Mini-Project 1 - Web Exploits Report

1. **SQL Injection**

- **Description**: sql injection to see all the info in database
- Steps
    - Open burp
    - Use a account to login to the dashboard
    - When searching for user do an SQL injection such as:
        - `name' OR '1' = '1`
- **Mitigations**: Sanitize the input of searches to ensure that it is the search term is the correct format.

2. **IDOR/URL manipulation**

- **Description**: Use URL manipulation in burp to see other peoples profiles.
- Steps
    - Open burp to sniff packets
    - Login using an account to get authenticated.
    - Find the get post request and change the id to gain access to other users.

Mitigations: Athenticate that the page requested is allowed by a cookie. Will not show pages inless it has proper cookie.

3. **Session attacks**

- **Description**: Create a new admin account by spoofing a post for new account
- Steps
    - Spoof a new account post request.
    - Change the values in post request to be admin
    - Login using new account and gain access to admin panel
- **Mitigations**: When creating the form did not send boolean value for admin privileges. Default all new accounts are non admin and must be changed directly by hand.

4. **XSS**

- **Description**: Upload a image tag that has scrip
- Steps
    - When creating a new account, add an image that closes out the tag and includes XSS
    - Example: `//asdlkfjadsklfasdf.dev" onerror="alert('pwned')" >`
- **Mitigations**: Sanitize the url to ensure it is a proper link.

Password management (hashing vs salt + pepering passwords)

Hashing is a one way encryption algorithm that produces a set length of characters from a given word. This ensures that the password is not held by the server. This can be easily defeated by using a rainbow table (table of common already hashed passwords). To mitigate this some sites will use a salt. This creates a separate hash for the same password but if not implemented correctly then a hacker can find the salt and use a program(hashcat) and a rainbow table. Peppering is like hashing but there is a fixed alphabet of salts where one is selected at random and used to hash the password. On login the site will hash the password with each pepper and compare to what is in the database. If the alphabet a-z lowercase and uppercase was used it would take the hacker 52 times longer to crack the password with a hash.