Banffblogg (48 marks)

In this assignment, you will analyze the security for BanffBlogg, a hypothetical blogging site for mountain-themed posts. BanffBlogg allows users to create and delete their own posts as well as share their posts and view other users' posts (if they have been shared by that user).

Each post is given a post-id, a number associated with that post, and knowledge of the post-id is required to access posts. You'll find three versions of BanffBlogg at the following website:

`https://heroicsquirrel.com/(last 5 ucid digits)/`

You'll need the password stored in D2L as a grade item.

Each of these blogs differ only in the logic of how the post-ids are generated. Your task is to figure out how post-ids are generated and figure out a privilege escalation attack in order to tamper with the website.

To do this, go to the website itself and interact with it. Run your browser with the web console open to the network tab. While running it, look at the network traffic that is generated. Try adding new posts and deleting your posts, and see the network traffic that performs this. Look at how the posts that have been shared with you are loaded. With this information, figure out how you may be able to escalate your privileges to read, add, and delete posts of other users without permission.

Submission

Submit a pdf file describing how you achieved each attack, what was process that you performed. Write this in full sentences. *Do not* include screenshots, because your interactions with the webserver are logged to determine the actual successful completion of the task. Write clearly and concisely.

Be sure not to collaborate on this assignment because once you know the attack it is trivial to do and it can be tricky to give a hint without giving away too much of the answer. The point of this assignment is to figure out how to attack the website, not to simply replicate the attack, and it will be very apparent from the webservers interactions if one just goes to the website and immediately and correctly replicates the attack. If you need help or hints, please reach out to the professor or the TA, *not other students*.

Banffblogg 1 (16 marks)

Visit `bb1` on heroic squirrel and perform the following attacks:

- View one of Alice's posts *not shared* with you.
- View all of Alice's posts *not shared* with you.
- Delete one of Bob's posts that he has shared with you.
- Add a new post under Bob's name with your UCID in the post's data.

Banffblogg 2 (16 marks)

Visit `bb2` on heroic squirrel and perform the following attacks:

- View one of Alice's posts not shared with you.
- View all of Alice's posts not shared with you.
- Delete one of Bob's posts he has *not shared* with you.
- Add a new post under Bob's name with your UCID in it.

Hint: look at the shape of a post-id. What function has such a string as its output, and what are plausible inputs?

Banffblogg 3 (16 marks)

Visit `bb3` on heroic squirrel and perform the following attacks:

- Delete one of Alice's posts she has shared with you.
- Delete one of Alice's posts she has not shared with you.
- View one of Bob's posts not shared with you.
- View all of Bob's posts not shared with you.

Hint: if you are using your approach from the previous question and doing a brute-force search, it is not going to work. Are there other ways to learn possible values? Look for patterns of posts across users.