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









 \rightarrow 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.