For this assignment you will be finding vulnerabilities in another group’s Homework 2. Your deliverable for this homework will be a written document, as well as any other files to carry out the exploits that you found. To do this homework, you should do the following:

1. You and your partner must find a homework 2 group which neither of you was a part of. You will exchange homework 2s with this group, and find vulnerabilities in their code (while they find vulnerabilities in yours).

2. You and your partner should review/analyze the other group’s code. You should write an initial section in your report that details your analysis: what parts do you think are vulnerable? Which parts were done securely? What kinds of exploits do you think you might be able to carry out? What kinds do you think it is immune to? Why?

3. Construct exploits against the code. For each possible avenue of attack that you think might exist, construct an example attack which demonstrates the exploit. In particular, you should run their code, carry out the attack, and make sure you see the expected results. Detail these in a second section of your report.

4. Meet up with the group whose code you have analyzed/exploited. Demonstrate your attacks, and review their code with them. During this review, you should explain your findings, and ask any other questions you might have. If this review gives you ideas for other attacks, you should construct them, write about them, and show the other group.

5. The other group will also show you the vulnerabilities that they found in your code. You should write a third section of your report detailing what you learned about the security of your code, and how you could have fixed it.

Your deliverable for this assignment is the writeup described above. If any of your attacks have files to carry them out (javascript code, html files,....) you should submit them along with this writeup. This writeup MUST be in pdf format (No Word documents). Any supplemental files should be in their natural format (e.g., plain text for source code).

It is possible (though HIGHLY unlikely) that the code you are analyzing is completely free of security flaws. If you believe this is the case, you should TRIPLE check (and think about all the attack types we discussed) , and if you are still convinced it is flawless, you should write up an justification that will convince both me and your TA that there are NO security problems.

As one final note: you are expected to carry out this assignment responsibly. You should run the target code on one of your own servers, and only attack it there. You should not carry out any attack which causes negative impacts on other systems (e.g., do not carry out a DDOS attack which harms network performance). If you suspect you can inject code, inject something harmless as proof-of-concept. If in doubt, please ask.