

Web-Oriented Programming
CS215 Winter 2011 – Final (D. Hepting)
April 13, 2011
CL435 – 14:00-17:00

PLEASE READ: There are 90 marks available (and 180 minutes in which to complete the exam). The exam is closed book. You have been given 3 exam booklets: 2 to hand in and the other (optionally) for rough work (please return it if it is unused). Answer Part 1 in the 1st booklet, and Part 2 in the 2nd booklet. **Think quality over quantity (don't fill all available space!)** Questions about exam questions will not be answered during the exam – note your assumptions in your answers.

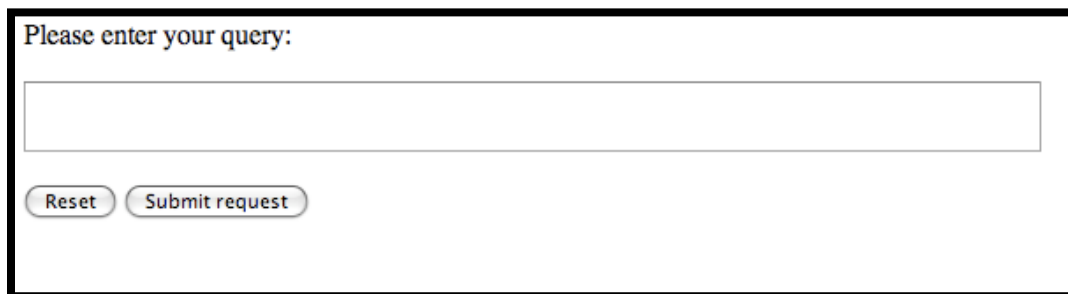
Part 1 (answer 15/18; 3 marks each = 45 total marks). For each question below, do: a) answer the question itself (1 mark, 1-2 sentences); b) identify the significance (1 mark, 1-2 sentences); and c) provide an example (1 mark, 1-2 sentences).

1. What is “====” in JavaScript? How is it different from “===”?
2. What is DOM?
3. Why is server-side code useful?
4. What are 2 of the main http methods?
5. What are coupling and cohesion?
6. Why should one sanitize inputs?
7. What is a 3-tiered web architecture?
8. What inline style sheets?
9. Why is it important to validate XHTML (and other code)?
10. Is alert() a good idea in JavaScript?
11. What does onblur() permit?
12. Why are schemas useful for XML?
13. How can regular expressions in be useful in JavaScript?
14. Why might you use XML?
15. Why are normal forms important in database design?
16. What are cookies?
17. What is the Pseudo-code Programming Process?
18. What is XSLT?

Part 2 (answer all 5; 9 marks each = 45 total).

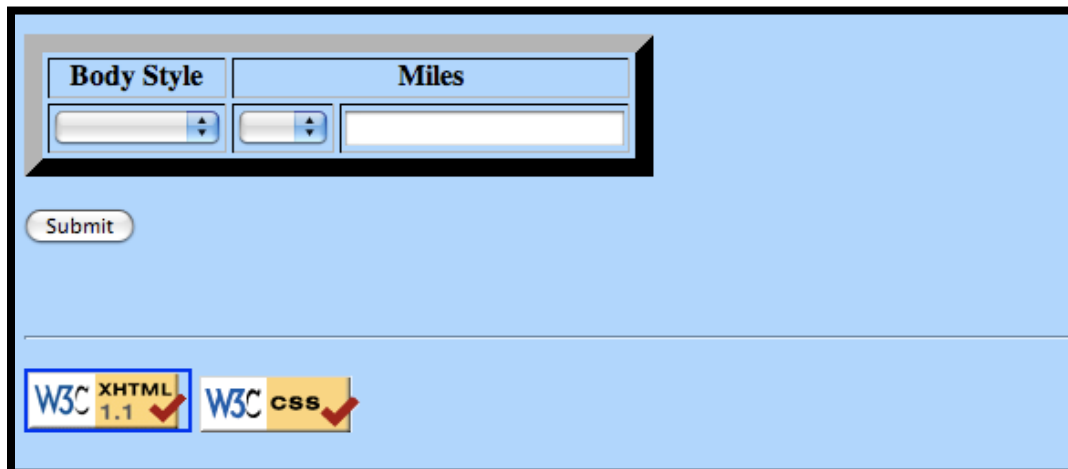
1. How would you use Ajax and PHP to create a dynamic select list from which a user can choose (as we discussed in class)? Identify how the different technologies would work together and provide pseudo-code for each (6 marks). Why is Ajax appropriate for this functionality? How would this functionality be different without Ajax? (3 marks)

2. Why can PHP short tags cause problems? (2 marks) What is a way to work around these problems? (2 marks). How is it possible to debug PHP (and web development in general) depending on whether the server is setup with security in mind? (5 marks)
3. How would you use sessions to ensure that the user who is requesting access to a privileged area of website actually has the needed authority (5 marks)? What is a session fixation attack and what are some ways to protect against it (4 marks)?
4. What are the vulnerabilities possible in allowing a user to enter an SQL query as shown in the first screenshot below (4 marks)? Write some pseudo-cfcode and describe how the second screenshot could provide a more secure (and usable) interface (5 marks).





Please enter your query:

This screenshot shows a simple web form with a text input field and two buttons: 'Reset' and 'Submit request'.



Body Style **Miles**

This screenshot shows a more complex form with two dropdown menus labeled 'Body Style' and 'Miles', and a 'Submit' button. At the bottom, there are two logos: 'W3C XHTML 1.1' and 'W3C CSS', both with checkmarks.

5. Identify 4 issues with the following code (4 marks) and describe improvements for each (4 marks). Why should the code we write be readable and understandable by someone else (1 mark)?

```
void HandleStuff(CORP_DATA & inputRec, int crntQtr, EMP_DATA
empRec,
    double &estimRevenue, double ytdRevenue, int screenX, int
screenY,
    COLOR_TYPE &newColor, COLOR_TYPE &prevColor, StatusType
&status,
    int expenseType)
{
int i;
for (i = 0; i < 100; i++ ) {
    inputRec.revenue[i] = 0;
    inputRec.expense[i] = corpExpense[ crntQtr ][i];
}
UpdateCorpDatabase( empRec );
estimRevenue = ytdRevenue * 4.0 / (double) crntQtr;
newColor = prevColor;
status = SUCCESS;
if (expenseType == 1) {
    for (i = 0; i < 12; i++ )
        profit[i] = revenue[i] - expense.type1[i];
}
else if (expenseType == 2) {
    profit[i] = revenue[i] - expense.type2[i];
}
else if (expenseType == 3) {
    profit[i] = revenue[i] - expense.type3[i];
}
```