# Web & System Security – Homework 08

## Problem 1

Please refer to the source file session\_example\_loggedin.html.

## Problem 2

Both pages encode the strings as follows:

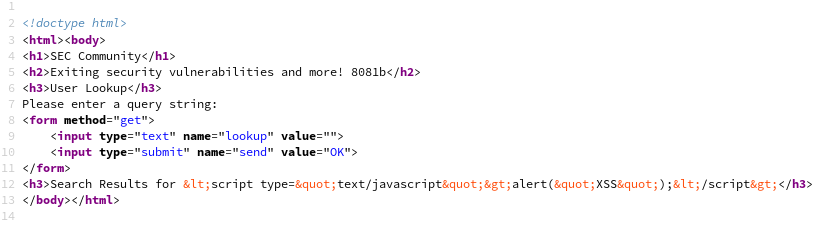
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Aß | Bü | C+ | D& | E% | F. |
| Aß | Bü | C%2B | D%26 | E%25 | F. |

We can use an input like

<script type="text/javascript">alert("XSS");</script>

to produce a different output. For xss-search-1a.py we receive:



and for xss-search-1b.py:

The second page uses the escape function to convert the characters <,> and “ to &lt; , &gt; and &quot; such that the input is interpreted as a string, whereas the first page executes the script and therefore poses a security risk.

## Problem 3

## Problem 4

Please refer to the file problem04.sql.