CS490-004 Network Programming
Possible Quiz Questions (Quiz #11)
on November 19th, 2026

The following is a list of possible questions for our quiz on November 19th. Some of the questions will not be asked in the quiz. All the questions that will appear in the quiz will appear exactly as shown below (however, numeric parameters may be changed). The quiz is closed textbook, closed notes and closed neighbors. Note that the questions, which did not appear in this quiz, still may appear in the exams. You will find a solution for these questions during lectures.

#1: In XSS (Cross Site Script) attacks, who prepare CGI program (Perl source code files) used for the attack?

#2: In XSS (Cross Site Script) attacks, where malicious scripts are executed?

#3: In XSS, why don't attackers send malicious CGI forms directly to web clients?

#4: What security weakness in third-party web servers XSS attackers use for performing XSS attacks?

#5: What is the most effective solution for preventing XSS attacks (from the viewpoint of network programming)?

#6: If XSS attacks successfully happen, whose fault are they?

#7: In CSRF (Cross-Site-Request-Forgery) attacks, good websites are used in a different way than XSS attacks use good websites. Explain how the way CSRF use good websites.

#8: What is the key HTML feature CSRF attackers use in performing their CSRF attacks?

#9: How do CSRF attackers manage to let our browsers to grab cookies when CSRF attackers forward their malicious CGI forms to good websites?

#10: If CSRF attacks successfully happen, whose fault are they?

#11: Complete the following table by summarizing the differences between XSS and CRSF:

Major Differences	XSS	CSRF
Who (or what) executes scripts as a part of the attack?		
Who prepare the scripts as a part of the attack?		
What malicious activities do the attackers aim for?		

#12: Which of XSS attacks and CSRF are harder to prevent? Why?

(first research question)

#13: How are "session hijacking attacks" performed (what do attackers abuse)?

#14: If "session hijacking attacks" successfully happen, whose fault are they?

#15: How are "session fixation attacks" performed (what do attackers abuse)?

#16: If "session fixation attacks" successfully happen, whose fault are they?

#17: Why did web browser venders adopt "inclusion of session ID" in HTTP FET command-line?

(second research question)

#18: Describe how "HTTP-header-injection attacks" are performed by attackers to hijack your SNS account?

#19: If "HTTP-header-injection attacks" successfully happen, whose fault are they?