ACTION TODAY

a) Add to your existing web site a page where we upload 2 files (same type) and the system concatenate the 2 files together (see PHP function file_put_contents).

Ex.:

```
$d2=fopen($datafile2,"r"); //open the file to be added in read mode
file_put_contents($datafile1,$d2,FILE_APPEND);//concatenate d2 to datafile1
```

b) Add the password checking to the basic login script investigated during the lecture. (use the database example at the end of this document).

c) Use an encryption method for the password. Remember that, in any case, all the parameters have to be JavaScript checked before sending to the server.

d) This is not enough to protect the private part of the web site. Add a cookie to check that the client has already logged in. (see PHP function **setcookie(name,value,dateexpire)**). Modify all the scripts accordingly.

Ex.:

```
      $date = time() + 3600; //1h session
      setcookie("yourname", $_POST['username'], $date); //username coming from
the HTML form
```

e) Why cookies are not a good option to do the job? Think about it.

f) 2/3 words about Cross Site Scripting (XSS) if we have enough time.

g) That's it for today ;-)

Database + table + config file

```
CREATE DATABASE `masterbio` DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;
CREATE TABLE `masterbio`.`users` (
`id` MEDIUMINT NOT NULL AUTO_INCREMENT PRIMARY KEY ,
`username` VARCHAR( 60 ) CHARACTER SET utf8 COLLATE utf8_unicode_ci NOT NULL ,
`password` VARCHAR( 60 ) CHARACTER SET utf8 COLLATE utf8_unicode_ci NOT NULL
) ENGINE = MYISAM ;
```

CONFIG.PHP

```
//it is assumed these are the correct values;-)
$host="localhost";
$login="root";
$passwd="yourpasswd"; or "" if no password
$dbname="masterbio";
$table="users";
?>
```

Simple login script LOGIN.PHP

```
<?php
include("./config.php");
if (isset($_POST['submit'])) {
$connection=mysql_connect($host, $login, $passwd) or die("impossible de se connecter");
mysql_select_db($dbname) or die("impossible d'aller sur la bd");

//RECHERCHE DU USER
$query="SELECT * FROM ".$table."  WHERE username = '".$_POST['username']."'";
$check = mysql_query($query) or die("essayer plus tard!");
//si le client n'est pas ds la bd il doit s'enregistrer
$numberOfRow = mysql_num_rows($check);
if ($numberOfRow == 0) {//il n'y a aucune ligne correspondante
die("Vous n'existez pas. Cliquer <a href=register.php>ici</a> pour vous enregistrer");
}
//on doit maintenant checker le password maison le fait pas pour l'instant
//tout est OK - on ferme la connection et on envoie le client sur la page member.php
mysql_close($connection);
$header="location:member.php”;//we go to the member page
header($header);
}
else
{// le client n'est pas loge -
//on envoie le formulaire
?>
<form action="<?php echo $_SERVER['PHP_SELF']?>" method="post">
<table border="0">
<tr><td><h1>Login form</h1></td></tr>
<tr><td colspan="0">Username:</td><td>
<input type="text" name="username" maxlength="20">
</td></tr>
<tr><td align="right">
<input type="submit" name="submit" value="Login">
</td></tr>
</table>
</form>
</body>
<?php } ?>
```