Web Security III

Question 1 ***CSRF++***

Patsy-Bank learned about the CSRF flaw on their site described above. They hired a security consultant who helped them fix it by adding a random CSRF token to the sensitive `/transfer` request. A valid request now looks like:

```
https://patsy-bank.com/transfer?to=bob&amount=10&token=<random>
```

The CSRF token is chosen randomly, separately for each user.

Not one to give up easily, Mallory starts looking at the welcome page. She loads the following URL in her browser:

```
https://patsy-bank.com/welcome?name=<script>alert("Jackpot!");</script>
```

When this page loaded, Mallory saw an alert pop up that says "Jackpot!". She smiles, knowing she can now force other bank customers to send her money.

(a) What kind of attack is the welcome page vulnerable to? Provide the name of the category of attack.

(b) Mallory plans to use this vulnerability to bypass the CSRF token defense. She'll replace the `alert("Jackpot!");` with some carefully chosen JavaScript. What should her JavaScript do?

(c) `patsy-bank.com` sets `SameSite=strict` for all of its cookies. Does this stop the attack from part (b)? Assume the welcome page does not require a user to be logged in.

(d) Mallory wants to attack Bob, a customer of Patsy-Bank. Name one way that Mallory could try to get Bob to click on a link she constructed.

Question 2 ***Clickjacking***

In this question we'll investigate some of the click-jacking methods that have been used to target smartphone users.

(a) In many smartphone browsers, the address bar containing the page's URL can be hidden when the user scrolls. What types of problems can this cause?

(b) Smartphone users are used to notifications popping up over their browsers as texts and calls arrive. How can attackers use this to their advantage?

(c) QR codes haven't taken off and become ubiquitous like some thought they would. Can you think of any security reasons why this might be the case?

Question 3 ***Web Security Wrap-Up: UI-Based Attacks and Privacy***

(a) **Phishing**

A phishing attacker tries to gain sensitive user information by tricking users into going to a fake version of a website they trust. The attacker might convince the user to go to what *appears* to be their bank and to enter their username and password.

i. What are some ways that attackers try to fool users about the site they are going to? How do they convince people to click on links to sites?

ii. What are some defenses you should employ against phishing?

(b) **Clickjacking**

Smartphone users are used to notifications popping up over their browsers as texts and calls arrive. How can attackers use this to their advantage?

(c) **Web Tracking**

What kind of information do sites gain about you when you visit them? How could a business learn about many of the sites you visit and construct a detailed profile of you based on your web habits?