Lab 8: The Poisoned Pen

1 Introduction

The door is locked, Detective. So we must steal the key.

You have proven you can map a network and find the open windows. But some targets have no open windows. Some targets live behind heavy steel doors (Authentication) and thick concrete walls (Databases). To breach these, you cannot use force. You must use guile.

The Baker Street Society has targeted a corrupt front organization. They operate a secure internal web application. We cannot break in from the outside; we need someone on the inside to open the door for us. That "someone" is the Administrator.

Your mission is a two-stage con. First, you must set a trap to steal the Administrator's digital identity. Second, once you have assumed their identity, you must interrogate their archives and force them to reveal their secrets.

Trick the browser. Trick the database. Steal the Hash.

2 The PI Code (Web Measures)

The rules of engagement have shifted. You are operating on the Application Layer.

Precision Strikes. Web servers are fragile. Unlike a port scan, a bad web query can crash the database or lock out accounts. You are a grifter, not a vandal. Proceed with caution.

Target Scope. You are authorized to attack the specific web application URL provided below. Do not attempt to attack the hosting infrastructure, the university network, or any other sites hosted on the same server.

3 The Setup

The target web application is hosted deep within the internal network and is not accessible from the public internet. To reach it, you must tunnel your traffic through the Society's secure Jump Host.

3.1 Establishing the Tunnel

You must construct an **SSH Tunnel** to forward a local port on your machine to the target server. This will allow you to access the internal website using your own browser.

Execute the following command in your terminal:

```
ssh -L 4334:130.208.246.228:4334 <username>@130.208.246.239 -N
```

- Replace `<username>` with your RU username (e.g., `student23`).
- When prompted, use the mission password: `icyb2025lab7!#?`
- **Note:** The `-N` flag means the terminal will hang and "do nothing." This is normal. Leave this terminal window open to keep the tunnel alive.

3.2 Accessing the Target

Once the tunnel is established, open your web browser and navigate to:

`http://localhost:4334`

You have been provided with a low-level "Guest" account to begin your investigation.

4 The Job

Your operation is divided into three primary acts. You must perform them in order to reach the prize.

4.1 Act I: The Trap

The Administrator checks the message board regularly. This is your vector. You must leave a message—a "Poisoned Pen"—that will compromise their browser. Your goal is to identify a vulnerable field and utilize it to exfiltrate the Administrator's Session Cookie.

4.2 Act II: The Masquerade

A cookie is a digital badge. If you hold the Admin's cookie, the server believes you *are* the Admin. Use the credentials you stole in Act I to impersonate the Administrator and gain access to the restricted management interface.

4.3 Act III: The Interrogation

Now that you have Admin privileges, you have access to search forms and data entry points reserved for management. However, the secrets are not listed on the screen; they are buried deep in the database structure.

Your objective is to force the database to reveal its contents. You must extract the user list and specifically retrieve the **Administrator's Password Hash**.

4.4 Act IV: The Side Hustle (Bonus Objectives)

A master detective notices what others miss. The Society suspects the application suffers from deeper structural flaws.

Once you have control, navigate to the /**bonus** area. Test the boundaries of their filing system. Just because you are requesting one file, does that mean you cannot reach others? Can you trick the server into handing you the contents of `flag.txt`?

5 The Dossier

The Baker Street Society requires a detailed forensic account of your con. To receive full payment (credit), your Field Report must meticulously document the following:

The Payload: The exact code you used to steal the cookie, and where you planted it.

The Keys: The content of the Admin Cookie you stole.

The Attack: Document exactly how you manipulated the database to reveal its secrets. Show your work.

The Loot: The specific text of the Administrator's Password Hash found within the database.

The Bounty (Bonus): If you successfully exploited the vulnerability in the /**bonus** area to read `flag.txt`, document your method and the flag content here. This will significantly increase your compensation (grade).

Plant the trap. Wear the mask. Dump the data.