Instructions

There are **85 total points**. When asked to provide your answer within a figure or table, be careful to not exceed box boundaries. Bubbles must be filled out completely: ● is correct, ⊘ ⊙ ⊗ are incorrect All answers must be given within the provided circles, answer boxes, figures or tables. Write your full name in the box to acknowledge the instructions.

Permitted materials: one 8.5x11-inch double-sided handwritten note sheet. No books, printouts, or other notes, and no electronic devices of any kind (including phones, laptops, tablets, smartwatches, and calculators).

Ethics

1. [4 points]: According to the Menlo Report, which of the following ethical principles should guide cybersecurity research? (Select all that apply.)

◯ Respect for Persons

◯ Beneficence

◯ Justice

◯ Respect for Property

◯ Respect for Law and Public Interest

> **Case Study:** A cybersecurity researcher discovers a critical vulnerability in a widely-used IoT device that could allow attackers to gain unauthorized access to users' home networks. The researcher wants to publish their findings to raise awareness and encourage the manufacturer to fix the issue. However, the manufacturer argues that public disclosure could put millions of users at risk before a patch is available, and threatens legal action under the Computer Fraud and Abuse Act (CFAA). The researcher must decide whether to publish immediately, delay publication to allow for coordinated disclosure, or not publish at all.

2. [3 points]: Use the principle of *beneficence* to present an argument **in favor** of immediate publication.

(Answer inside the box)

Initials: ____

3. [4 points]: Use the principle of *justice* to present an argument **against** immediate publication.

(Answer inside the box)

4. [3 points]: A security researcher wants to study password reuse patterns by analyzing data from previous data breaches. The researcher plans to use this data to develop better password policies and security recommendations. However, the data contains plaintext passwords and personal information of millions of users who never consented to having their information used for research purposes. Which ethical principle is most directly violated by using this data without user consent?

◯ Justice

◯ Beneficence

◯ Respect for Law and Public Interest

◯ Respect for Persons

◯ None of the above

Foundations

5. [3 points]: In Thompson's "Reflections on Trusting Trust," what is the main lesson about trust in computing systems?

◯ Compilers always produce trustworthy output

◯ Source code inspection is sufficient to verify system security

◯ You cannot fully trust code that you did not completely create yourself

◯ Open source software is inherently more trustworthy

◯ Backdoors in compilers are easy to detect through code review

6. [4 points]: According to Anderson's "Why Cryptosystems Fail," which of the following are examples of how cryptosystems fail due to people and operational issues rather than cryptographic weaknesses? (Select all that apply.)

◯ ATM fraudsters exploiting weaknesses in how PIN verification is implemented

◯ Bank employees being bribed or coerced to compromise security

◯ Mathematical weaknesses in encryption algorithms

◯ Poor key management and storage practices

◯ Failure to properly audit and monitor system access

Public Key Infrastructure

7. [4 points]: Which of the following statements correctly describes the role of a Certificate Authority (CA) in Public Key Infrastructure (PKI)? (Select all that apply.)

◯ A CA issues digital certificates that bind public keys to identities

◯ A CA encrypts all communication between clients and servers

◯ A CA verifies the identity of entities before issuing certificates

◯ A CA stores the private keys of all entities in the PKI

◯ If a CA's private key is compromised, all certificates issued by that CA become untrustworthy

8. [4 points]: In Assignment 1, you captured HTTP and HTTPS traffic with Wireshark. Describe what specific differences you observed in the packet traces between HTTP and HTTPS traffic, and explain why self-signed certificates generate browser warnings.

(Answer inside the box)

9. [3 points]: Explain what happens when a Certificate Authority (CA) is compromised and how this affects the security of the entire PKI system.

(Answer inside the box)

Authentication

10. [4 points]: OAuth 2.0 allows users to grant third-party applications access to their resources without sharing their passwords. ◯ Yes ◯ No

11. [3 points]: Explain why or why not.

(Answer inside the box)

Initials: ____

12. [4 points]: Which of the following are security benefits of using OAuth 2.0 instead of sharing passwords directly? (Select all that apply.)

◯ Users don't need to share their passwords with third-party applications

◯ Access tokens can be limited in scope and expire automatically

◯ Users can revoke access to third-party applications without changing their password

◯ OAuth 2.0 provides stronger encryption than traditional password authentication

◯ Applications only receive the minimum permissions needed to function

13. [3 points]: What is a potential security risk of OAuth 2.0 implementations?

◯ Improperly configured scopes could grant excessive permissions

◯ OAuth 2.0 transmits passwords in plaintext

◯ Access tokens are permanently valid

◯ OAuth 2.0 doesn't support HTTPS

Denial of Service and Botnets

14. [4 points]: Which of the following characteristics make DNS particularly suitable for amplification attacks? (Select all that apply.)

◯ DNS responses are typically much larger than DNS queries

◯ DNS servers will respond to queries with spoofed source IP addresses

◯ DNS operates over UDP, which doesn't require connection establishment

◯ DNS queries always require authentication

15. [4 points]: Which of the following are typical characteristics that make denial of service attacks difficult to defend against? (Select all that apply.)

◯ Attack traffic is often difficult to distinguish from legitimate traffic

◯ Attacks often involve asymmetry where small requests generate large responses

◯ IP address spoofing makes attribution difficult

◯ Attacks always target a single specific port

◯ Attackers can use reflection to hide the true source of the attack

Web Security

16. [4 points]: Which of the following best describes the Same-Origin Policy in web browsers?

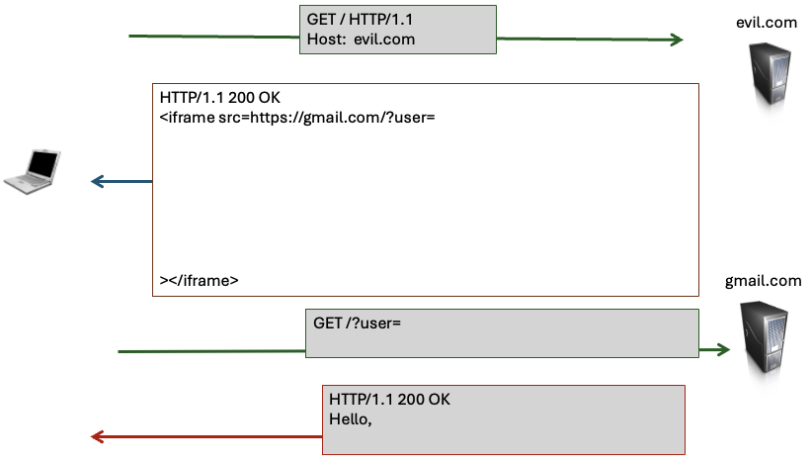
◯ Scripts can only access resources from the same protocol, domain, and port

◯ All websites must use the same security certificates

◯ Cookies are shared between all websites on the same domain

◯ HTTPS connections are required for all cross-domain requests

17. [4 points]: The diagram below shows a **reflected XSS** attack. Fill in the blank box to show the malicious payload.



18. [3 points]: Which of the following are effective defenses against Cross-Site Scripting (XSS) attacks? (Select all that apply.)

◯ Input validation and sanitization to remove or encode dangerous characters

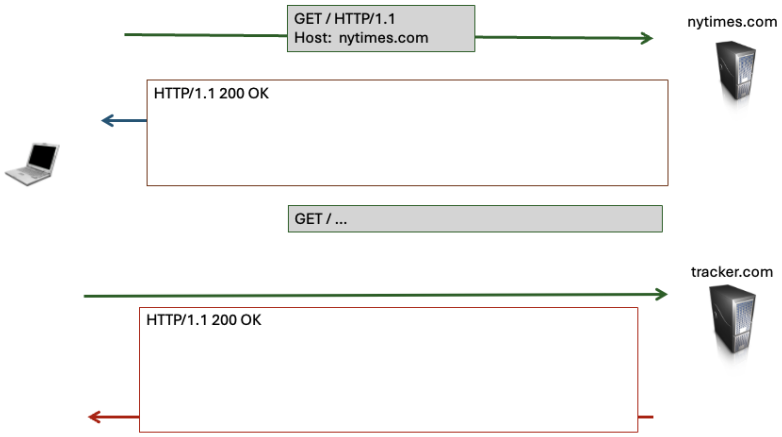
◯ Content Security Policy (CSP) headers to restrict script execution

◯ Output encoding when displaying user-generated content

◯ Using HTTPS instead of HTTP

Web Tracking

19. [4 points]: The diagram below shows third-party tracking. Fill in the boxes to show: (1) What code nytimes.com includes to trigger the browser to contact the tracker (2) The HTTP request to the tracking server.



Initials: ____

20. [3 points]: Which of the following techniques can be used for browser fingerprinting to track users even after they delete cookies? (Select all that apply.)

◯ Canvas fingerprinting using HTML5 canvas rendering

◯ Collecting browser and system information like screen resolution and installed fonts

◯ Measuring timing differences in JavaScript execution

◯ Setting persistent cookies with long expiration dates

◯ Checking installed browser plugins and extensions

DNS Security

21. [3 points]: What was the primary vulnerability exploited in the Kaminsky DNS cache poisoning attack?

◯ Predictable transaction IDs and source ports in DNS queries

◯ Unencrypted DNS communication

◯ Weak authentication in DNS servers

◯ Buffer overflows in DNS parsing code

22. [3 points]: Explain what privacy risks exist when DNS queries are sent unencrypted, and what information can be observed by network intermediaries.

(Answer inside the box)

23. [3 points]: What security or privacy problem does DNSSEC solve?

(Answer inside the box)

24. [2 points]: When DNS-over-HTTPS is enabled, network administrators can still monitor DNS queries by inspecting traffic at the local DNS resolver. ◯ Yes ◯ No

Feedback

25. [1 point]: Interest (1=Boring!; 10=Amazing!): ☐ Difficulty (1=Too easy; 10=Too hard): ☐

26. [1 point]: 1. One thing you liked about the course so far. 2. One suggestion for improvement:

(Answer inside the box)

Initials: ____