Problem 1 (15 points)
Consider data that is input to a Web form. Such data is often transferred to the server by including it in a URL. Suppose the input is validated on the client. For example, suppose the following order has been checked by the client:

http://www.things.com/orders/\texttt{final}&\texttt{custID=112}&\texttt{num=55}&\texttt{qty=20}&\texttt{price=10}&\texttt{shipping=5}&\texttt{total=205}

This URL is interpreted to mean that the customer with ID number 112 has ordered 20 of item number 55, at a cost of $10 each, which, with $5 shipping, gives a total cost of $205. Q

Show three ways in which a client named Mallory can cheat the server.

Problem 2 (30 points).
Find and point the buffer overflow in the code below. Illustrate an attack using the stack image we covered in class. Show how the buffer overflow can be eliminated.

**Algorithm 1** Code snippet of a vulnerable function.

```c
1. ...
2. char buf[64], in[MAX_SIZE];
3. printf("Enter buffer contents: ");
4. read(0, in, MAX_SIZE - 1);
5. printf("Bytes to copy: ");
6. scanf("\%d", &bytes);
7. memcpy(buf, in, bytes);
8. ...
```

Problem 3 (25 points).
What will the following code print? Why? Identify the line where the vulnerability is. Explain the vulnerability. Show how the vulnerability can be eliminated.

**Algorithm 2** Example vulnerability.

```c
1. void called (int foo){
2. if (foo = 1) printf("foo");
3. else printf("bar");
4. }
5. int main (){
6. called(2);
7. return 0;}
```

Problem 4. (30 points) Remember how in the Wannacry ransomware, the malware generates a new public and private key pair $pk_v, pr_v$ for each victim, then stores the private key encrypted with the attacker’s public key $pk_A$, as $E(pk_A, pr_v)$. When the victim pays the ransom, the attacker decrypts the victim’s private key, $pr_v = D(pr_A, E(pk_A, pr_v))$.

(a - 10 points). Describe how the ransomware can perform this operation. There are several possibilities, but just choose one. Specifically, describe where the ransomware would store its private key $pr_A$, and how it can access it to decrypt $E(pk_A, pr_v)$.

(b - 20 points) Show how the approach that you have described for point (a) would make the ransomware or its developer, vulnerable. That is, describe how would an anti-malware tool be able to perhaps disable the ransomware or make progress toward finding out who is the person or organization behind it.