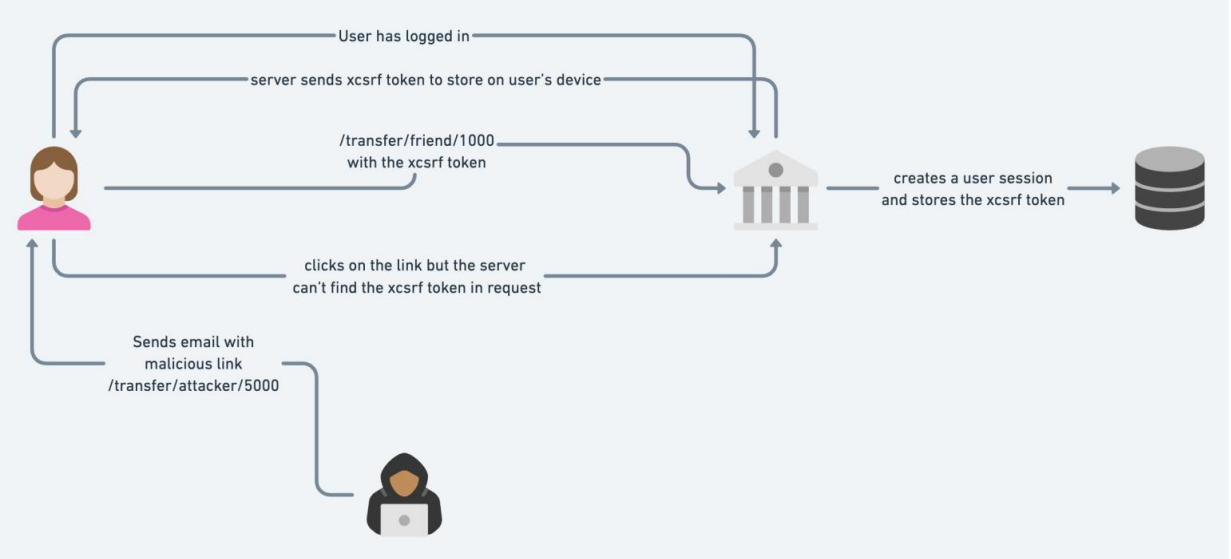
- **CSRF**
  - CSRF (Cross-Site Request Forgery) is an attack where a malicious website tricks a logged-in user's browser into sending an unauthorized request to a trusted website using the user's existing session/cookies.
  - The browser automatically attaches cookies, so the server thinks the request is legitimate.
  - Example:
    - Lets say bank website is **bank.com** and attacker's website is **evil.com**
    - **Victim** logs in
      - ```
        User → bank.com → Login successful
        Browser stores session cookie: JSESSIONID=xyz
        ```
    - Victim visits malicious site
      - ```
        <form action="https://bank.com/transfer" method="POST">
            <input type="hidden" name="amount" value="10000"/>
            <input type="hidden" name="to" value="attacker"/>
        </form>

        <script>
          document.forms[0].submit();
        </script>
        ```
    - Browser sends request
      - ```
        POST /transfer
        Cookie: JSESSIONID=xyz
        ```
    - **Cookie is valid; money transfer successful; money is *gone*.**
  - So basically, **CSRF** attacks doesn't steal password; It uses user's cookies stored in the browser to steal the data/money.
  -
    - F
    - F
    -
        ```



- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- F
- vf