Passwords

Friday, October 20, 2017 11:30 PM

Password Strength

- Accounts are only as secure as their passwords
- Most users have the same weak password everywhere
- If you want to protect them against brute-force-attacks your application should have good requirements for passwords
  - Should contain lower case letter, capitals, numbers, and special characters
  - The longer the password, the better, consider using a passphrase instead

Forgot Password

- Web applications frequently provide their users with the ability to retrieve a forgotten password
- Unfortunately, many web applications fail to implement the mechanism properly
  - The information required to verify the identity of the user is often overly simplistic

***You can also keep guessing usernames and the site will basically tell you if they exist or not based on whether it errors out or prompts you for the secret question (to which you can brute force the answer)

Multi Level Login 1 (2FA)

- A multi level login should provide a strong authentication
  - This is achieved by adding a 2nd layer
- After having logged in with your user name and password you are asked for a 'Transaction Authentication Number' (TAN)
  - This is often used by online banking
  - You get a list with lots of TANs generated only for you by the bank
  - Each TAN is used only once
  - Another method is to provide the TAN by SMS

<u>Solution</u>

- Login as normal with Jane
- Use WebScarab as you submit the TAN
  - You will see that the hidden TAN is 1
- Login as Jane as the hacker
- It will prompt you for a different TAN that you don't know
  - Just change the hidden TAN back to 1 enter the TAN 1 that you do know

Multi Level Login 2 (2FA)

- A multi level login should provide a strong authentication
  - This is achieved by adding a 2nd layer
- After having logged in with your user name and password you are asked for a 'Transaction Authentication Number' (TAN)
  - This is often used by online banking
  - You get a list with lots of TANs generated only for you by the bank
  - Each TAN is used only once
  - Another method is to provide the TAN by SMS
    - This has the advantage that an attacker cannot get TANs provided by the user

<u>Solution</u>

- Similar approach as in 1
- Login as yourself

- Launch webscarab before entering your TAN
- Intercept the HTTP request
- Change the name from Joe to Jane