資訊安全實務與管理 Homework #1

利用HTML和PHP(或ASP/JSP等)撰寫一個Web應用系統，功能說明如下：

1. 首先須輸入帳號及密碼登入系統，輸入內容限英數字，以避免SQL Injection 攻擊。
2. 可使用文字檔或資料庫等方式儲存使用者資料，至少含帳號、密碼(加密)及姓名。
3. 輸入帳密正確即登入成功，顯示"歡迎<姓名>"訊息，並利用Session進行會談管理。
4. 登入成功頁面同時顯示"登出"按鈕，按下後刪除Session，並跳回登入頁面。
5. 登入動作須留存紀錄(log)，可紀錄於文字檔或資料庫，至少應留存帳號、來源IP、時戳及結果(成功或失敗)。
6. 未經登入直接跳至任一頁面應重導至登入頁面。
7. 五分鐘內連續登入失敗三次應鎖定(不接受登入)五分鐘。
8. 具修改密碼功能，密碼須符合複雜度要求(八碼以上，含數字及大小寫英文字母)，且不得與前三代相同。

對照表 ：

項次	程式碼檔名	程式碼段落 （行）	說明
1	process_register.php	23-27	在註冊時進行檢查
2	process_register.php	29-41	儲存在資料庫 account
3	process_login.php	54-58	確認登入成功並建立session
	home.php	22、35-37	顯示歡迎訊息 進行會談管理
4	home.php	4-13、39-42	
5	process_login.php	60-65	儲存在資料庫 rec_login
6	home.php	15-19	
7	process_login.php	69-86	
8	process_change_password.php	A11	

資料庫說明如下

資料庫說明 : 共有2個表格，account 和 rec_login

- account （可於註冊頁面插入新的資料）

  username : 帳號，不可重複

  realname : 姓名

  password : 目前的密碼（取hash）

  password1 : 前一次的密碼（若未更改過密碼則為NULL）

  password2 : 前兩次的密碼（若未更改過密碼則為NULL）

  測試資料:

username	realname	password	password1	password2
jerry123	Jerry	$2y$10$geHZ0Ou2v9qfa4yQF4LJ5ezgVt6KdCJKsIIEE8Pd69m4msOdZzJnC	NULL	NULL
pollychen1	polly1	$2y$10$vajA5FuQGObnePIqvd3j9eY0ucM00IFGLLCVzbUhtjW.gdXfbK7TG	NULL	NULL
pollychen123	Polly Chen	$2y$10$j8gtmkbaZEnUXrG4uPYVXeIyA6ovHVUk7LMEfQ.kcrotgdqHWqwoe	$2y$10$KDcKirDbhguTla1NdVWpmOIfmAfpsN.H2EKTYzBTvkeWOLXzX0BSS	NULL

- rec_login（記錄登入狀態）

  username : 帳號 login_time : 時戳

  result : 是否登入成功 （1為成功，0為失敗）

  locked : 是否被鎖定（5分鐘內三次失敗即為鎖定，1為鎖定）

  ip_address : IP位址（因在本地端測試，下圖為本地主機IPV6地址）

  測試資料:

username	login_time	result	locked	ip_address
pollychen123	2024-11-17 14:08:30	1	0	::1
jerry123	2024-11-17 14:08:57	0	0	::1
jerry123	2024-11-17 14:12:00	0	0	::1
jerry123	2024-11-17 14:13:55	0	1	::1
pollychen1	2024-11-17 14:14:47	1	0	::1