CSE 345/545: Foundations to Computer Security
END-SEMESTER EXAM (TOTAL OF 70 + 10 POINTS)
Deadline: 48 hrs
Instructions:

- Do your questions individually.
- Make one PDF file for writing your solutions in the format <RollNo>_ENDSEM.pdf
- State your assumptions (if any) in your solutions.
- All the queries must be posted in the classroom. No response will be provided for unreasonable queries.
- **Answer the questions in bullet points. Keep your responses crisp and to the point.**

---

1. [Web Basics and Security Concerns]

   Keep your answers in the requested format. Every question has two parts. In part (a) simply write the code you wrote to perform the XSS attack, (b) Mention the html tag you used or updated to perform the attack. The first one is done for you as an example. You will be awarded marks iff both a and b are correct. **[10]**

   a. Visit https://xss-quiz.int21h.jp and perform an XSS attack to inject the following JavaScript command: alert(document.domain); You can use the hint given on the webpage.
   Write the code you used to perform the attack.
   Solution: <script>alert(document.domain);</script>

   Mention the html code for the component you used or updated to perform the attack.
   Solution: <input type="text" name="p1" size="60" value="">

   Example: The code used is: <script>alert(document.domain);</script> and html code (we have entered the code in the search bar to perform the XSS attack): <input type="text" name="p1" size="60" value="">. You can copy the element code by right clicking on it from the inspect menu. Note that the html code must come from the original webpage, i.e., you should copy the original element even if you have made changes to perform the attack. You don't have to write the keyword "Solution:" in your answers.

b. Visit https://xss-quiz.int21h.jp/stage2.php and perform an XSS attack to inject the following JavaScript command: alert(document.domain); You can use the hint given on the webpage.

   Write the code you used to perform the attack.
   Mention the html code for the component you used or updated to perform the attack.

c. Visit https://xss-quiz.int21h.jp/stage-3.php and perform an XSS attack to inject the following JavaScript command: alert(document.domain); You can use the hint given on the webpage.

   Write the code you used to perform the attack.
   Mention the html code for the component you used or updated to perform the attack.

d. Visit https://xss-quiz.int21h.jp/stage_4.php and perform an XSS attack to inject the following JavaScript command: alert(document.domain); You can use the hint given on the webpage.

   Write the code you used to perform the attack.
   Mention the html code for the component you used or updated to perform the attack.

e. Visit https://xss-quiz.int21h.jp/stage--5.php and perform an XSS attack to inject the following JavaScript command: alert(document.domain); You can use the hint given on the webpage.

   Write the code you used to perform the attack.
   Mention the html code for the component you used or updated to perform the attack.

2. **The principle of least common mechanism** states that mechanisms used to access resources should not be shared.
   The principle of fail-safe defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object.

   A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts.
   a. Discuss how this technique might prevent legitimate users from accessing the system. Why is this action a violation of the principle of least common mechanism? **[5]**

   b. One can argue that this is an example of fail-safe defaults, because by blocking access to an account under attack, the system is defaulting to a known, safe state. Do you agree or disagree with the argument? Justify your answer. **[5]**

3. [Ethics] **[5]**
   Which among the ten commandments of computer ethics are violated in each of the following case :
   a. Your neighbours installed a new wifi connection. You are trying different password breaking techniques to get the password and use it.
   b. Almost all of your friends are using a pirated version of Windows OS and MS Office software. You also do it because you think there's no harm in it.
   c. You wrote a program that hacks into all the speakers of your institute and rickrolls all the classrooms in the middle of the class.
   d. You are selected to be a part of a research lab with high performance computing infrastructure. You are strictly told to only perform activities on the HPC that are related to your research work. Instead, you start to mine Bitcoin on the HPC.
   e. Your friend was working on their system and accidentally left it open due to a sudden call for a meeting from their advisor. You jump on this opportunity to sneak around your friend's system and their email.

4. According to OWASP, the top 10 Web Application Security Risks in 2021 are listed on this link: https://owasp.org/www-project-top-ten. These include broken access control, injection, security logging and monitoring failures, and so on.

In bullet points, mention each of the 10 security risks as a heading, answer whether you handled it in your application (project submission) or not. If the answer is yes, then explain how you handled it, otherwise explain what you could have done to handle it.

Note: Marks will not be deducted if you answer "no" to these points. Keep your answers as honest as possible. **[10]**

5. The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information *does not* add appreciably to the security of a system. Then, give an example of a situation in which it *does*. **[5]**

6. [IIITD - The Electronic Mail Policy]
   The policy first warns users that their electronic mail is not private. Mails may be read accidentally, in the course of normal system maintenance, or in other ways stated in the full policy. The policy also warns users that electronic mail can be forged or altered as well as forwarded (and the forwarded messages may be altered).

   Following are lists of what users should, and should not, do. They may be summarized as "think before you send; be courteous and respectful of others; and don't interfere with others' use of electronic mail." The list emphasizes that supervisors have the right to examine employees' electronic mail that relates to the job. Surprisingly, the university does not ban personal use of electronic mail, probably in the recognition that enforcement would demoralize people and that the overhead of carrying personal mail is minimal in a university environment. The policy does require that users not use personal mail to such an extent that it interferes with their work or causes the university to incur extra expense.

   In a private company, this would be unnecessary, but the University is bound to respect parts of the Indian Constitution. Also, as an educational institution, the university takes the issues surrounding freedom of expression and inquiry very seriously. Would a visitor to campus be bound by these policies? The final answer to this is yes.

   Consider the IIITD-policy on reading electronic mail. A research group wants to obtain raw data from a network that carries all network traffic to the Department of SSH.
   a. Discuss the impact of the electronic mail policy on the collection of such data. **[5]**

b. How would you change the policy to allow the collection of this data without abandoning the principle that electronic mail should be protected? **[5]**

7. Let k be the encipherment key for a Caesar cipher. The decipherment key differs; it is (26–k). One of the characteristics of a public key system is that the encipherment and decipherment keys are different. Then, why is the Caesar cipher a classical cryptosystem, but not a public key cryptosystem? **[5]**

8. [Checksum Functions]

    a. What is a checksum function in the context of Cryptography? Is the identity function, which outputs its own input, a good cryptographic checksum function? Why or why not? **[2.5]**
    b. Is the sum program, which **exclusive or**'s all words in its input to generate a one-word output, a good cryptographic checksum function? Why or why not?
    Example: suppose the input has words FCS and Endsem. The sum program will convert both the words into bits, perform exclusive OR to generate one-word output. **[2.5]**

9. Fisch, White, and Pooch (https://ieeexplore.ieee.org/document/367314) define four levels of log sanitization.
    a. Simple sanitization, in which all information except the commands issued by an intruder are deleted.
    b. Information-tracking sanitization, in which sensitive information is entered into a symbol table as it is encountered, a unique identifier is assigned, and whenever that information is encountered it is replaced with the associated identifier.
    c. Format sanitization, in which compressed or encoded data is transformed into its original form, the original form is sanitized using information-tracking sanitization, and the resulting data is returned to its transformed format.
    d. Comprehensive sanitization, in which all data is analyzed and sanitized as in information-tracking and format sanitization.

    Discuss the level of anonymity of each level of sanitization. Which level could be automated, and to what degree would human oversight be required? **[10]**

10. **[BONUS]** Assume that a Cypherpunk remailer reorders messages. It has a pool of n – 1 messages at all times. When the nth message arrives, one of the n messages is selected at random and forwarded. An attacker floods the server with enough messages to force the n – 1 messages in the original pool to be sent.
    a. Assuming that the message to be sent is chosen according to a uniform random distribution, what is the expected number of messages that the attacker would have to send to achieve this goal? **[5]**
    Hint: The expectation of a uniform random distribution is (b+a)/2, where b=maximum value in the distribution, a=minimum value in the distribution.
    b. How can the attacker determine when all the messages originally in the pool have been sent? **[5]**