Tasks to Solve During Seminar 3

Internet Applications, ID1354

Write a document with your answers to the following tasks, and upload it to Bilda at the end of the seminar. The format of the document is not important. Only one document per group is required, each group member uploads the same document.

Mandatory Task

All members of the group shall, in turn, explain and motivate their program to the other group members. Write a brief summary of differences, and comment on advantages and disadvantages of the different solutions. Do not write about minor layout differences.

Optional Tasks

Solve as many of these tasks as time allows, and write your solutions in the same document as the mandatory task. If the solution is a piece of code, just paste the code in the document, without bothering about figures or formatting. The tasks may be solved in any order, you do not have to start from task one.

Task 1, Frameworks

a) It is almost always the case that a http request is received by one php file, which then includes another file containing the next view (otherwise the code will be terribly messy). This means that the URL does not match the path to the file with the view. If we are using a framework with routing functionality, the URL does not even match the path of the file handling the http request. *Make sure you understand why!*

Now, suppose a browser has made an HTTP request to **`http://www.myserver.se/abc/def`**. The server framework maps this URL to the file **`classes/ghi.php`**, which includes **`views/jkl.html`**. The view that is now displayed in the browser is the HTML code in **`views/jkl.html`**.

1) Which URL is now displayed in the browser's address field?

2) The layout of **`views/jkl.html`** is specified in **`resources/css/mno.css`**. **`jkl.html`** contains a link to **`mno.css`**, which path shall that link have?

b) Is there any feature you miss in the id1354-fw framework? Maybe handling request or application lifetime variables the same way session variables are handled? Or the possibility to include data in a view without writing php code? Or possibility to include fragments like header and footer without writing php? Try to find out how some missing feature could be implemented. You do not have time to implement it in code, just try to understand how it could be done. Ask the teacher for hints if you wish.

c) Try to understand how some existing functionality in the framework is implemented, for example session handling, routing or including views. You can try to figure out a possible implementation on your own or read the framework's source code. Ask the teacher for hints if you wish.

Task 2, Security

Try to perform an attack on one of your sites. You can, for example, try to impersonate another user, with one of the strategies below.

1. Perform a session fixation attack as suggested on slide 47 of the presentation from lecture 9. That is, create a web page that sets the PHPSESSID cookie, let the attacked user visit that page and then log in to tasty recipes. Finally, use the preset session id to impersonate that user.

2. Steal the session of a logged in user, by reading that user's PHPSESSID cookie and setting your own cookie to that value. You can try to get the logged in user's cookie with an XSS attack, as suggested on slide 38 of the presentation from lecture 9.

3. If someone in the group has a packet sniffer tool (that can monitor all network traffic), use it to read the user's password or PHPSESSID cookie.

4. If you fail to steal the session, you can still check the outcome of a successful attack by just reading the PHPSESSID cookie on the logged in user's computer.