Homework 6

Due Date: **Friday, 12/12, 11:59pm**

Instructions

1. Unless otherwise specified, any assignment involving programming may be completed with the programming language of your choice. If asked, you should be able to explain the details of your source code (e.g. program design and implementation decisions).
2. You are bound by the Stevens Honor System. All external sources must be properly cited, including the use of LLM-based tools (e.g. ChatGPT). Your submission acknowledges that you have abided by this policy.

Additional Instructions

1. Solutions are to be uploaded on Gradescope under the corresponding assignment names.

Problem 1 - (*40 pts*) E2E, Apple, and the UK

In early 2025, the UK Government issued a so-called Investigatory Powers Act 2016 (IPA) "technical capability notice" (TCN) to Apple. The notice demanded that Apple build a "backdoor" into users' cloud data — meaning that, under the order, UK security agencies would get broad access to files stored with Apple's cloud service globally.

The demanded access would have undermined the security of the company's high-security offering, Advanced Data Protection (ADP), which provides end-to-end encryption such that only the user can decrypt their iCloud data. Under ADP, not even Apple can view the data.

Apple refused to comply with the notice and withdrew ADP from the UK; as of February 21, 2025, new UK users can no longer enable ADP.

After pulling ADP, Apple filed a legal challenge at the Investigatory Powers Tribunal (IPT), arguing that the UK government's demand violated privacy and encryption norms. The hearing was scheduled in closed court, though media and civil-society organizations have pushed for public transparency, arguing it's a case of broad public interest.

On August 18, Tulsi Gabbard posted that the UK would be dropping their TCN.

1. Read the following series of short articles to familiarize yourself with the details of the controversy.
   - Brodkin, Jon. "UK demands Apple break encryption to allow gov't spying worldwide, reports say". *Ars Technica*. 2025-02-07. Online.
   - Belanger, Ashley. "Apple pulls end-to-end encryption in UK, spurning backdoors for gov't spying".

     Ars Technica. 2025-02-21. Online.
   - Brodkin, Jon. "Apple refuses to break encryption, seeks reversal of UK demand for backdoor". *Ars Technica*. 2025-02-21. Online.
   - Kleinman, Zoe. "UK backs down in Apple privacy row, US says". *BBC*. 2025-08-19. Online.
   - Fraser, Graham. "Court documents shed new light on UK-Apple row over user data". *BBC*. 2025-08-29. Online.
2. Write a short response (50-200 words) in response to each of the following prompts.
   1. (*10 points*) Identify the stakeholders involved in the case, both those directly involved and those who would be affected, and what is at stake for each group or individual.
   2. (*10 points*) Identify the technologies relevant to this story and why they are the subject of contention between Apple and the UK. What is the relationship between the technology(-ies) and each party?

3. (*10 points*) Make an argument for both Apple and the UK government defending their ethical position based on the *interests* they are trying to protect and *harms* they are trying to prevent. Refer to part 1 of the Vallor reading to formulate your argument.
4. (*10 points*) What are the ethical values in tension in this case? Pick the side that you think has a stronger argument by identifying which interests and/or harms outweigh the other *in this particular instance* and justify your decision with scenarios or concrete examples.

Problem 2 - (*60 pts*) XSS and CSRF CTFs

Complete the following `pwn.college` challenge. For each challenge, 10 points will come from completion, 10 points from code submission, and 10 points for sufficient explanation of your source code. Partial credit may be obtained for providing source and explanation if these were on the right track.

Any source code or terminal commands used should be included in your PDF submission, as Gradescope will not accept additional files.

1. *XSS 2* from the *Web Security* module
   - **Hint 1**: The goal is to inject an HTML element with javascript that will be executed when the victim loads the page.
2. *CSRF 1* from the *Web Security* module
   - **Hint 1**: The victim will first log in to the vulnerable website, then visits an attacker-controlled website. The idea is that when the victim visits the attacker's server, the malicious server will force the victim to make an unintended HTTP request to the vulnerable site that can trigger unintended actions.
   - **Hint 2**: You will need to write a simple web server that you control to carry out this attack. A simple flask server dine in the same manner as the `pwn.college` challenge servers will work nicely.
   - **Hint 3**: `redirect` exists in the Flask library and might help you out here.