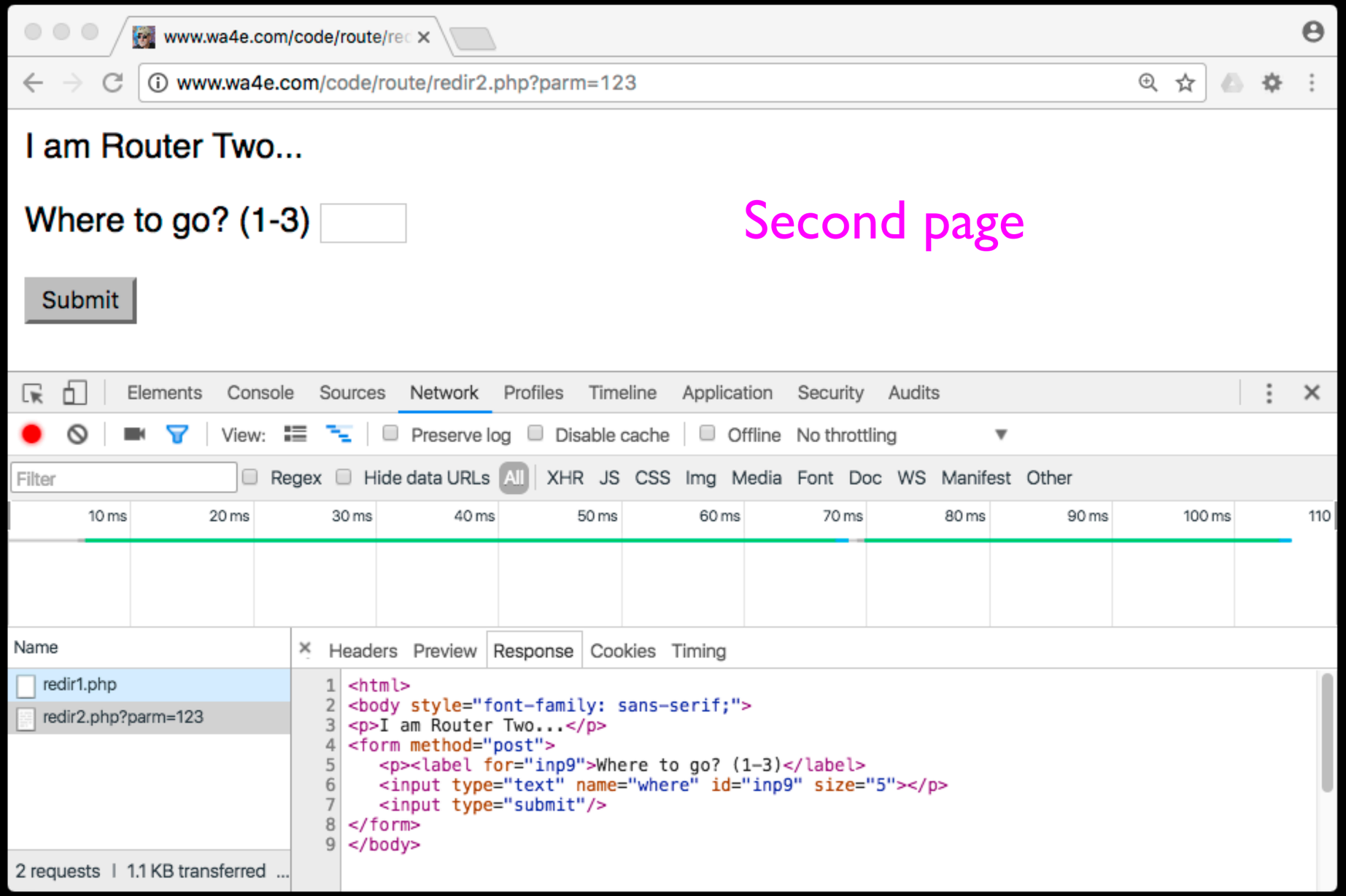
http://php.net/manual/en/function.header.php

```php
<?php
    session_start();
    if ( isset($_POST['where']) ) {
        if ( $_POST['where'] == '1' ) {
            header("Location: redir1.php");
            return;
        } else if ( $_POST['where'] == '2' ) {
            header("Location: redir2.php?parm=123");
            return;
        } else {
            header("Location: http://www.dr-chuck.com");
            return;
        }
    }
?>
<html>
<body style="font-family: sans-serif;">
<p>I am Router Two...</p>
<form method="post">
   <p><label for="inp9">Where to go? (1-3)</label>
   <input type="text" name="where" id="inp9" size="5"></p>
   <input type="submit"/></form>
</body>
```

http://www.wa4e.com/code/sessions/redir1.php


www.wa4e.com/code/route/rec
www.wa4e.com/code/route/redir1.php
I am Router One...
Where to go? (1-3) 1
Submit
www.wa4e.com/code/route/rec
www.wa4e.com/code/route/redir1.php
I am Router One...
Where to go? (1-3) 2
Submit
www.wa4e.com/code/route/rec
www.wa4e.com/code/route/redir1.php
I am Router One...
Where to go? (1-3) 3
Submit
www.wa4e.com/code/route/rec
www.wa4e.com/code/route/redir1.php
I am Router One...
Where to go? (1-3)
Submit
www.wa4e.com/code/route/rec
www.wa4e.com/code/route/redir2.php?parm=123
I am Router Two...
Where to go? (1-3)
Submit
Dr. Charles R. Severance Hom
www.dr-chuck.com
New: Tsugi: A PHP framework for IMS LTI Tools
New: MOOCs: Charles Severance at TEDxKalamazoo
Free Courses / Educational Material:
Gratipay
Select Language
Tweets by @drchuck
drchuck
@drchuck


www.wa4e.com/code/route/rec
www.wa4e.com/code/route/redir2.php?parm=123
I am Router Two...
Where to go? (1-3)
Submit
After we entered "2"
and pressed "Submit"
Elements Console Sources Network Profiles Timeline Application Security Audits
View: Preserve log Disable cache Offline No throttling
Filter Regex Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 80 ms 90 ms 100 ms 110
Two pages were retrieved
Name Status Type Initiator Size Time Waterfall 100.00 m
redir1.php 302 text/html Other 388 B 63 ms
redir2.php?parm=123 200 document http://www.wa4e.com/... 705 B 35 ms
2 requests | 1.1 KB transferred | Finish: 35 ms | DOMContentLoaded: 42 ms | Load: 42 ms

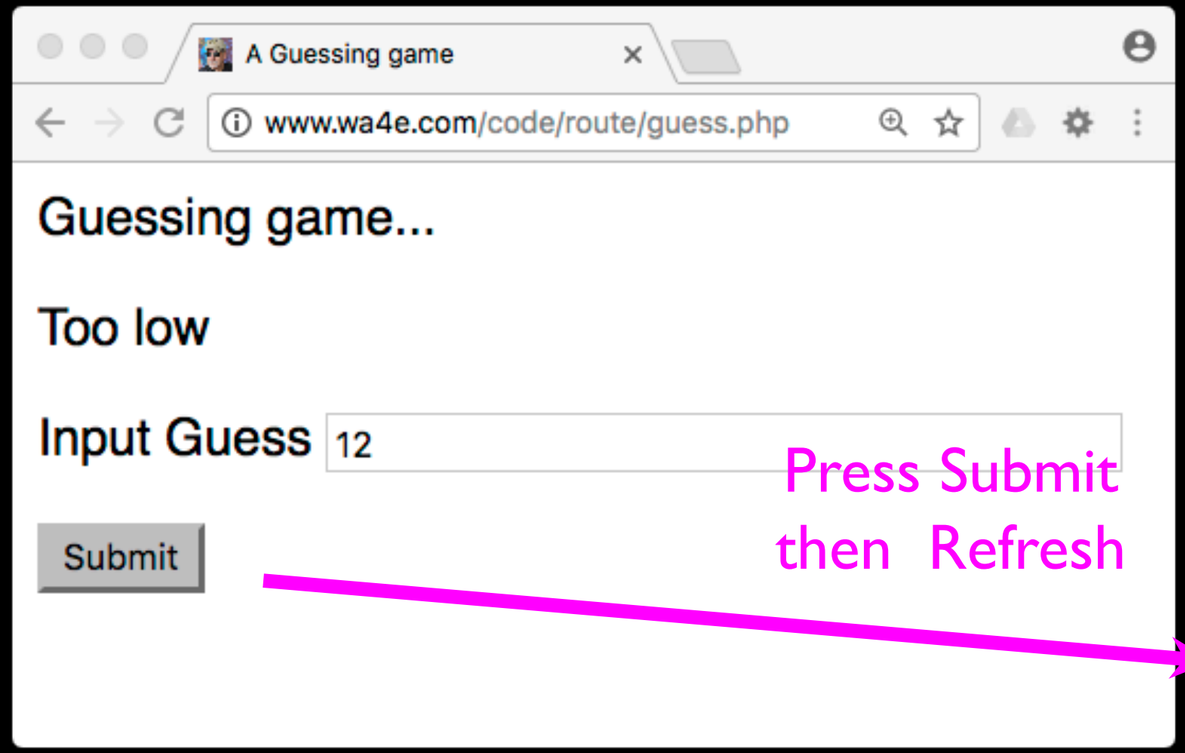

www.wa4e.com/code/route/rec
www.wa4e.com/code/route/redir2.php?parm=123
I am Router Two...
Where to go? (1-3)
Submit
Second page
Elements Console Sources Network Profiles Timeline Application Security Audits
View: Preserve log Disable cache Offline No throttling
Filter Regex Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 80 ms 90 ms 100 ms 110
Name
redir1.php
redir2.php?parm=123
2 requests | 1.1 KB transferred ...
Headers Preview Response Cookies Timing
1 <html>
2 <body style="font-family: sans-serif;">
3 I am Router Two...
4 <form method="post">
5 <label for="inp9">Where to go? (1-3)</label>
6 <input type="text" name="where" id="inp9" size="5">
7 <input type="submit"/>
8 </form>
9 </body>

POST / Refresh / Redirect

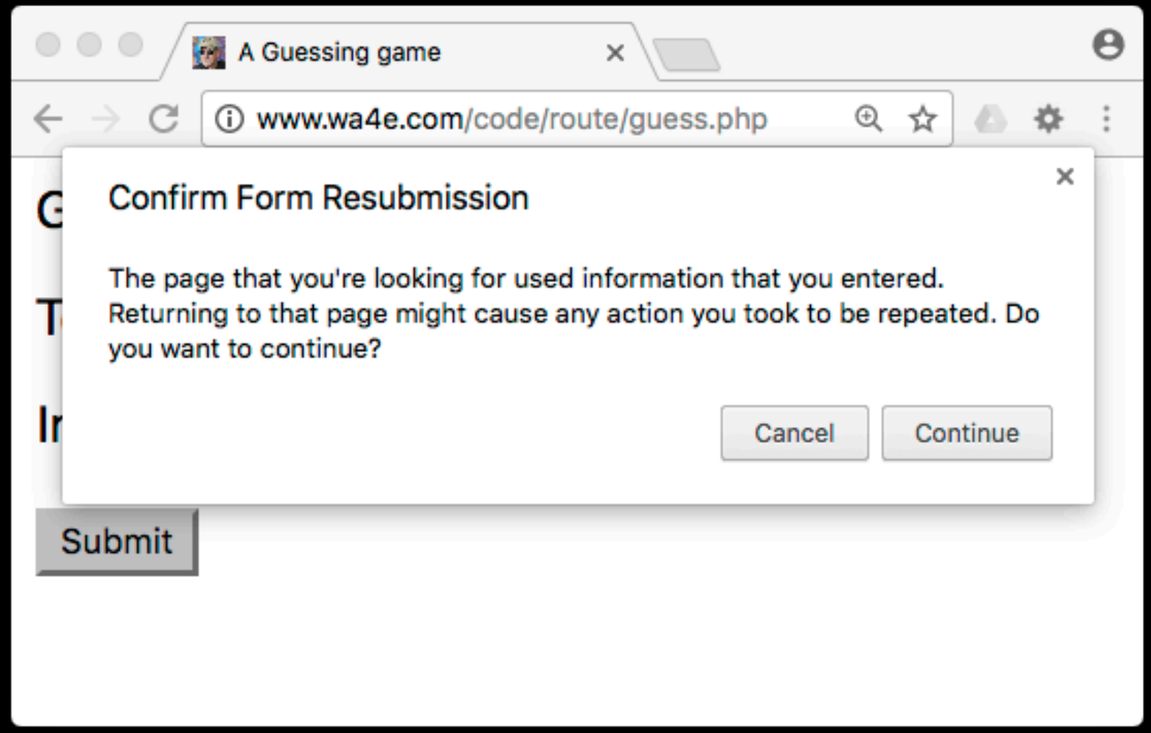
POST / Refresh / ☹

- Once you do a POST, if you refresh, the browser will re-send the POST data a second time.
- The user gets a pop-up that tries to explain what is about to happen.

guess.php



Press Submit
then Refresh

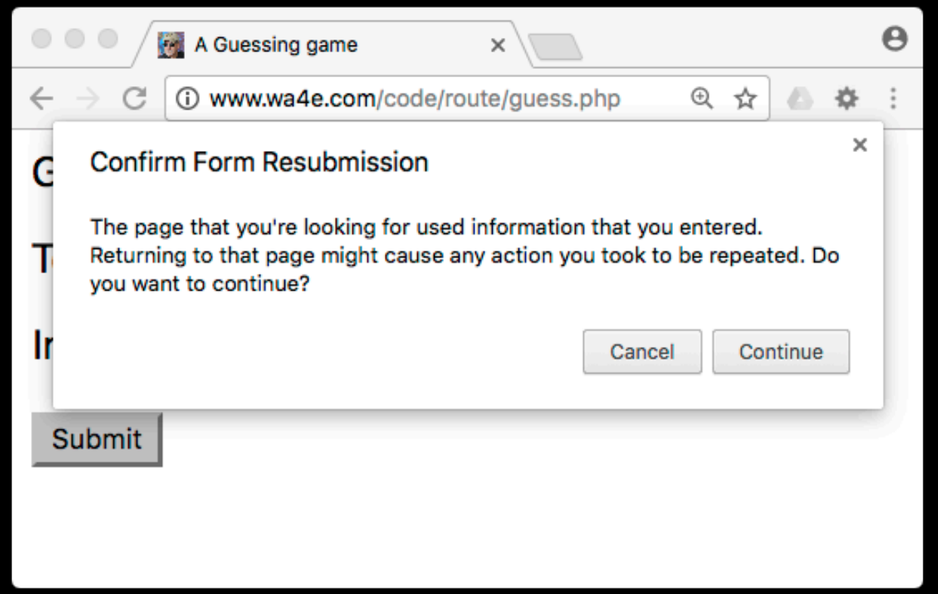


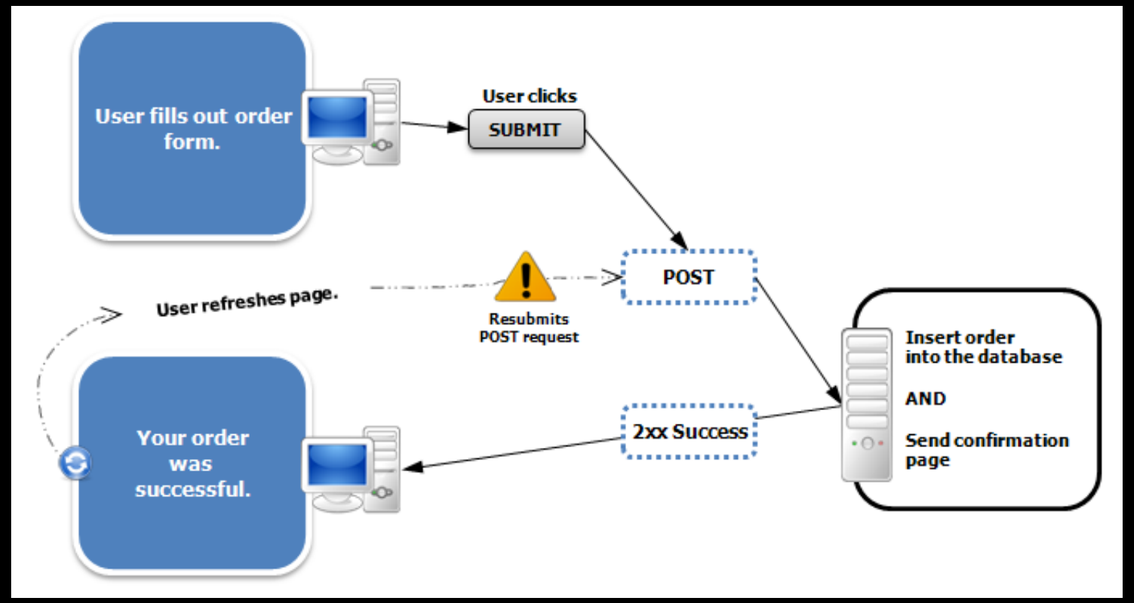
No Double Posts

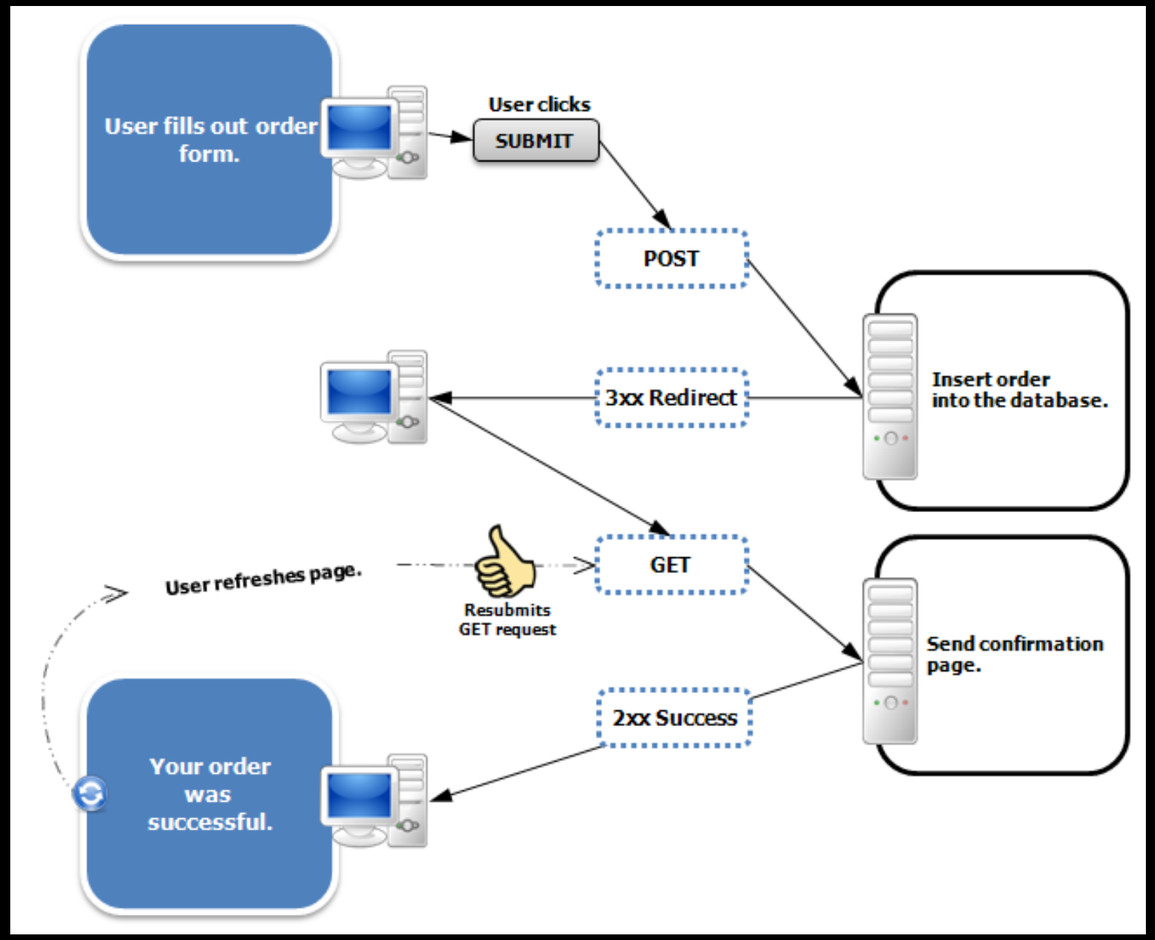
- Typically POST requests are adding or modifying data whilst GET requests view data
- It may be dangerous to do the same POST twice (say withdrawing funds from a bank account)
- So the browser insists on asking the user (out of your control)
- Kind of an ugly UX / bad usability

POST Redirect Rule

- The simple rule for pages intended for a browser is to never generate a page with HTML content when the app receives POST data
- Must redirect somewhere - even to the same script - forcing the browser to make a GET after the POST







https://en.wikipedia.org/wiki/Post/Redirect/Get

(Review)

```
<?php
    $guess = '';
    $message = false;
    if ( isset($_POST['guess']) ) {
        // Trick for integer / numeric parameters
        $guess = $_POST['guess'] + 0;
        if ( $guess == 42 ) {
            $message = "Great job!";
        } else if ( $guess < 42 ) {
            $message = "Too low";
        } else {
            $message = "Too high...";
        }
    }
?>
<html>
<head>
    <title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php
   if ( $message !== false ) {
        echo("<p>$message</p>\n");
    }
?>
<form method="post">
   <p><label for="guess">Input Guess</label>
   <input type="text" name="guess" id="guess" size="40"
 <?php   echo 'value="' . htmlentities($guess) . '"';
?>
   /></p>
   <input type="submit"/>
</form>
</body>
```

http://www.wa4e.com/code/sessions/guess.php

(Review)

```
<?php
    $guess = '';
    $message = false;
    if ( isset($_POST['guess']) ) {
        // Nifty trick
        $guess = $_POST['guess'] + 0;
        if ( $guess == 42 ) {
            $message = "Great job!";
        } else if ( $guess < 42 ) {
            $message = "Too low";
        } else {
            $message = "Too high...";
        }
    }
?>
<html> ...
```

```
<?php
    $guess = '';
    $message = false;
    if ( isset($_POST['gu
        // Trick for inte
        $guess = $_POST['
        if ( $guess == 42
            $message = "G
        } else if ( $gues
            $message = "T
        } else {
            $message = "T
        }
    }
?>
<html>
<head>
    <title>A Guessing gam
</head>
<body style="font-family:
<p>Guessing game...</p>
<?php
   if ( $message !== fals
        echo("<p>$message
    }
?>
<form method="post">
   <p><label for="guess">
   <input type="text" nam
 <?php   echo 'value="' .
?>
   /></p>
   <input type="submit"/>
</form>
</body>
```

(Review)

```
...
?>
<html>
<head>
    <title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<p>Guessing game...</p>
<?php   if ( $message !== false )  {
        echo("<p>$message</p>\n");
    }
?>
<form method="post">
   <p><label for="guess">Input Guess</label>
   <input type="text" name="guess" id="guess" size="40" <?php   echo
'value="' . htmlentities($guess) . '"';
?>
   /></p>
   <input type="submit"/>
</form>
</body>
```

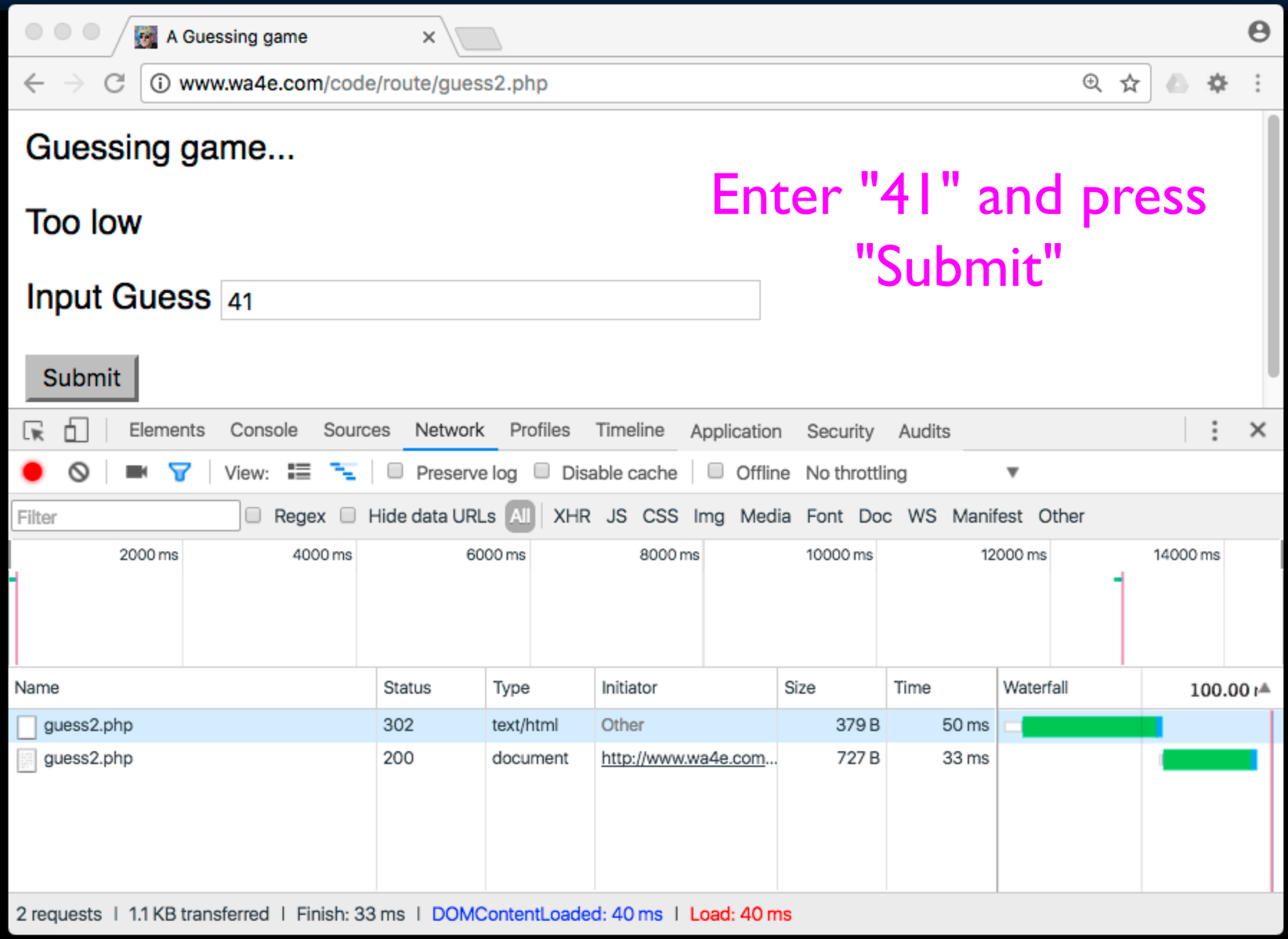
(Improved)

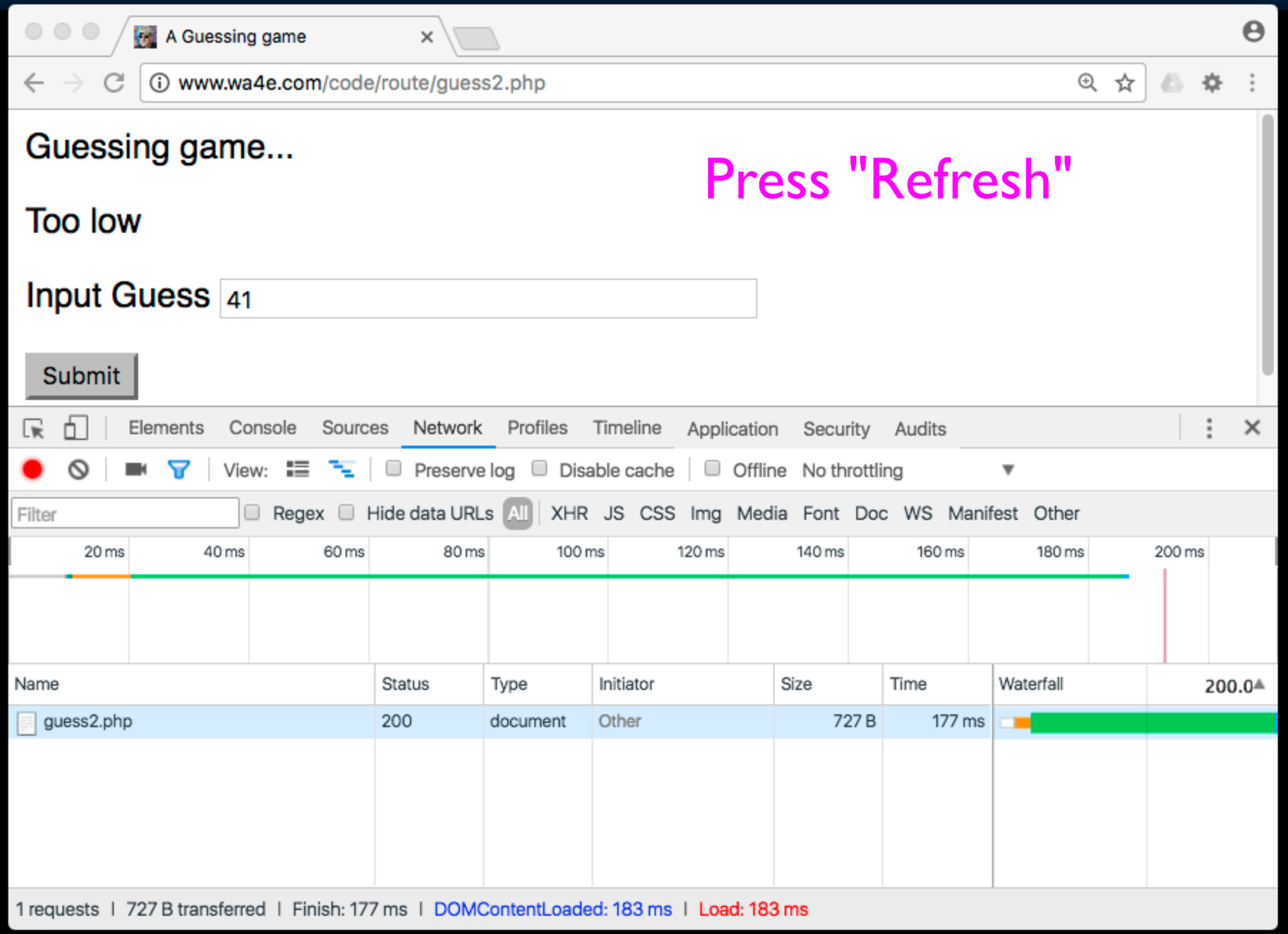
```
<?php
    session_start();
    if ( isset($_POST['guess']) ) {
        $guess = $_POST['guess'] + 0;
        $_SESSION['guess'] = $guess;
        if ( $guess == 42 ) {
            $_SESSION['message'] = "Great job!";
        } else if ( $guess < 42 ) {
            $_SESSION['message'] = "Too low";
        } else {
            $_SESSION['message'] = "Too high...";
        }
        header("Location: guess2.php");
        return;
    }
?>
<html>
```

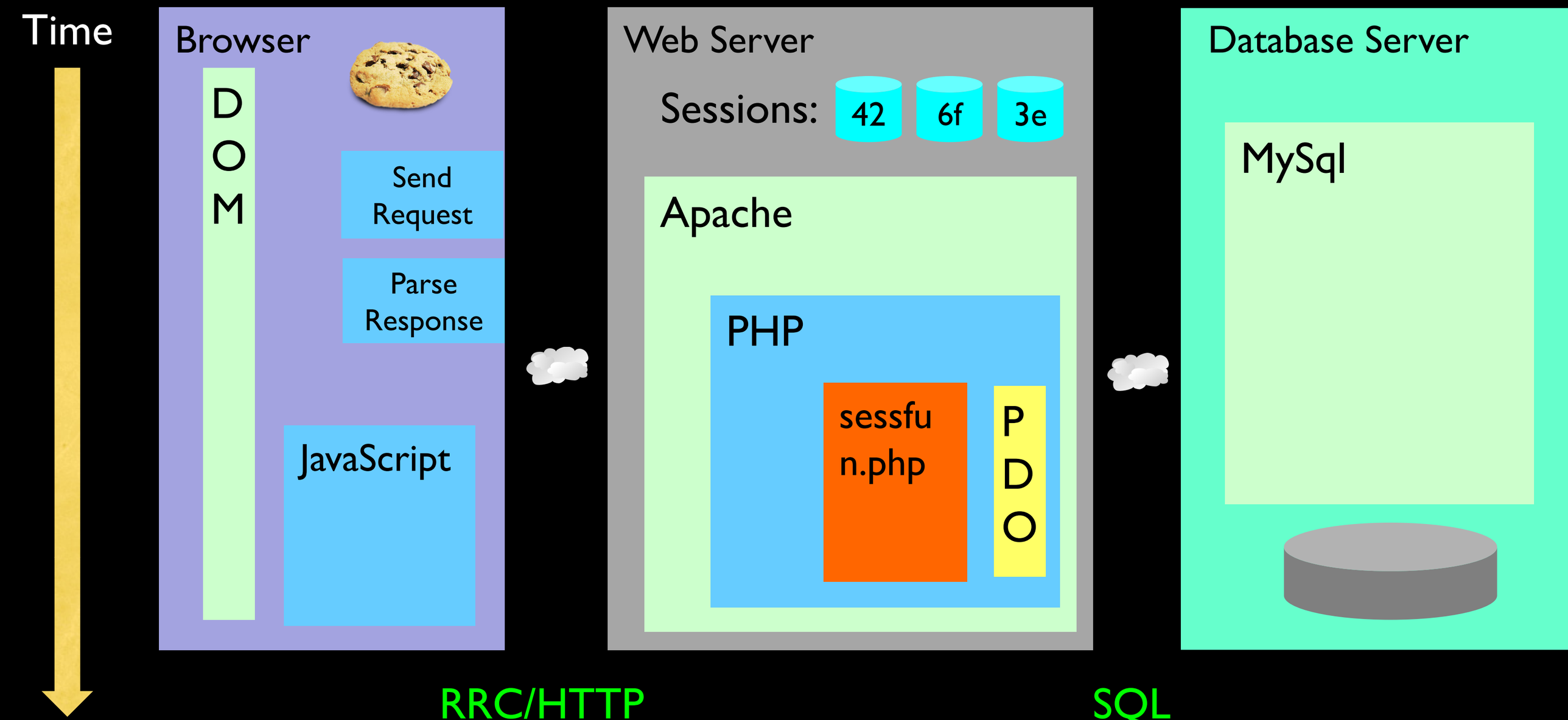
http://www.wa4e.com/code/sessions/guess2.php

guess2.php

```
<html>
<head>
<title>A Guessing game</title>
</head>
<body style="font-family: sans-serif;">
<?php
$guess = isset($_SESSION['guess']) ? $_SESSION['guess'] : '';
$message = isset($_SESSION['message']) ? $_SESSION['message'] : false;
?>
<p>Guessing game...</p>
<?php
   if ( $message !== false )  {
        echo("<p>$message</p>\n");
   }
?>
<form method="post">
   <p><label for="guess">Input Guess</label>
   <input type="text" name="guess" id="guess" size="40"
    <?php   echo 'value="' . htmlentities($guess) . '"';?>
   /></p>
   <input type="submit"/>
</form>
</body>
```


A Guessing game
www.wa4e.com/code/route/guess2.php
Guessing game...
Too low
Input Guess 41
Submit
Enter "41" and press "Submit"
Elements Console Sources Network Profiles Timeline Application Security Audits
View: Preserve log Disable cache Offline No throttling
Filter Regex Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
2000 ms 4000 ms 6000 ms 8000 ms 10000 ms 12000 ms 14000 ms
Name Status Type Initiator Size Time Waterfall
guess2.php 302 text/html Other 379 B 50 ms
guess2.php 200 document http://www.wa4e.com... 727 B 33 ms
2 requests | 1.1 KB transferred | Finish: 33 ms | DOMContentLoaded: 40 ms | Load: 40 ms

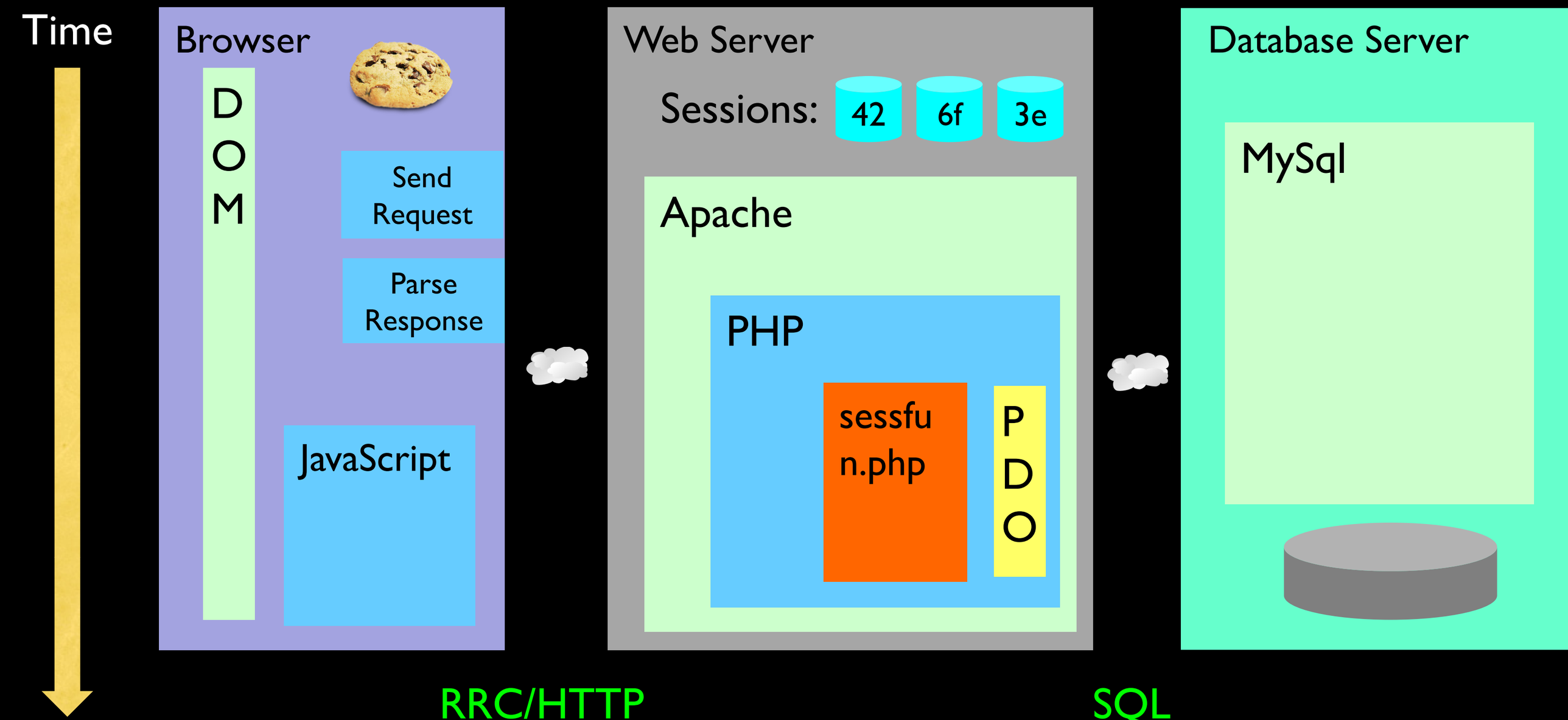

A Guessing game
www.wa4e.com/code/route/guess2.php
Guessing game...
Too low
Input Guess 41
Submit
Press "Refresh"
Elements Console Sources Network Profiles Timeline Application Security Audits
View: Preserve log Disable cache Offline No throttling
Filter Regex Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
20 ms 40 ms 60 ms 80 ms 100 ms 120 ms 140 ms 160 ms 180 ms 200 ms
Name Status Type Initiator Size Time Waterfall 200.0
guess2.php 200 document Other 727 B 177 ms
1 requests | 727 B transferred | Finish: 177 ms | DOMContentLoaded: 183 ms | Load: 183 ms


Time
Browser
DOM
Send Request
Parse Response
JavaScript
Web Server
Sessions:
42
6f
3e
Apache
PHP
sessfun.php
PDO
Database Server
MySql
RRC/HTTP
SQL

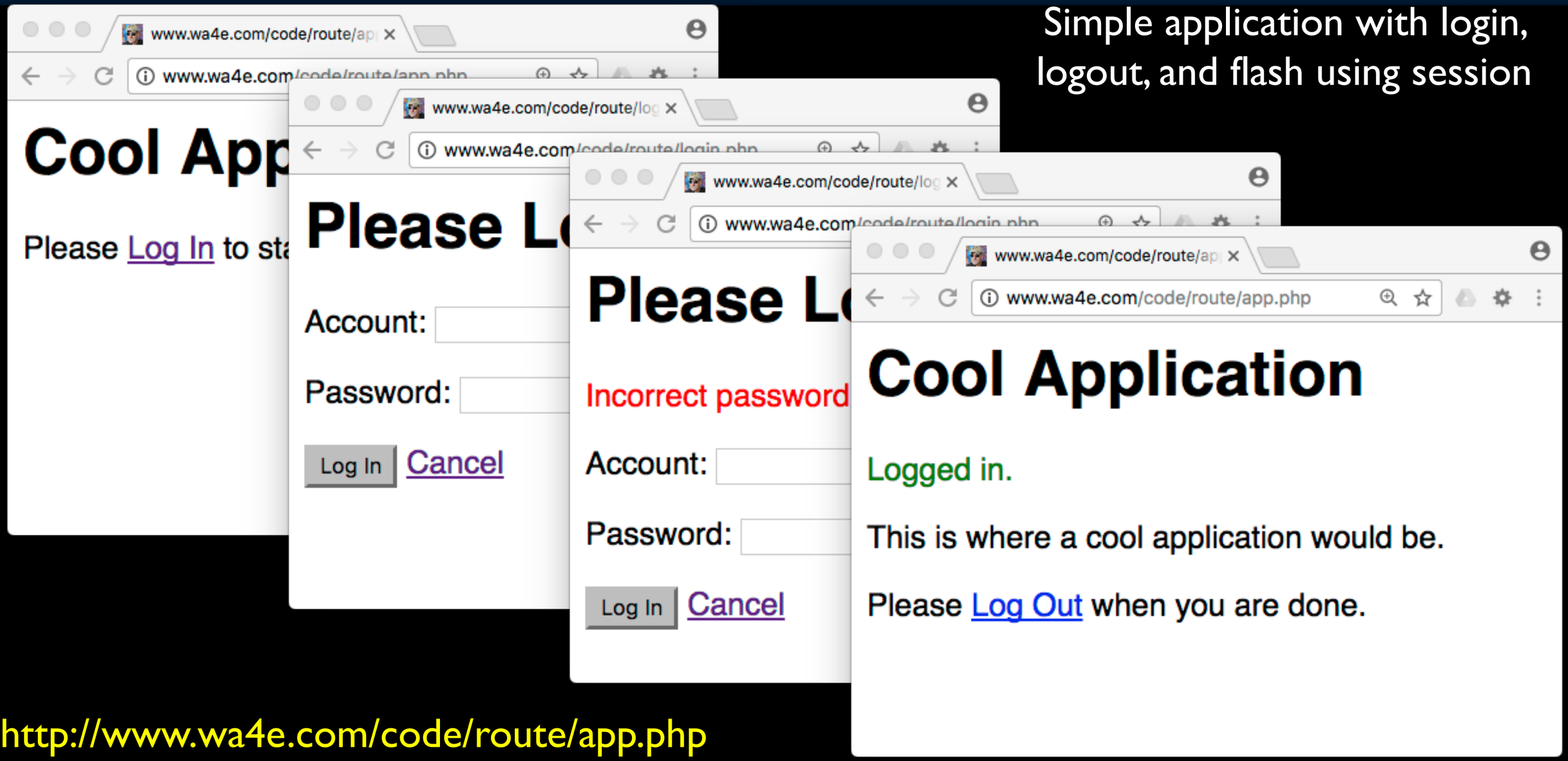
Implementing Login and Logout

Session / Authentication

- Having a session is not the same as being logged in.
- Generally you have a session the instant you connect to a web site.
- The Session ID cookie is set when the first page is delivered.
- Login puts user information in the session (stored in the server).
- Logout removes user information from the session.


Time
Browser
DOM
Send Request
Parse Response
JavaScript
Web Server
Sessions:
42
6f
3e
Apache
PHP
sessfun.php
PDO
Database Server
MySql
RRC/HTTP
SQL

Simple application with login, logout, and flash using session



http://www.wa4e.com/code/route/app.php

http://www.wa4e.com/code/route.zip

login.php

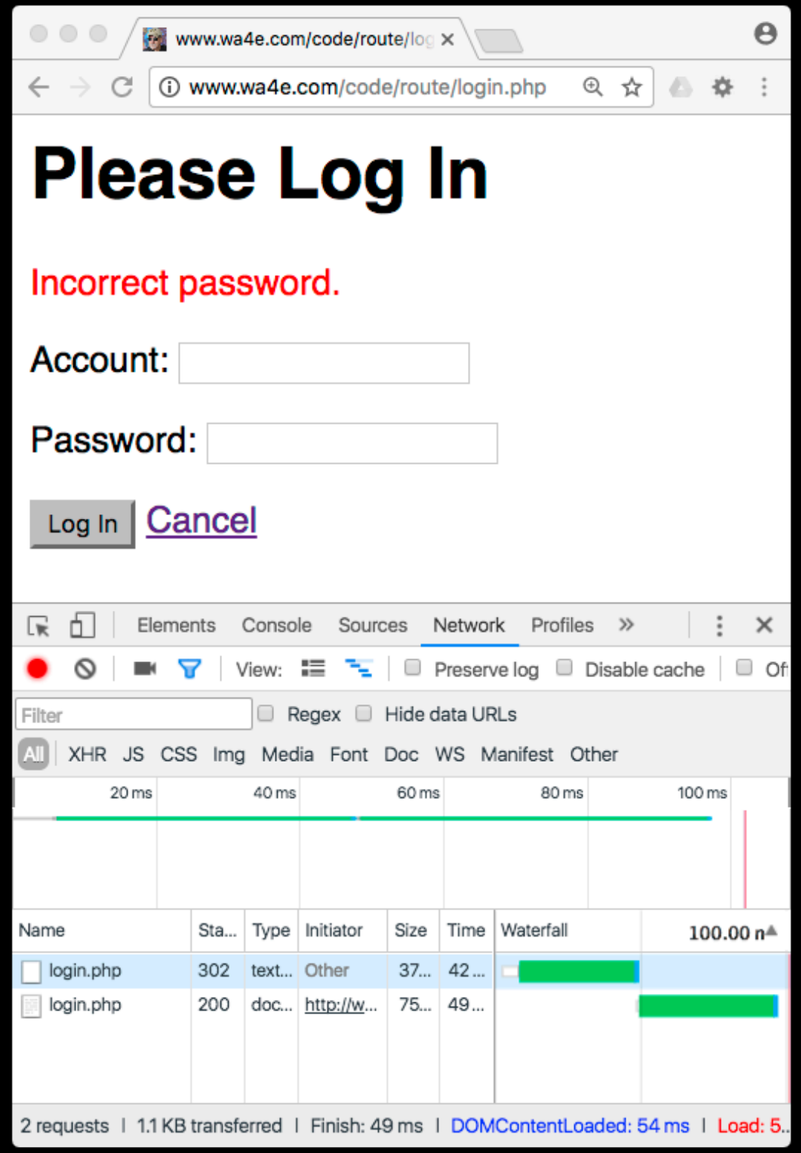
```
<body style="font-family: sans-serif;">
<h1>Please Log In</h1>
<?php
    if ( isset($_SESSION["error"]) ) {
        echo('<p style="color:red">'.$_SESSION["error"]."</p>\n");
        unset($_SESSION["error"]);
    }
    if ( isset($_SESSION["success"]) ) {
        echo('<p style="color:green">'.$_SESSION["success"]."</p>\n");
        unset($_SESSION["success"]);
    }
?>
<form method="post">
<p>Account: <input type="text" name="account" value=""></p>
<p>Password: <input type="text" name="pw" value=""></p>
<!-- password is umsi -->
<p><input type="submit" value="Log In">
<a href="app.php">Cancel</a></p>
</form>
</body>
```

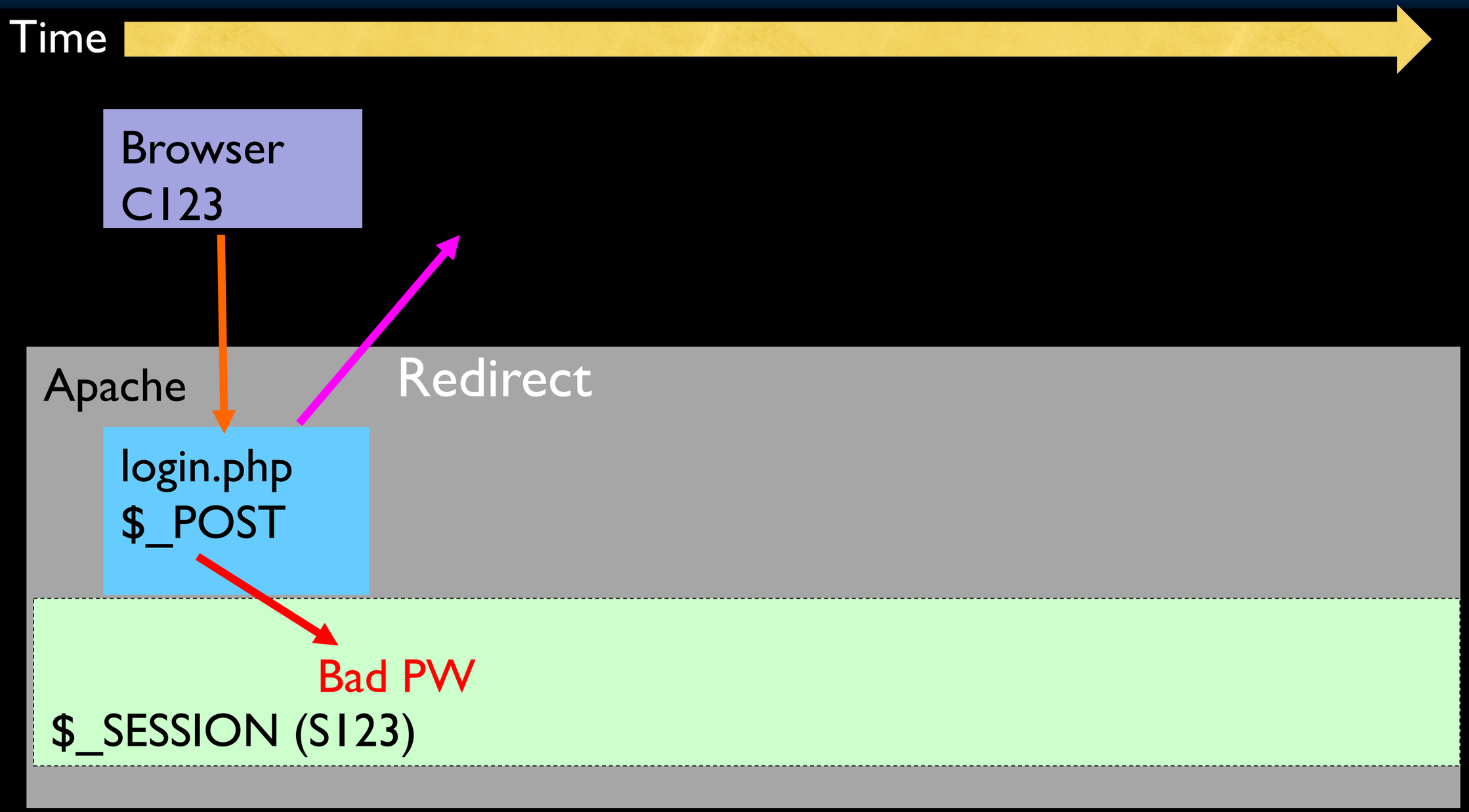
```php
<?php
    session_start();
    if ( isset($_POST["account"]) && isset($_POST["pw"]) ) {
        unset($_SESSION["account"]);  // Logout current user
        if ( $_POST['pw'] == 'umsi' ) {
            $_SESSION["account"] = $_POST["account"];
            $_SESSION["success"] = "Logged in.";
            header( 'Location: app.php' ) ;
            return;
        } else {
            $_SESSION["error"] = "Incorrect password.";
            header( 'Location: login.php' ) ;
            return;
        }
    }
?>
<html>
```

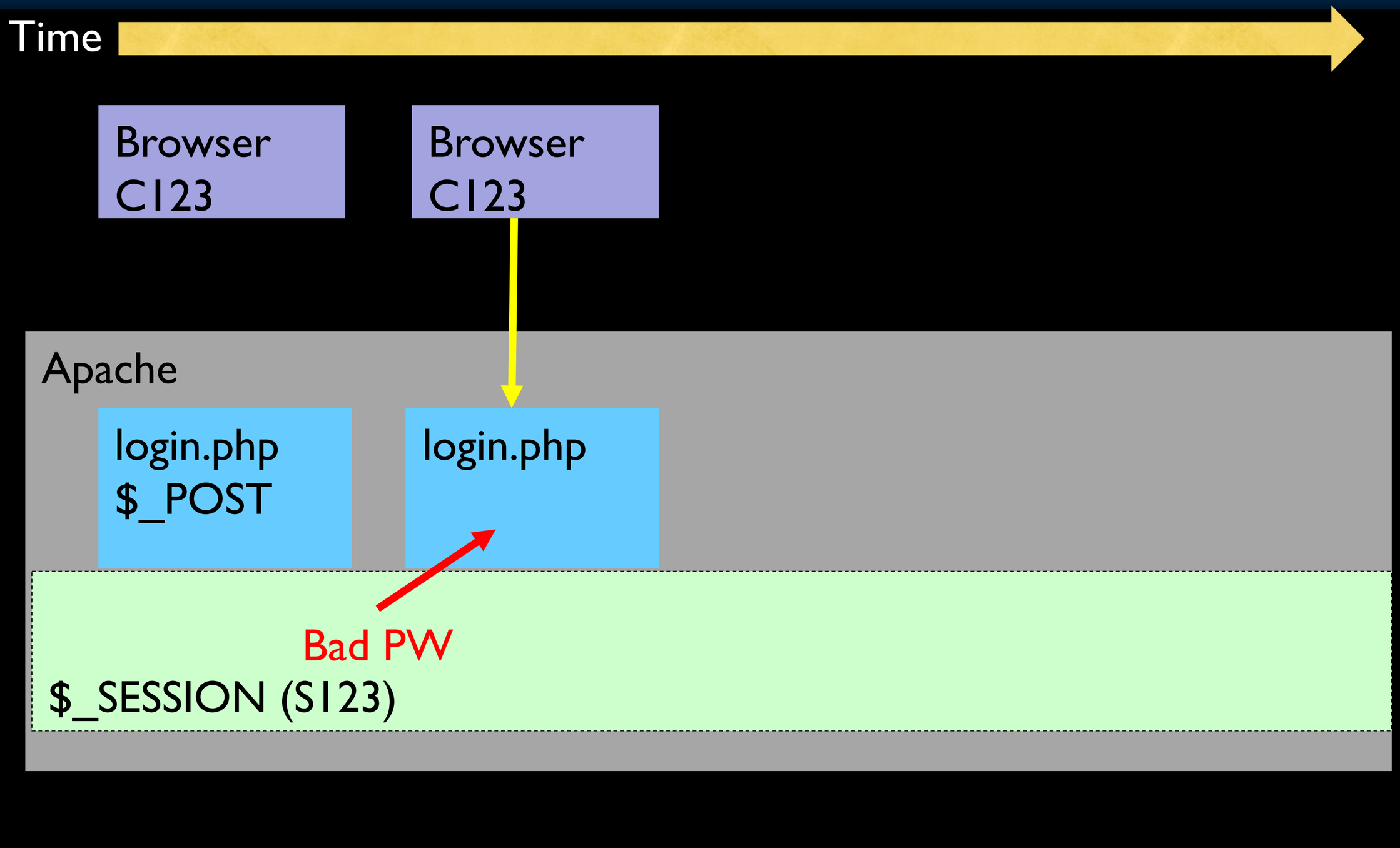
http://www.wa4e.com/code/sessions/login.php

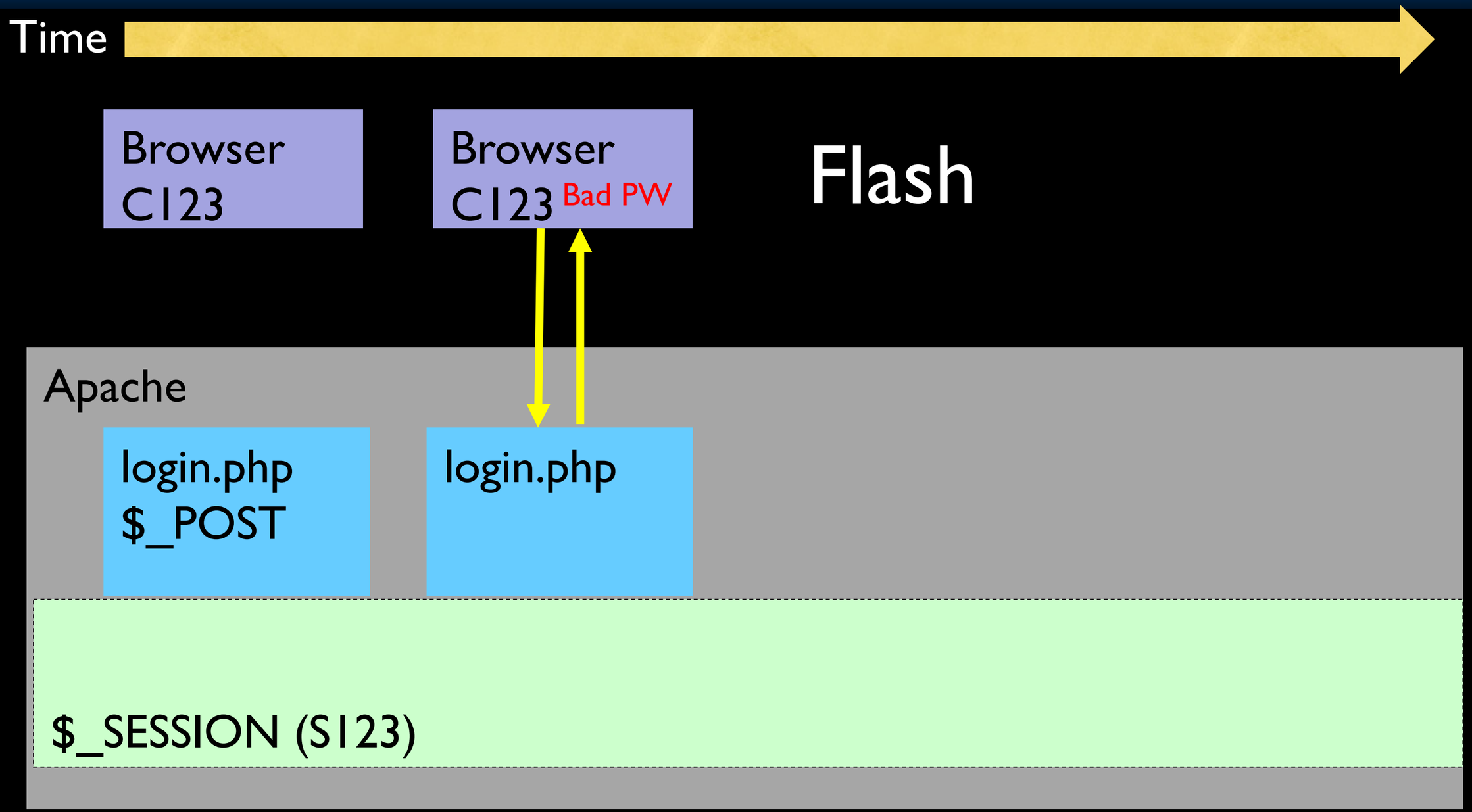
POST-Redirect-GET-Flash

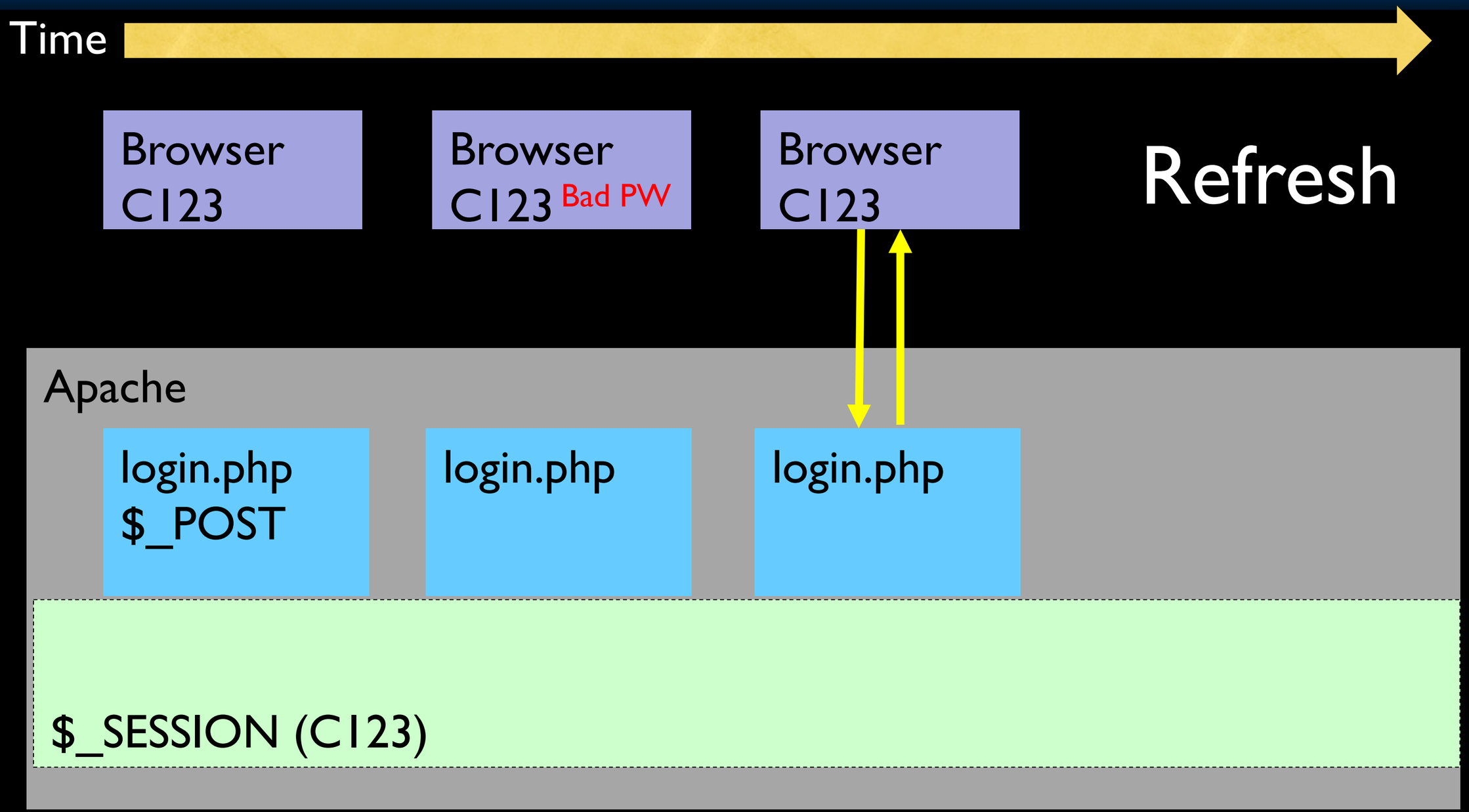
- POST detects error in input data and puts a message into $_SESSION and redirects
- GET sees the message in the session, displays it and then deletes it
- Flash = “Seen once”




Time
Browser
C123
Apache
Redirect
login.php
$_POST
Bad PW
$_SESSION (S123)


Time
Browser
C123
Browser
C123
Apache
login.php
$_POST
login.php
Bad PW
$_SESSION (S123)


Time
Browser C123
Browser C123 Bad PW
Flash
Apache
login.php $_POST
login.php
$_SESSION (S123)

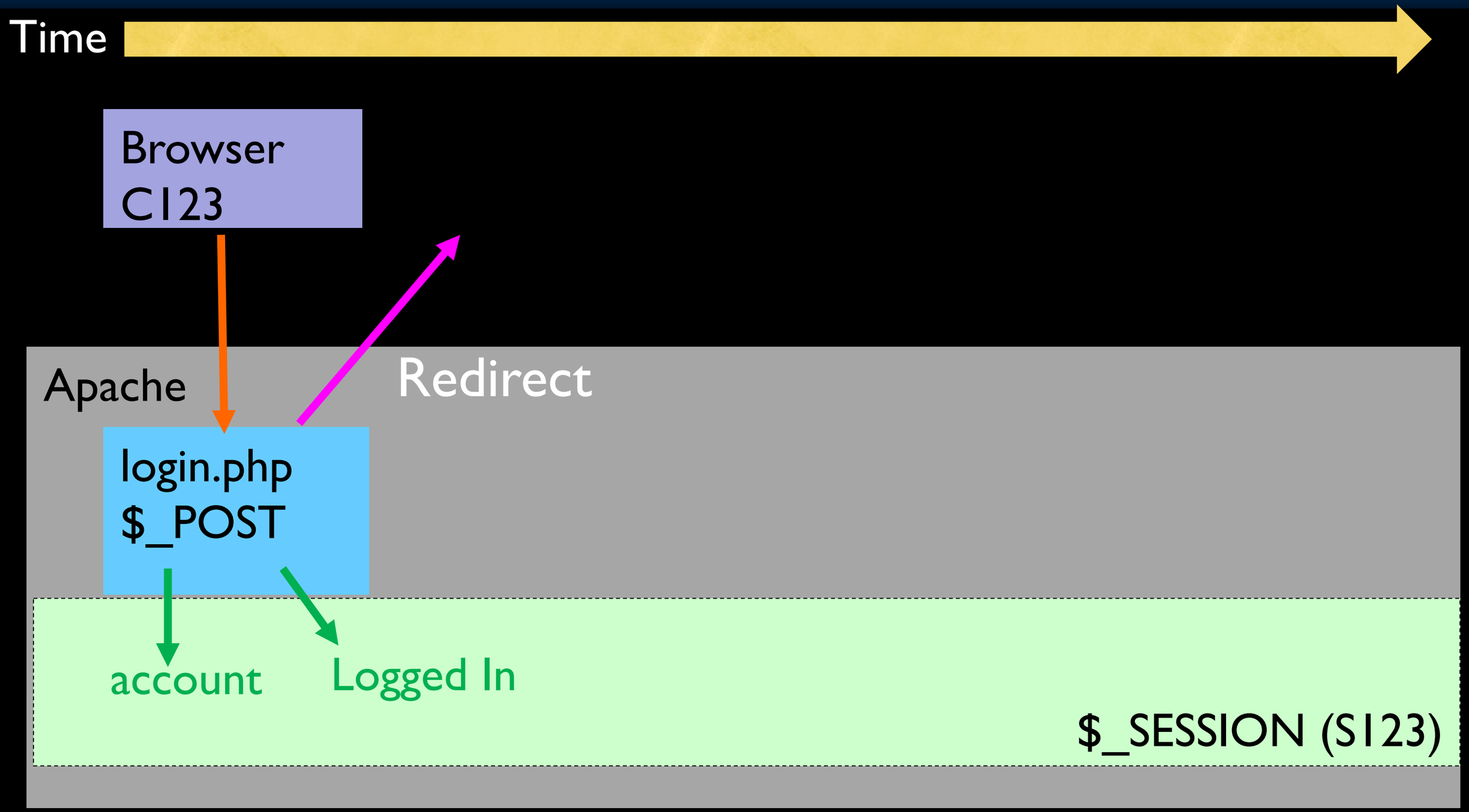

Time
Browser C123
Browser C123 Bad PW
Browser C123
Refresh
Apache
login.php $_POST
login.php
login.php
$_SESSION (C123)

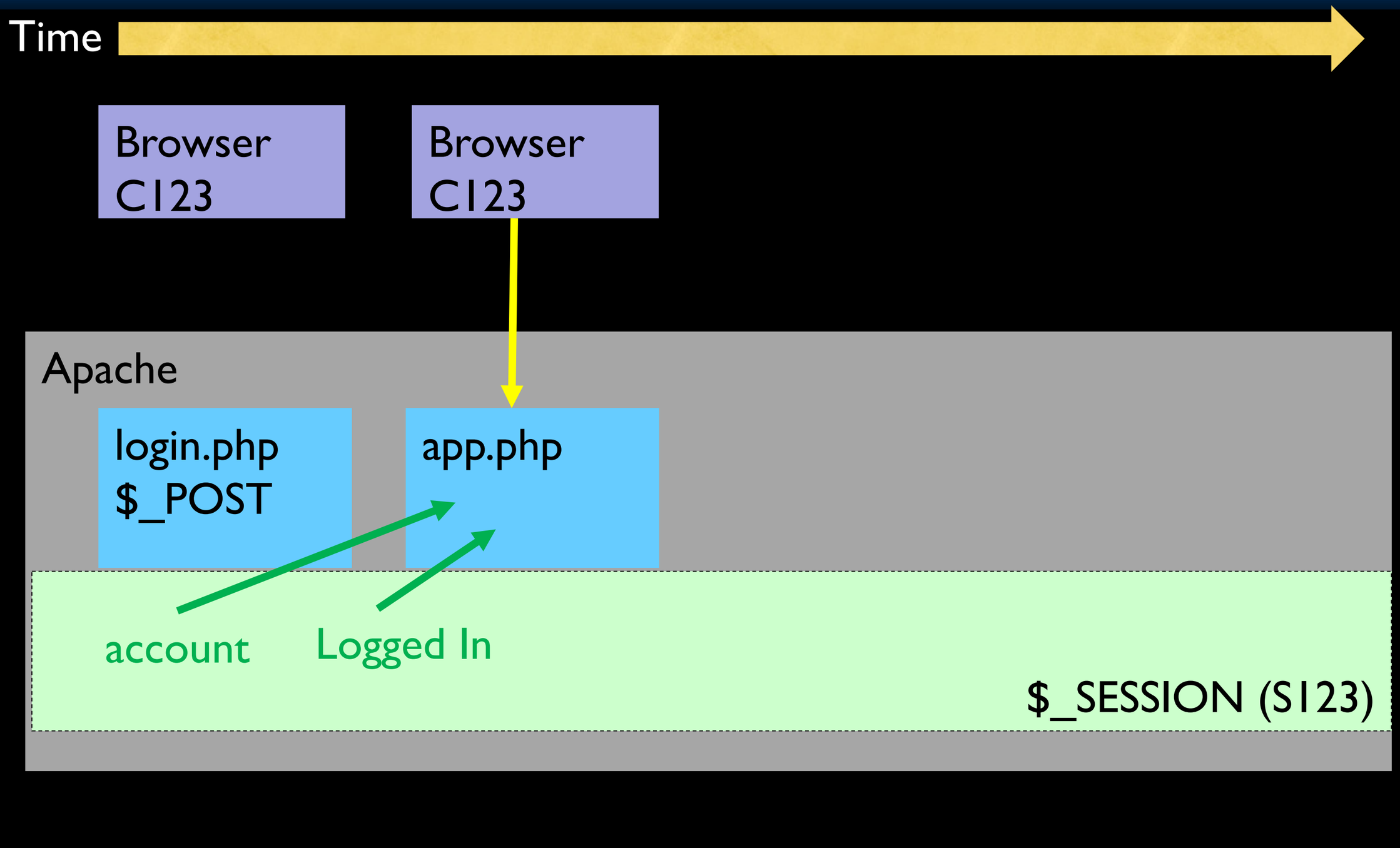
login.php

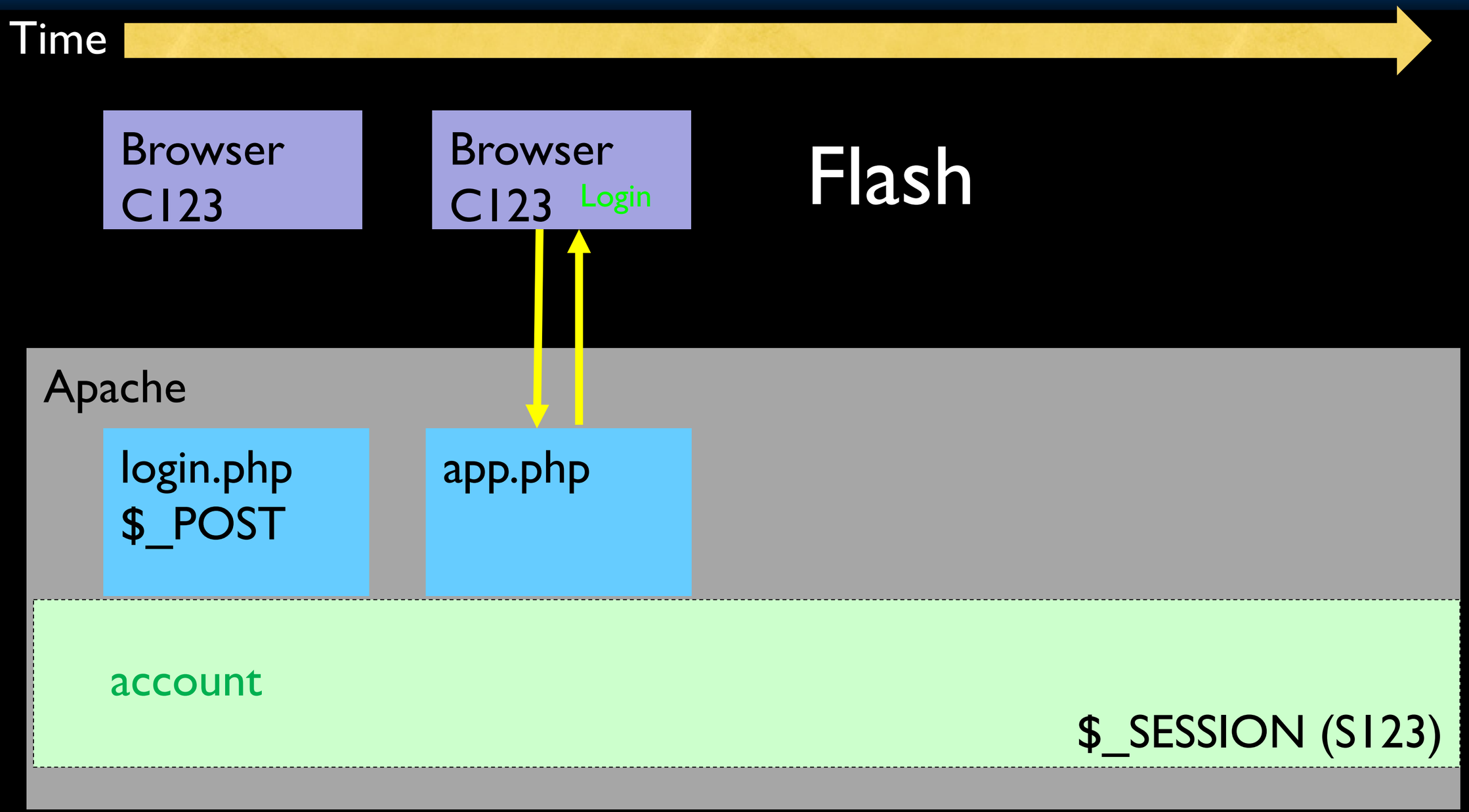
```
<body style="font-family: sans-serif;">
<h1>Please Log In</h1>
<?php
    if ( isset($_SESSION["error"]) ) {
        echo('<p style="color:red">'.$_SESSION["error"]."</p>\n");
        unset($_SESSION["error"]);
    }
    if ( isset($_SESSION["success"]) ) {
        echo('<p style="color:green">'.$_SESSION["success"]."</p>\n");
        unset($_SESSION["success"]);
    }
?>
<form method="post">
<p>Account: <input type="text" name="account" value=""></p>
<p>Password: <input type="text" name="pw" value=""></p>
<!-- password is umsi -->
<p><input type="submit" value="Log In">
<a href="app.php">Cancel</a></p>
</form>
</body>
```

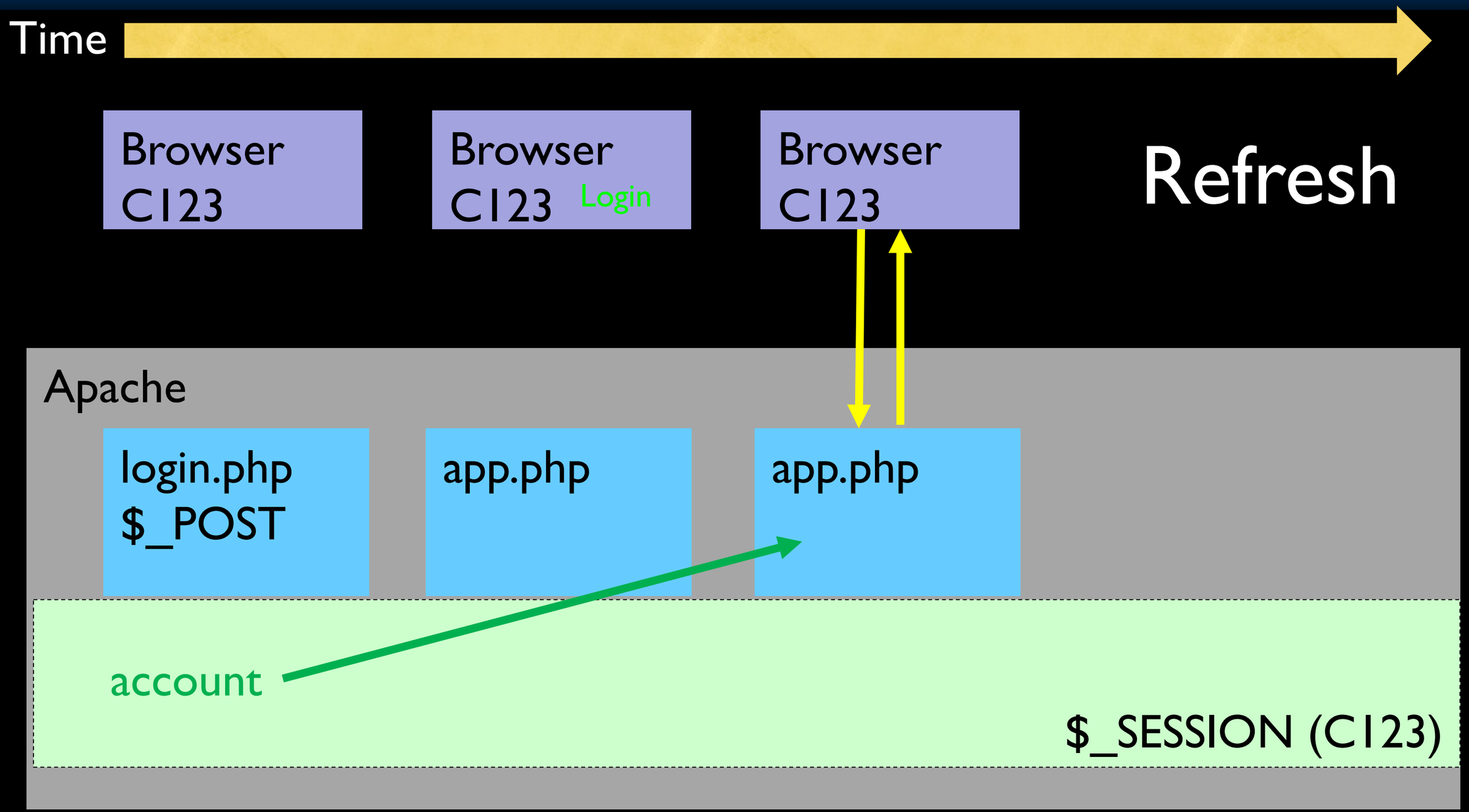
```
<html><head></head><body style="font-family: sans-serif;">
<h1>Cool Application</h1>
<?php
    if ( isset($_SESSION["success"]) ) {
        echo('<p style="color:green">'.$_SESSION["success"]."</p>\n");
        unset($_SESSION["success"]);
    }

    // Check if we are logged in!
    if ( ! isset($_SESSION["account"]) ) { ?>
       <p>Please <a href="login.php">Log In</a> to start.</p>
    <?php } else { ?>
       <p>This is where a cool application would be.</p>
       <p>Please <a href="logout.php">Log Out</a> when you are done.</p>
    <?php } ?>
</body></html>
```

http://www.wa4e.com/code/sessions/app.php


Time
Browser
C123
Apache
Redirect
login.php
$_POST
account
Logged In
$_SESSION (S123)

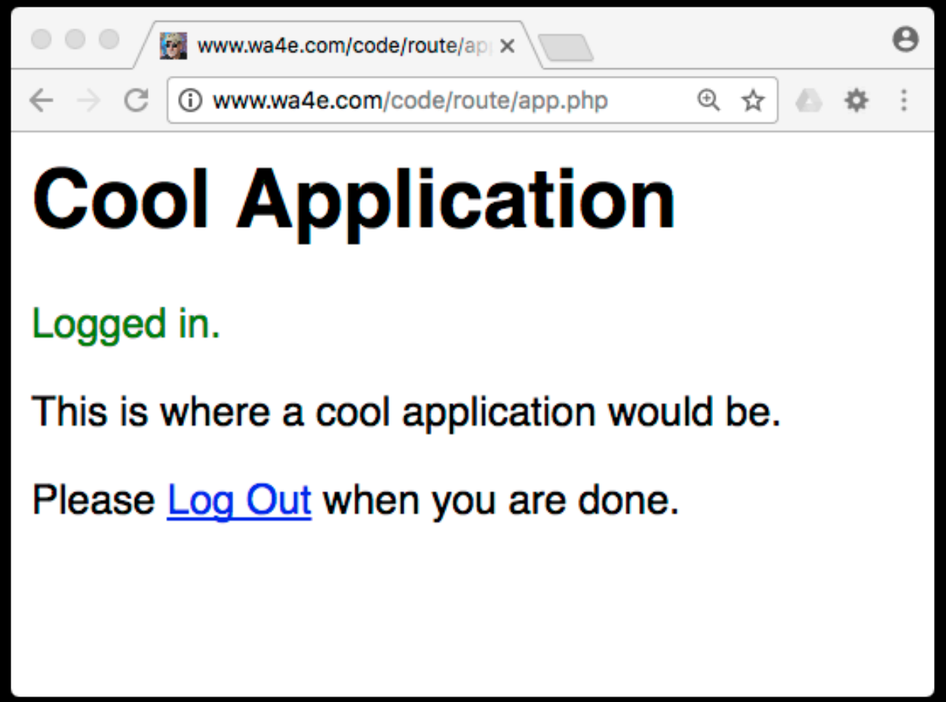

Time
Browser C123
Browser C123
Apache
login.php $_POST
app.php
account
Logged In
$_SESSION (S123)

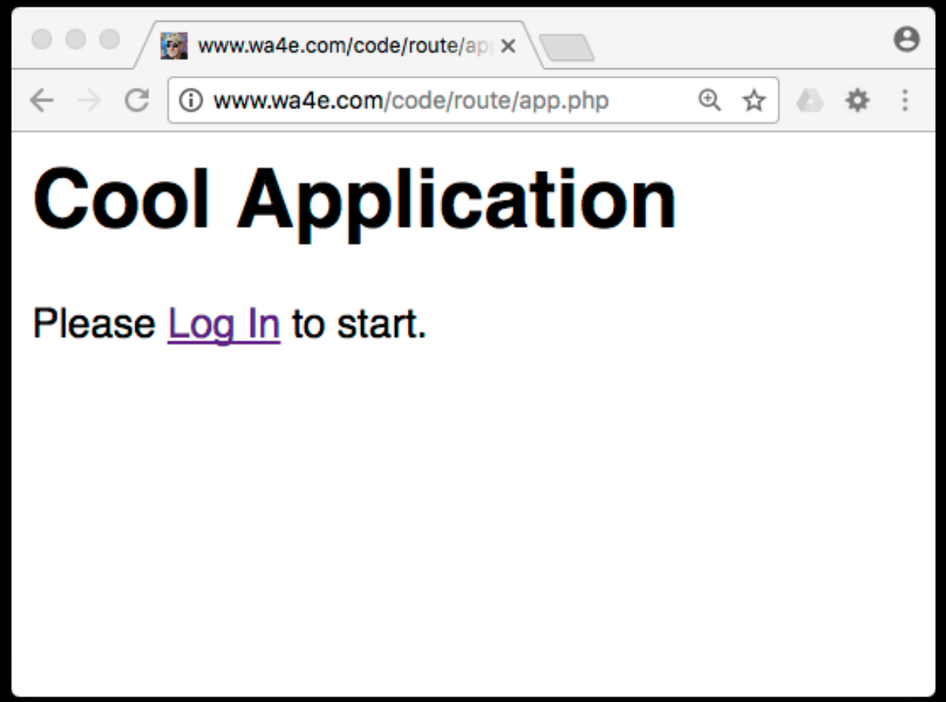

Time
Browser C123
Browser C123
Login
Flash
Apache
login.php $_POST
app.php
account
$_SESSION (S123)


Time
Browser C123
Browser C123 Login
Browser C123
Refresh
Apache
login.php $_POST
app.php
app.php
account
$_SESSION (C123)

logout.php

```php
<?php
    session_start();
    session_destroy();
    header("Location: app.php");
```





```
<html><head></head><body style="font-family: sans-serif;">
<h1>Cool Application</h1>
<?php
    if ( isset($_SESSION["success"]) ) {
        echo('<p style="color:green">'.$_SESSION["success"]."</p>\n");
        unset($_SESSION["success"]);
    }

    // Check if we are logged in!
    if ( ! isset($_SESSION["account"]) ) { ?>
        <p>Please <a href="login.php">Log In</a> to start.</p>
    <?php } else { ?>
        <p>This is where a cool application would be.</p>
        <p>Please <a href="logout.php">Log Out</a> when you are done.</p>
    <?php } ?>
</body></html>
```

http://www.wa4e.com/code/sessions/app.php

Summary

- Redirect
- Post-Redirect-Get
- Flash Messages
- Sessions and Login / Logout

Acknowledgements / Contributions

These slides are Copyright 2010- Charles R. Severance (www.dr-chuck.com) as part of www.wa4e.com and made available under a Creative Commons Attribution 4.0 License. Please maintain this slide in all copies of the document to comply with the attribution requirements of the license. If you make a change, feel free to add your name and organization to the list of contributors on this page as you republish the materials.

Initial Development: Charles Severance, University of Michigan School of Information

Insert new Contributors and Translators here including names and dates

Continue new Contributors and Translators here

Copyright Attribution

- Cookie Image: By brainloc on sxc.hu (Bob Smith) (stock.xchng) [CC BY 2.5 (http://creativecommons.org/licenses/by/2.5)], via Wikimedia Commons