Cookie Manipulation

- Cookies are used to authenticate users without asking them to enter a password at each page.
- They stored at the client side (in the browser).
- If not implemented properly, they can be modified to login as any user.

Cross Site Request Forgery

CSRF

- Requests are not validated at the server side.
- Server does not check if the user generated the request.
- Requests can be forged and sent to users to make them do things they don't intend to do such as changing their password.

CSRF Tokens

195.44.2.1

Request

http://facebook.com/password.php

Response

HTML page with UNIQUE TOKEN

→ Server will only accept form if the unique token is returned.

Mitigation

CSRF Vulnerabilities

Dynamic synchronizing tokens

1. Generate an unpredictable token that can not be reused.
   - Token needs to be a large value.
   - It must be random.
   - It should be unique.
   - Other factors can be included in the token generation algorithm.

2. Embed the token in the HTML page in a hidden form.
3. Verify the token when the form is submitted.