introduction to

SCRIPTING, DATABASES, SYSTEM ARCHITECTURE

WEB SERVICES III (advanced + quiz + A11)

Claus Brabrand

(((brabrand@itu.dk)))

Associate Professor, Ph.D.

(((Software and Systems)))

IT University of Copenhagen

Exam Eligibility

- Originally:

  "10 out of 11"

- Then, two things happened:

  "A8 optional" (technical problems)

  "A11 optional" (exam office deadline)

- Which then means:

  "10 out of 11" (A8 + A11 auto approved)

  = "8 out of *the* 9" (A1 – A7, A9, and A10)

- Now (strictly better for you):

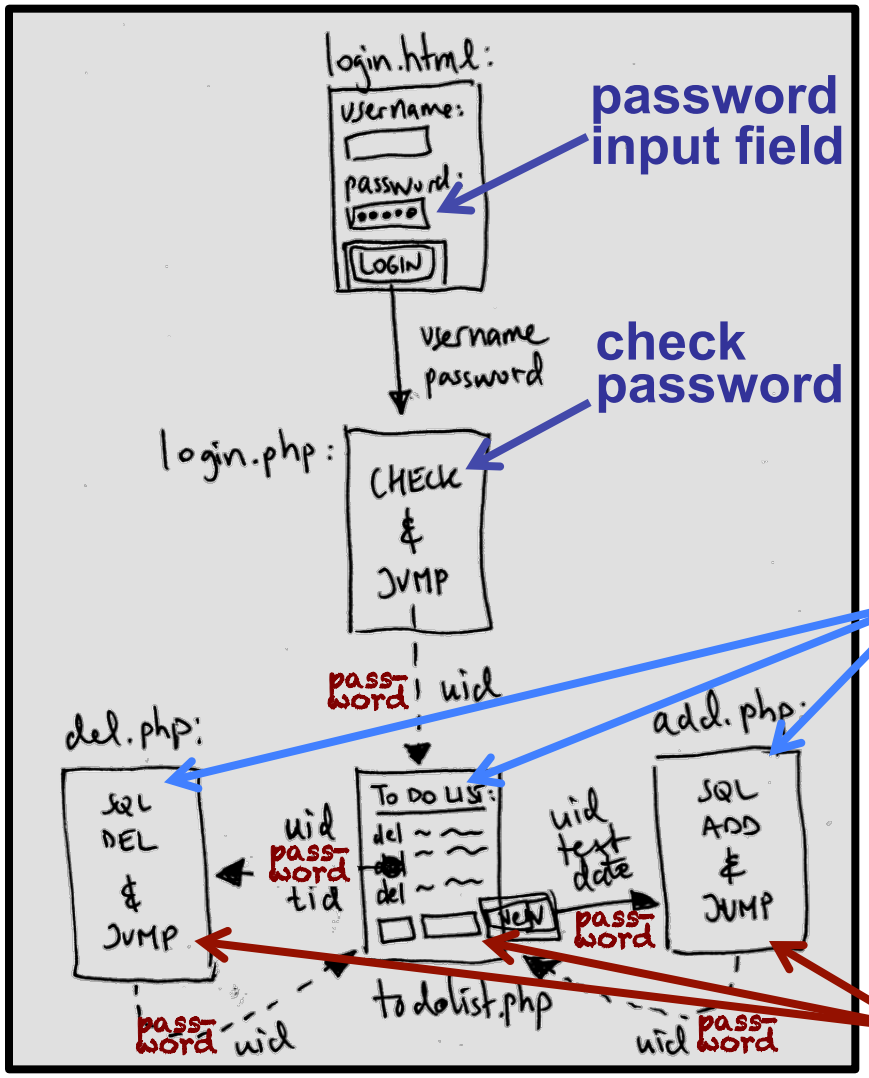
  "8" (any approved assignments)

Agenda

- Advanced topics:
  - Cookies
  - Sessions
  - User Authentication
  - Encrypted Communication
- Web Service: Quiz
- A11: Last Year's Exam (exam training)

User Authentication (log in)

- Recall To-Do-List:



Danger: insecure !
(a hacker can "bypass" login by "jumping" directly to todolist.php)

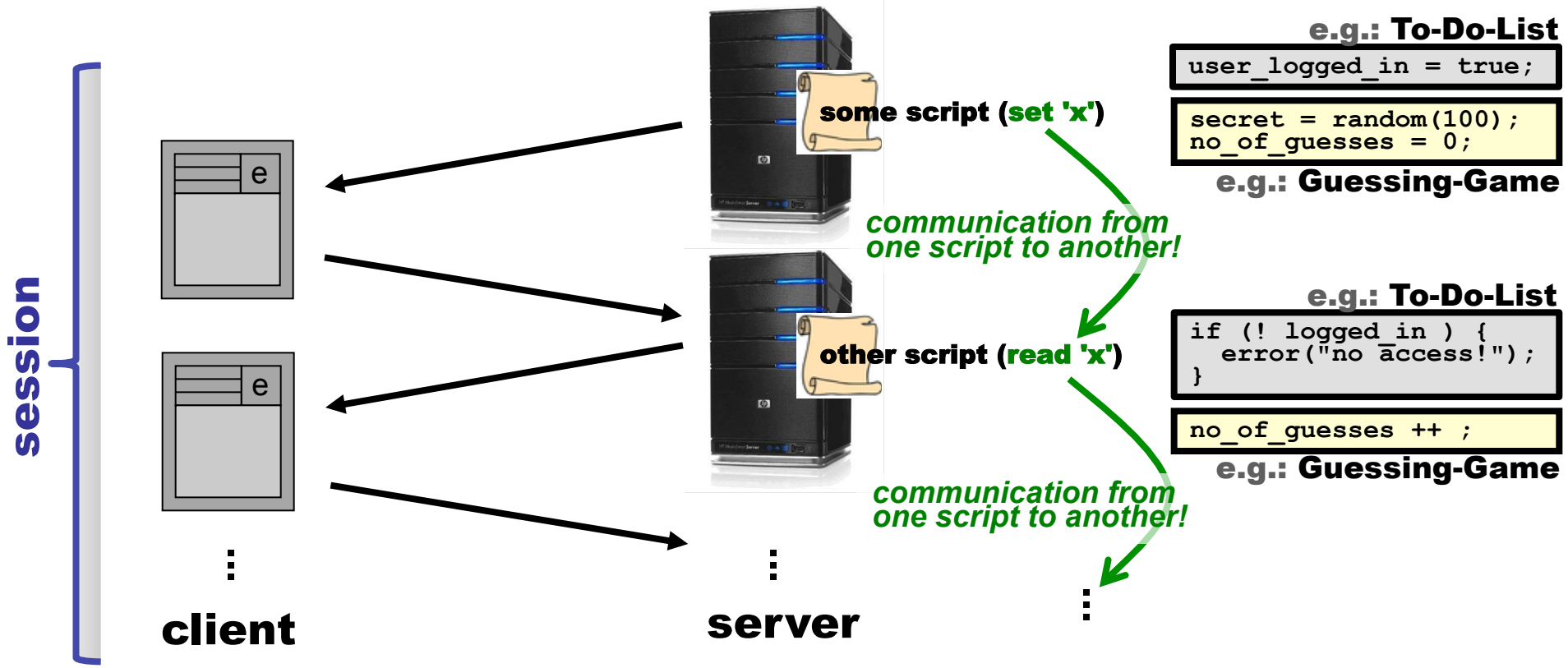
Solution: simply re-check password every single time!

... but then we'd also have to ! ...:

embed password (as 'hidden' input or extra "?" argument) **every single time!**

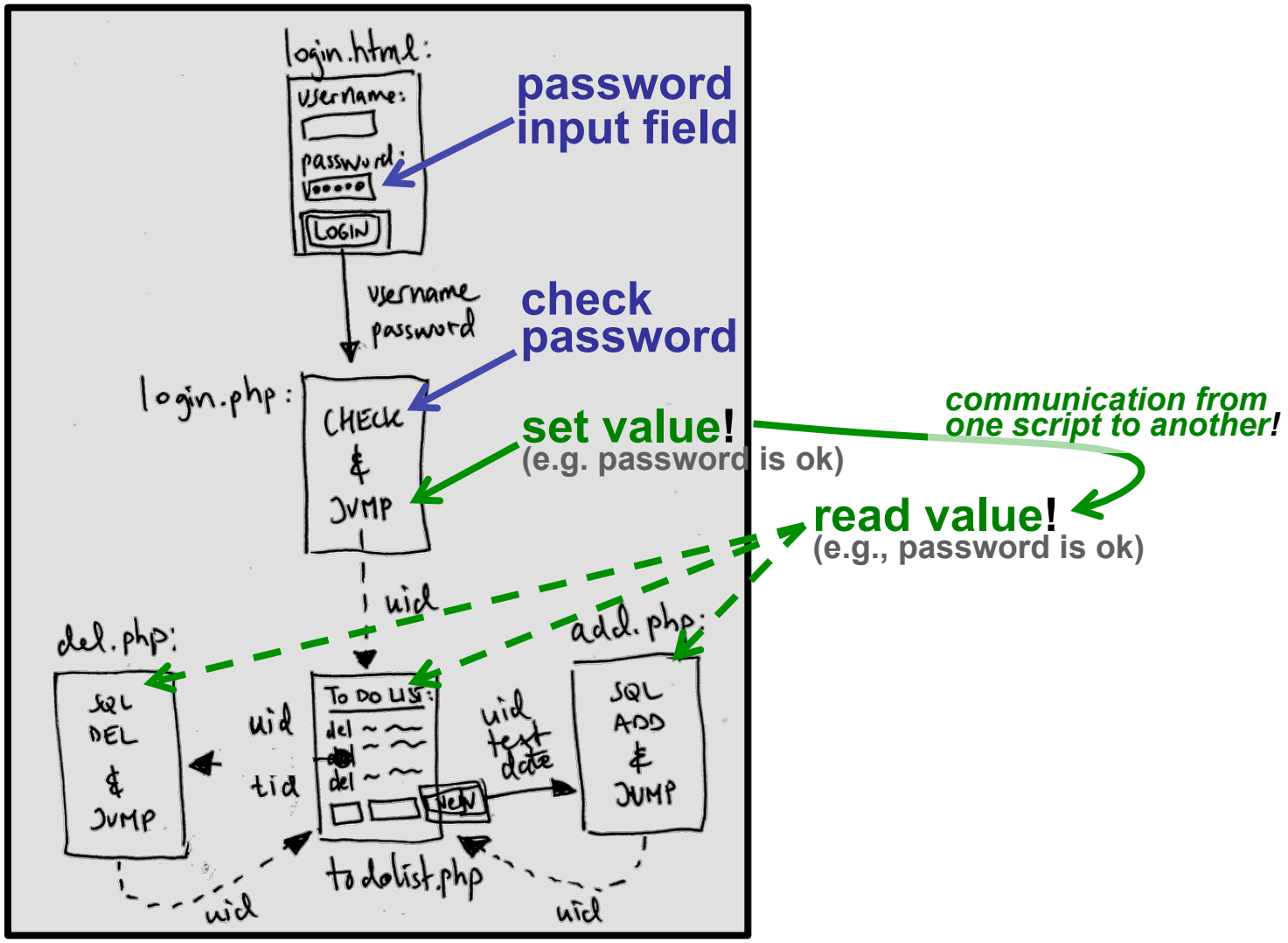
Session State

- Actually an instance of a more general issue:
  - We would like certain data to persist across ***several client-server interactions*** (known as a ***session***):



Session State

- Recall To-Do-List:



Three Types of State

- **Temporary State:**
  - Data local to one script
  - (i.e., PHP variables)

```
<?php
  $x = 42 ;
  echo $x ;
?>
```

- **Persistent State:**
  - Permanent data
  - (i.e., data we put in the database)

- **Session State:**
  - Data across many client-server interactions in a Web Service
    (use tons and tons of "hidden" fields or ...)

"Cookies":

Cookies in One Slide

- Example:

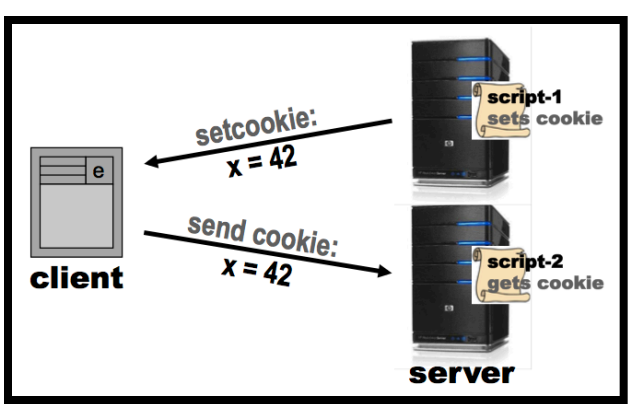
name

value

setcookie.php

```
<html>
  <body>
    <?php  setcookie("x", "42");  ?>
    Click
    <a href="getcookie.php">here</a>
    to see the cookie.
  </body>
</html>
```

Click here to see cookie



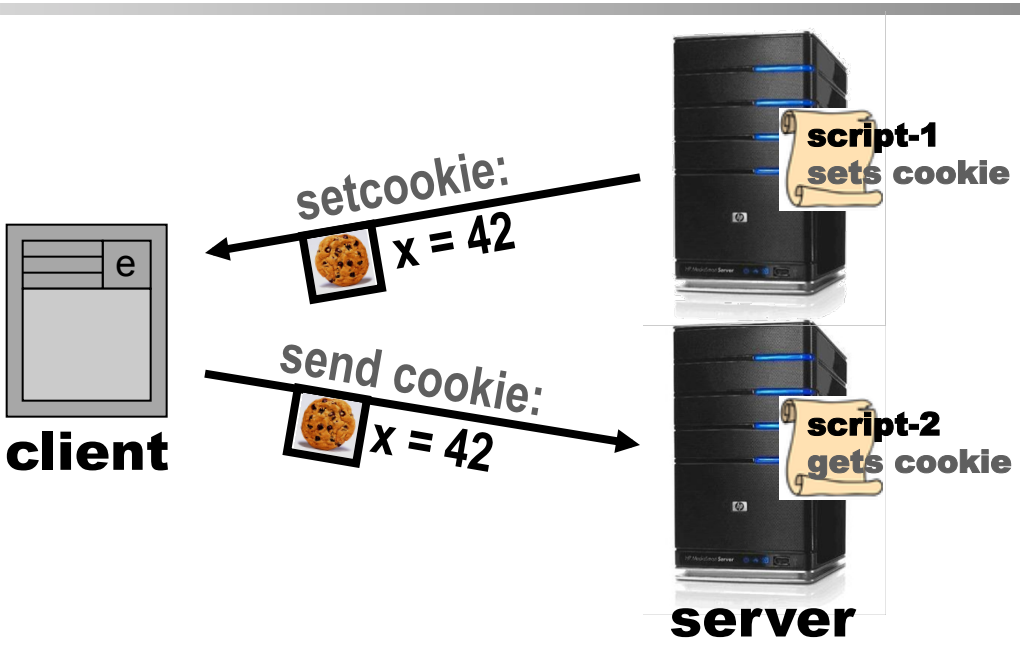

```
<html>
  <body>
    Cookie <b>x</b> has the value:
    <?php
      $v = $_COOKIE['x'] ;
      echo "<b>$v</b>" ;
    ?>
  </body>
</html>
```

reading value of cookie named 'x'

Cookie **x** has value: **42**

getcookie.php

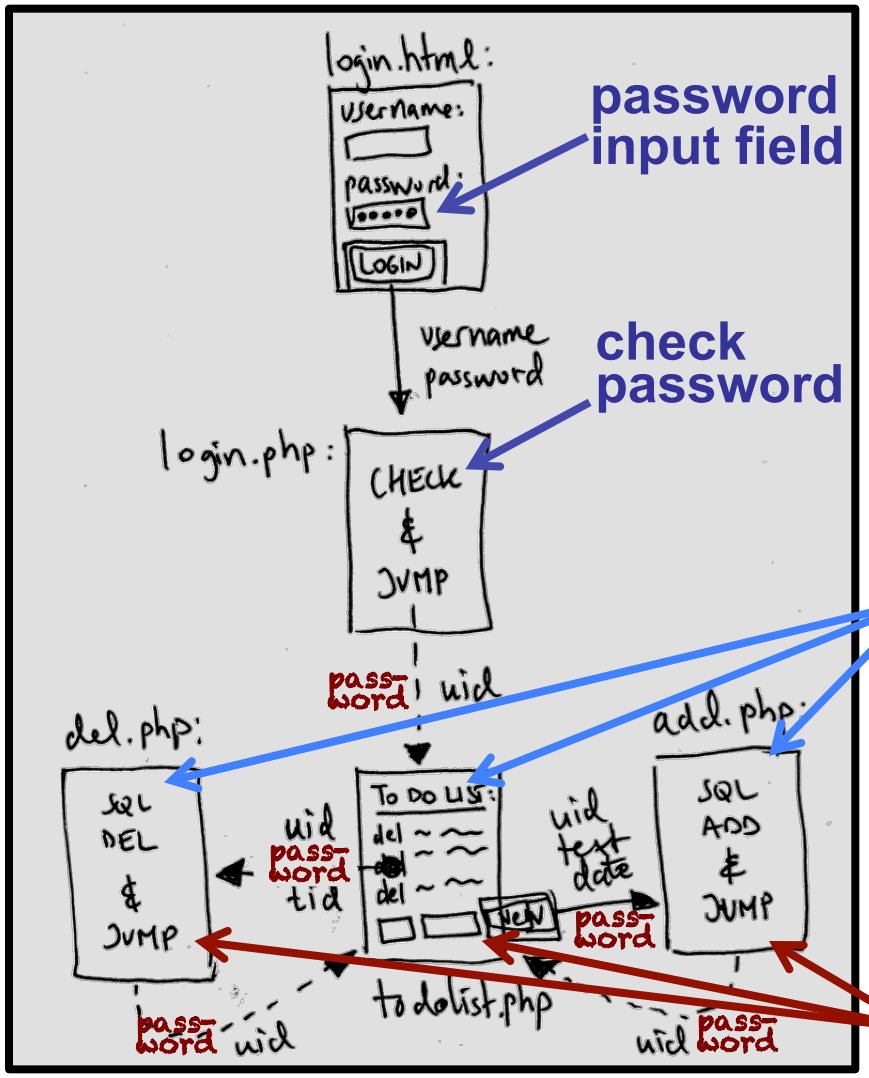
Limitations of Cookies



- Size limits (4000 chars in most browsers)
- Browsers only store a limited # of cookies
- They can be intercepted (eavesdropped)
- …

User Authentication (log in)

- Recall To-Do-List:



Danger: insecure !
(a hacker can "bypass" login by "jumping" directly to todolist.php)

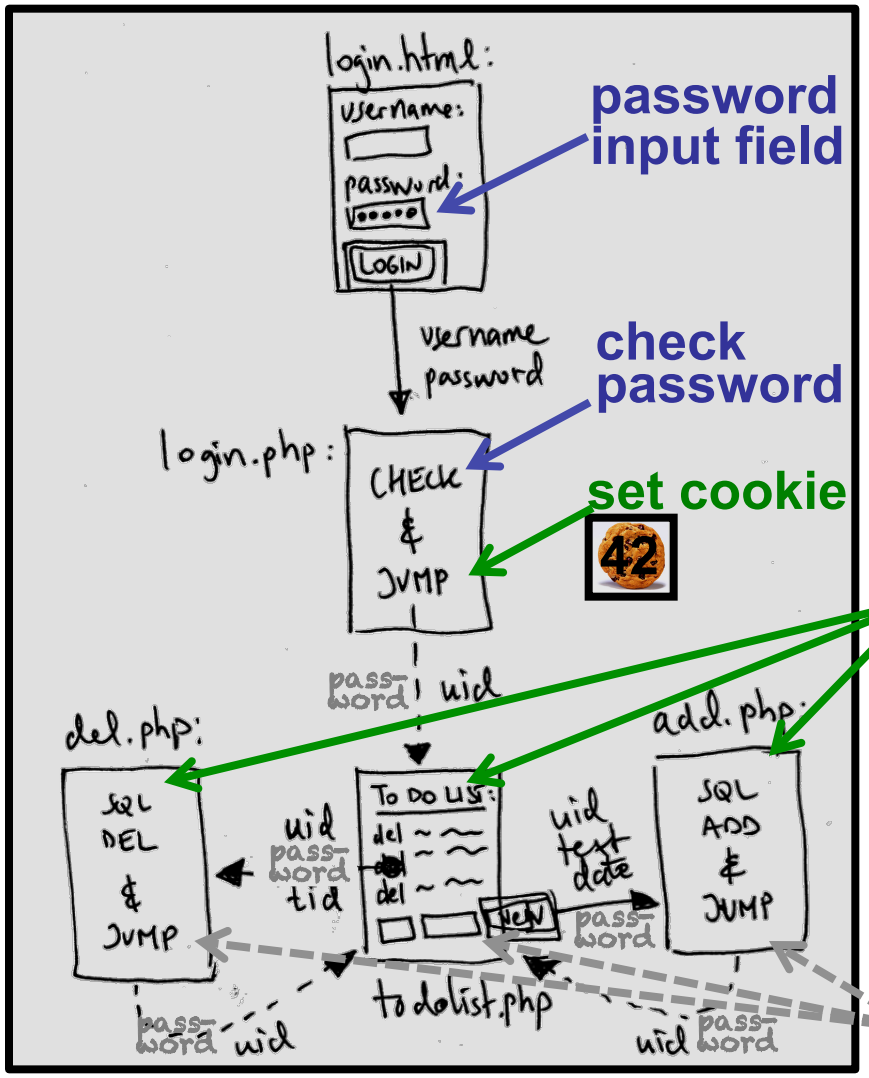
Solution: simply re-check password every single time!

... but then we'd also have to ! ...:

embed password (as 'hidden' input or extra "?" argument) **every single time!**

Authentication /w Cookies

- Recall To-Do-List:



Danger: insecure !
(a hacker can "bypass" login by "jumping" directly to todolist.php)

check cookie
42

Brower will auto'ly transmit Cookies every time for us!

Exercise on Cookies

- **script-1.html:**
  - Enter password and submit to 'script-2.php' (below)
- **script-2.php:**
  - Validate password (e.g.: "12345")
  - Set cookie (e.g.,: password_checked = "ok")
  - Make link to 'script-3.php' (below)
- **script-3.php:**
  - Read cookie
  - Check cookie: if (password_checked != "ok") { error(...); }

Sessions (home made)

- Now we can make ***"home made" sessions:***

```
if ( !isset($_COOKIE['sid']) ) { // 'sid' for 'session identifier'
    $sid = random(100000000) ;   // big random number (hard to guess)!
    setcookie("sid", $sid) ;
} else {
    $sid = $_COOKIE['sid'] ;
}
```

session_data:

sid	data
318381917	some-data...
723124842	other-data...
433102938	more-data...

- ***Write session data:***

```
mysql_query("INSERT INTO session_data (sid, data)
             VALUES ('$sid',' $data');");
```

- ***Read session data:***

```
$rows = mysql_query("SELECT * FROM session_data WHERE sid = '$sid';");
$row = mysql_fetch_array($rows);
$data = $row['data'] ;
```

- **Good news**: sessions are ***"built in"*** in PHP !

PHP Sessions

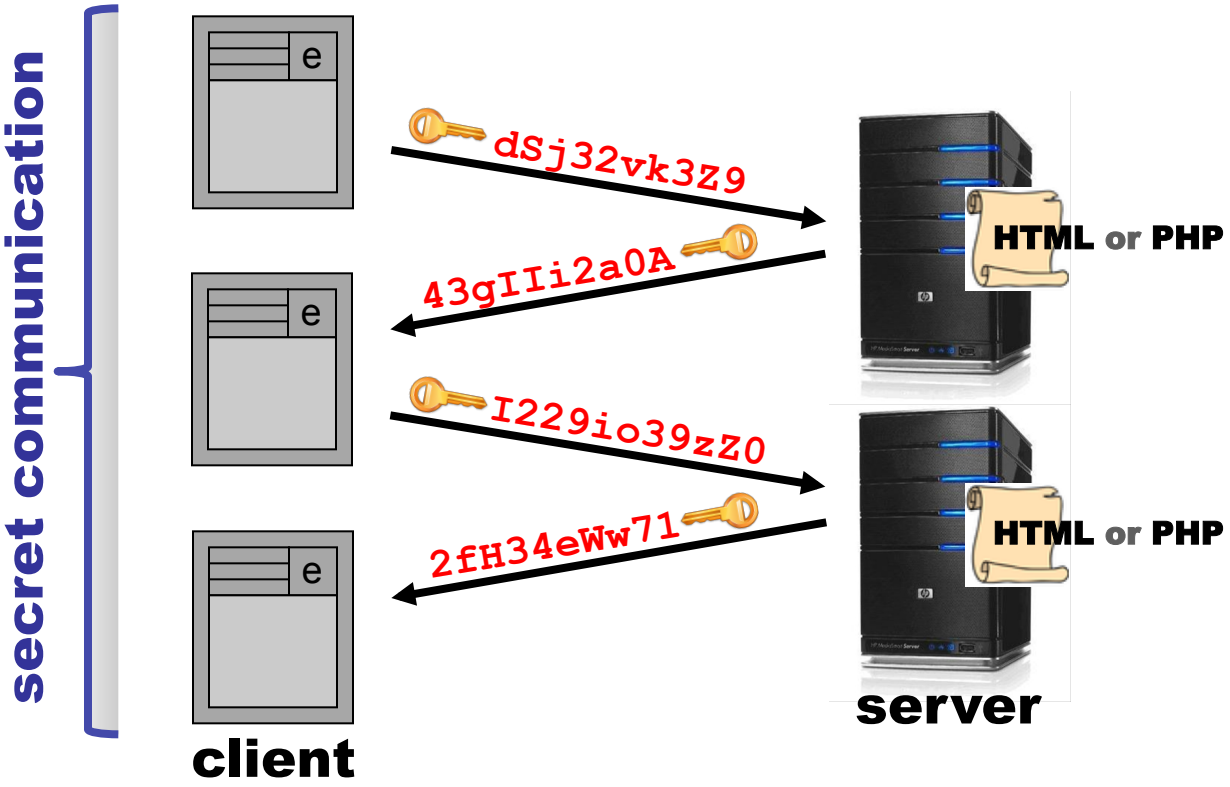
- ***Initialize session:***
  - ```
    session_start();    // uses Cookies much like in
                        // our "home made" sessions!
    ```
- ***Write session data:***
  - ```
    $_SESSION['x'] = $data ;  // write session data
    ```
- ***Read session data:***
  - ```
    $data = $_SESSION['x'] ;   // read session data
    ```
- ***Close session:***
  - ```
    $_SESSION = array() ;      // this saves memory!
    session_destroy();
    ```

Exercise on PHP Sessions

- **script-1.html:**
  - Enter password and submit to 'script-2.php' (below)
- **script-2.php:**
  - Start session
  - Validate password (e.g.: "12345")
  - Set session data (e.g.,: password_checked = true)
  - Make link to 'script-3.php' (below)
- **script-3.php:**
  - Read session data
  - Check session data: if (!password_checked) { error(...); }
  - Destroy session

Encrypted Communication

- **HTTPS** (Secure HTTP) uses **SSL** encryption:



- Just replace '`http`' with '`https`' in all URLs :-)

Agenda

- **Advanced topics:**
  - **Cookies**
  - **Sessions**
  - **User Authentication**
  - **Encrypted Communication**
- **Web Service: Quiz**
- **A11: Last Year's Exam** (exam training)

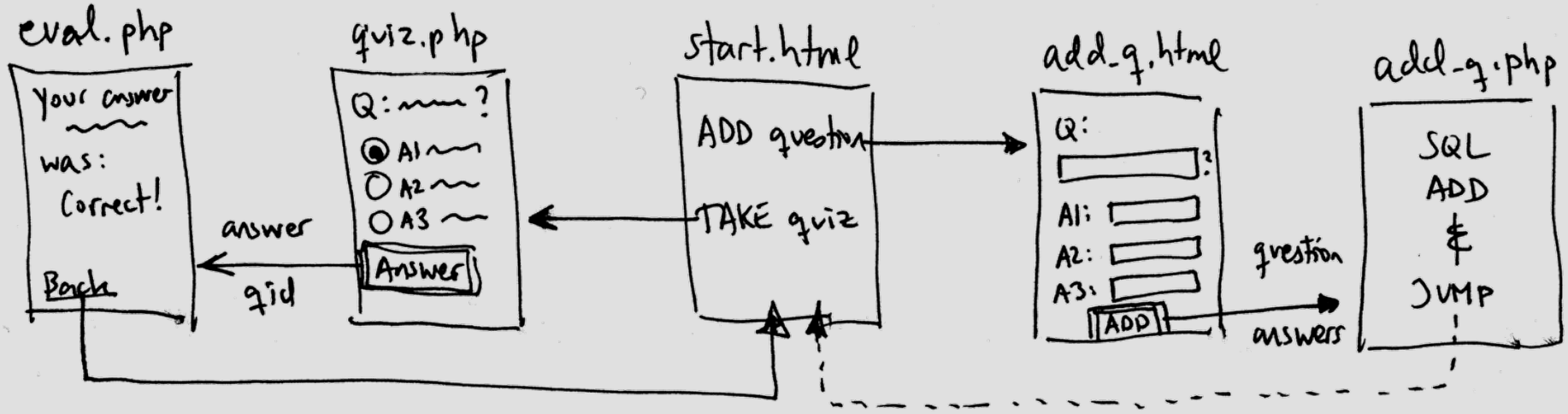
Quiz Service

Carry out the four web service steps:

- **3) site map**
- **1) data model**
- **2) database transactions**
- **4) "just" program it all (in PHP+SQL)**

Quiz Service

- 3) Site map:



Web Service: Quiz

```
CREATE TABLE questions (
  qid INT PRIMARY KEY AUTO_INCREMENT,
  question VARCHAR(100) NOT NULL,
  answer VARCHAR(50) NOT NULL,
  wrong1 VARCHAR(50) NOT NULL,
  wrong2 VARCHAR(50) NOT NULL
);
```

- 1) Data Model:

questions:

qid	question	answer	wrong1	wrong2
1	What is the average rainfall in Amazon basin?	2000 mm per year	200 mm per year	20000 mm per year
2	Who won the EURO 92?	Denmark	Germany	France

AUTO

- 2) Data Transactions:

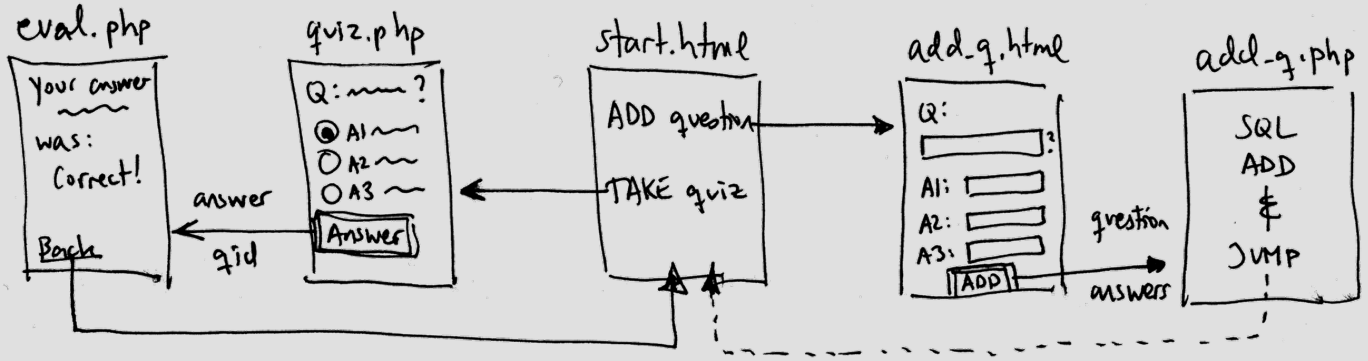
Add question:

```
INSERT INTO questions (question, answer, wrong1, wrong2)
VALUES ('Who won EURO92?', 'Denmark', 'Germany', 'France');
```

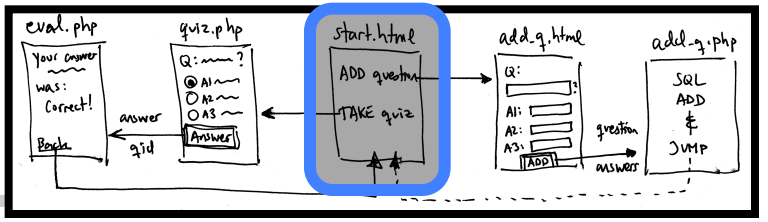
Select questions:

```
SELECT * FROM questions ;
```

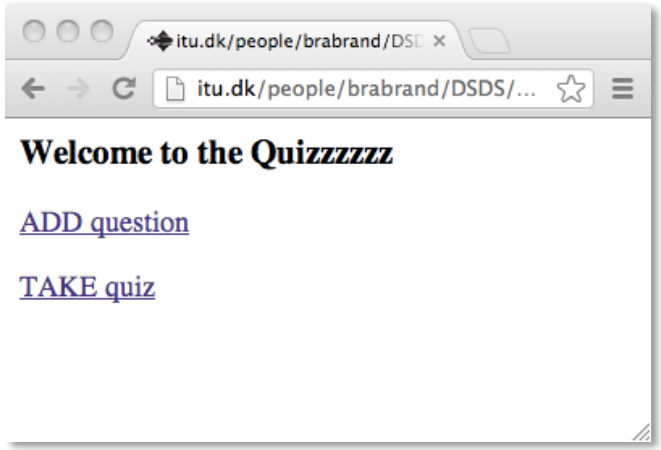
- 3) Sitemap:



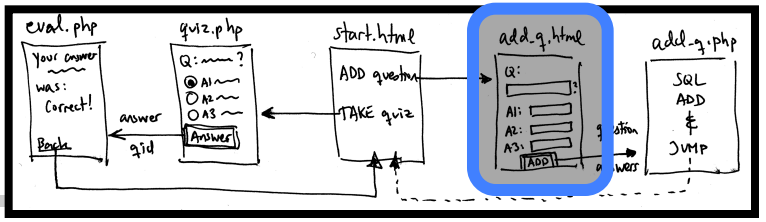
start.html



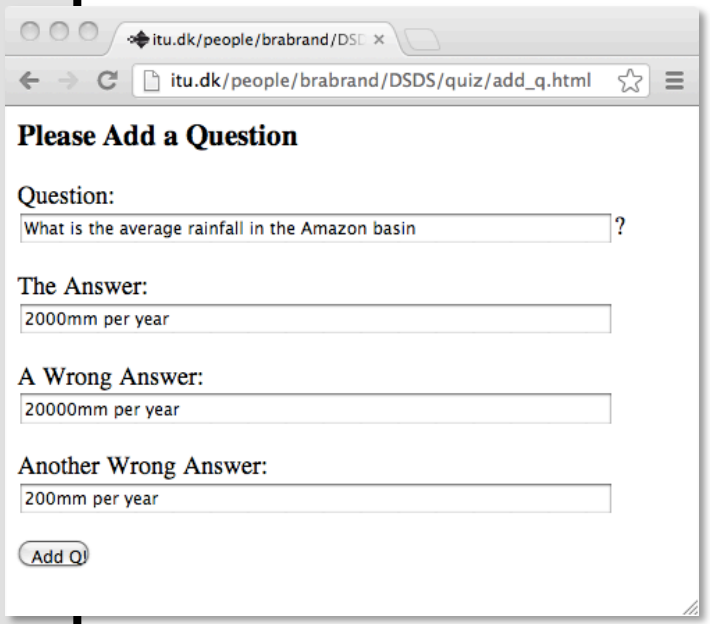

```
<html>
  <body>
    <h3>Welcome to the Quizzzzzz</h3>

    <a href="add_q.html">ADD question</a>
    <p/>
    <a href="quiz.php">TAKE quiz</a>

  </body>
</html>
```



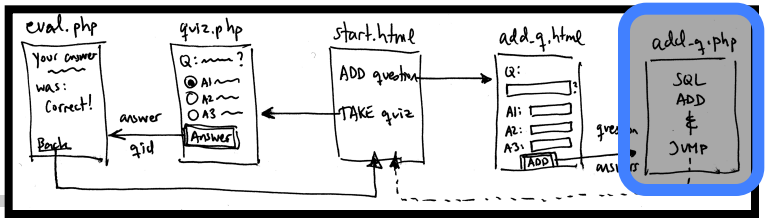
add_q.html




```
<html>
  <body>
    <h3>Please Add a Question</h3>

    <form action="add_q.php">
      Question:<br/>
      <input type="text" size="80" name="question"/>?
      <p/>
      The Answer:</br>
      <input type="text" size="80" name="answer"/>
      <p/>
      A Wrong Answer:</br>
      <input type="text" size="80" name="wrong1"/>
      <p/>
      Another Wrong Answer:</br>
      <input type="text" size="80" name="wrong2"/>
      <p/>
      <input type="submit" value="Add Q!"/>

    </form>

  </body>
</html>
```



add_q.php



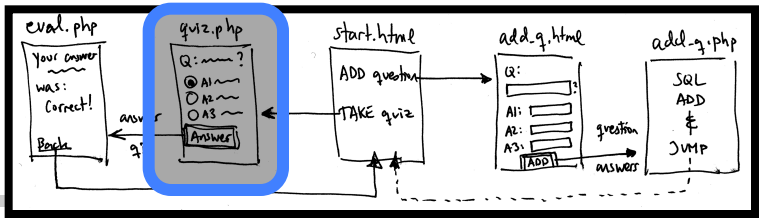

```php
<?php

include("fn_mydb_connect.php");
include("fn_input_validation.php");

mydb_connect();

$question = $_REQUEST['question'] ;
$answer = $_REQUEST['answer'] ;
$wrong1 = $_REQUEST['wrong1'] ;
$wrong2 = $_REQUEST['wrong2'] ;

chk_text($question);
chk_text($answer);
chk_text($wrong1);
chk_text($wrong2);

mysql_query("INSERT INTO questions (question, answer, wrong1, wrong2)
             VALUES ('$question', '$answer', '$wrong1', '$wrong2');");

header("Location: start.html");
mysql_close();

?>
```

SQL INSERT

&

JUMP

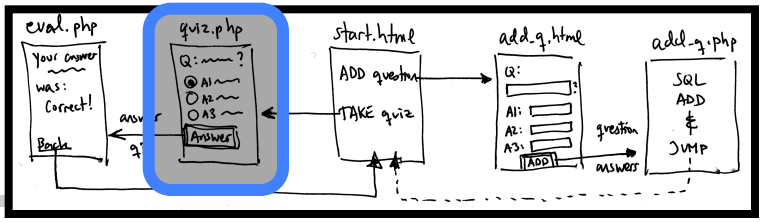
quiz.php (I/II)




```
<html><body>

<?php

include("fn_mydb_connect.php");

mydb_connect();

$rows = mysql_query( "SELECT * FROM questions ;" );
$count = mysql_num_rows($rows) ; // gives the # rows in select result

$r = rand(1, $count); // pick a random (row) number
for ($i = 0; $i < $r; $i++) { // go get the r^th row (via a for loop)
  $row = mysql_fetch_array($rows);
}

$question = $row['question'];
$qid = $row['qid'];
$answers[0] = $row['answer'];
$answers[1] = $row['wrong1'];
$answers[2] = $row['wrong2'];

shuffle($answers);
```

(... continues ...)

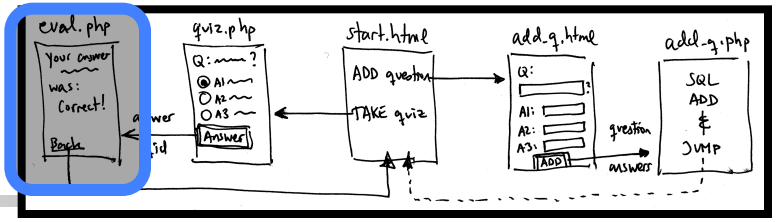
quiz.php (II/II)



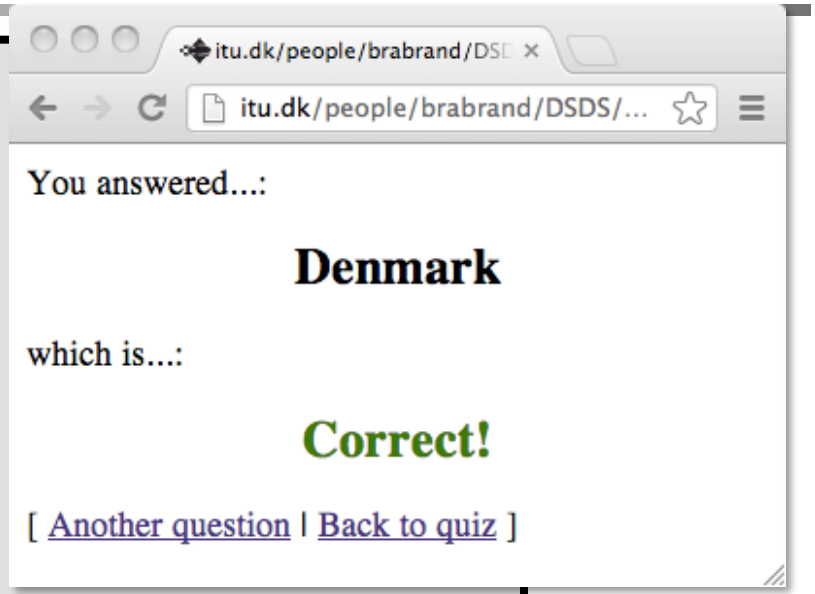
(... continued ...)

```
echo "The question is: <b>$question</b>?" ;

echo "<form action='eval.php'>
        <input type='hidden' name='qid' value='$qid'/>
        <input type='radio' name='answer' value='$answers[0]'/> $answers[0]
        <input type='radio' name='answer' value='$answers[1]'/> $answers[1]
        <input type='radio' name='answer' value='$answers[2]'/> $answers[2]
        <p/>
        <input type='submit' value='Done!'/>
      </form>" ;

mysql_close();

?>

</body></html>
```

eval.php (I/II)

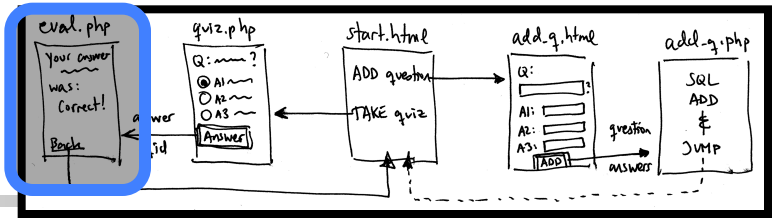



```
<html><body>

<?php

include("fn_mydb_connect.php");

mydb_connect();

$answer = $_REQUEST['answer'];
$qid = $_REQUEST['qid'];
chk_text($answer);
chk_heltal($qid);

$rows = mysql_query("SELECT * FROM questions WHERE qid = '$qid';");
$row = mysql_fetch_array($rows);

if ($row == NULL) {
  error("No such question!!!");
}
$correct_answer = $row['answer'];
```



(... continues ...)

eval.php (II/II)



(... continued ...)

```
echo "You answered...:
      <p align='center'><font size='+2'><b>$answer</b></font></p>
      which is...:" ;

if ($answer == $correct_answer) {
  echo "<p align='center'>
        <font size='+2' color='green'><b>Correct!</b></font></p>" ;
} else {
  echo "<p align='center'>
        <font size='+2' color='red'><b>Incorrect!</b></font></p>" ;
  echo "The correct answer is...:
        <p align='center'><font size='+2'><b>$correct_answer</b></font></p>" ;
}

mysql_close();

?>

<p/>
[ <a href="quiz.php">Quiz again</a> | <a href="start.html">Back to quiz</a> ]
</body></html>
```

Agenda

- **Advanced topics:**
  - **Cookies**
  - **Sessions**
  - **User Authentication**
  - **Encrypted Communication**
- **Web Service: Quiz**
- **A11: Last Year's Exam** (exam training)

Any Questions?

(Have a nice weekend)