Instructions. We will break into groups to discuss the following questions. Please think of as many solutions as you can. Be original! Maybe you will come up with something no one has thought of yet. Be prepared to talk about your solutions with the rest of the section.

Question 1 Authentication and Impersonation (20 min)

(a) The hip banking app Monogon claims that its two-factor authentication involving sending a verification text to a user’s smartphone, and a special identification card issued to all of its users, is the answer to all of its authentication problems. What are some problems with this statement?

(b) If a website is compromised with an XSS attack, can you think of ways to prevent the session ID cookie from being sent to the attacker, while preserving its functionality?

(c) Session cookies seem to solve the problem of authentication, but what are some reasons we sometimes still have to re-enter login information on websites?

(d) Who and what plays a part in ensuring that users can authenticate websites? What part does each actor play?

(e) How does protecting user information and privacy play a role in helping them avoid being victims of phishing schemes?
Question 2  
**Cooperative Authentication**  
(20 min)  
Monogon would like its users to be able to use existing credentials with other sites, like Twitter, to request profile information or post tweets for the user, if given permission, of course. To do so, engineers from both companies agree to work together to design an HTTP-based protocol.

(a) An early design suggests that users enter their Twitter credentials on Monogon’s website so that Monogon can attach them to Twitter API requests and have them be authenticated. What are some reasons this design would be scrapped?

(b) Instead, the engineers decide to have Monogon issue a request to `Twitter.com/Monogonauth`. Twitter’s server will check for the user’s session ID cookie, which will be sent along with the request, assuming the user has already logged into Twitter. If the cookie is valid, Twitter’s server will create, store, and return a secret token in its response to the request, which Monogon will use from now on to authenticate its requests to Twitter. Will this work?

(c) Design a protocol Twitter and Monogon could actually use. What kind of data needs to be exchanged? Who needs to store what? How can they exchange that data?

---

Question 3  
**Clickjacking**  
(10 min)  
In this question we’ll investigate some of the click-jacking methods that have been used to target the growing population of 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?