一、使用者個資的密碼，在資料庫沒有加密?

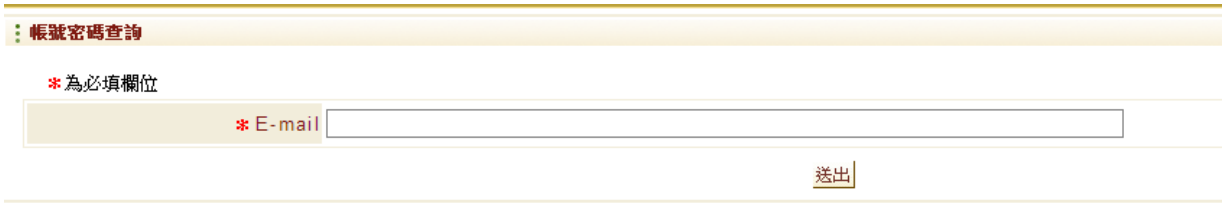
實驗步驟：

1. 進入APP會員中心，加入會員
http://cabletvweb.ncc.gov.tw/SWSFront35/MEMBER/MEMBER01001.aspx?FunId=MEMBER1001

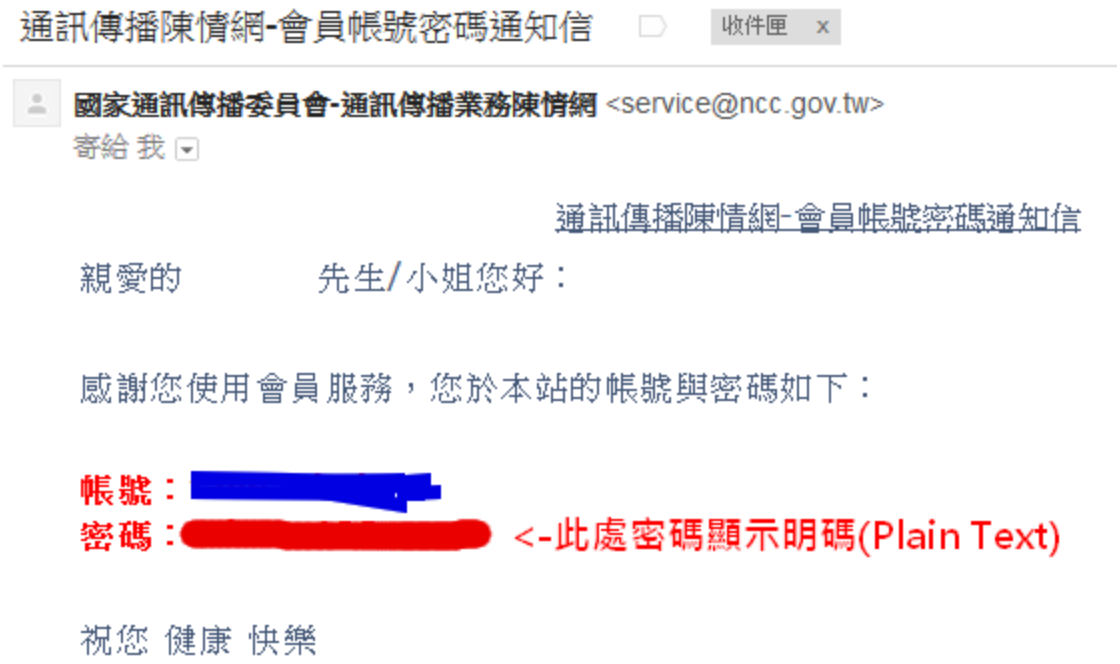

2. 註冊完畢後，去收信，再到網站輸入密碼，以啟動帳號。

3. 進入帳號密碼查詢頁面
http://cabletvweb.ncc.gov.tw/SWSFront35/MEMBER/MEMBER01002.aspx?FunId=MEMBER1002


4. 輸入註冊的email帳號




5. 收信可看到完整的明碼




資安風險議題：
寄出來的密碼信件，是屬於明碼(Plain Text)。代表儲存在資料庫時，可能是兩種狀況之一：

1.資料庫沒有將使用者的重要個資密碼採用如 Internet 慣用的單向函數加密(Hash function)，與Salt機制，此項技術早期的Unix/Linux系統早已採用。

2. 或者是其採用了「可還原密碼的加密機制」，所以信件寄出來可還原使用者原先設定的密碼。

最大風險：若資料庫被破解，使用者的慣用密碼，將直接全部揭露。

關於這段資安議題，可以參考資安專家部落格的建議：[我的密碼沒加密]

二、帳號個資註冊，沒有傳輸加密？

實驗步驟：
1. 加入會員
http://cabletvweb.ncc.gov.tw/SWSFront35/MEMBER/MEMBER01001.aspx?FunId=MEMBER1001


2. 點選同意後，看瀏覽器網址左上角(地球)，代表沒有傳輸加密！


如果有傳輸加密，可參考此政府入口網的會員加入系統 的網頁右上角，政府入口網有針對帳密傳輸的加密，這樣是安全的：

https://www.cp.gov.tw/portal/person/initial/Registry.aspx


資安風險議題：
使用者若在公用電腦、或者使用開放式Wi-Fi 連接註冊，包含帳號、姓名、email，都可以輕易被攔截

三、登入密碼，沒有加密？

實驗步驟：

1. 接續二的情境，收件拿到密碼後，進入登入頁面
http://cabletvweb.ncc.gov.tw/SWSFront35/MEMBER/MEMBER01000.aspx
可以發現此頁也沒有加密傳輸。


2. 第一次登入後，導入要求修改密碼頁面，結果這頁也沒有加密～


資安風險議題：

使用者若在公用電腦、或者使用開放式Wi-Fi 連接註冊，此兩處輸入密碼、修改密碼都可以輕易被攔截

給所有政府網站、以及大型電信商的資訊安全管理建議如下：

1. 建議政府涵蓋民眾個資的重要大型網站，全面導入ISO 27001的資訊安全管理流程，並且由第三方驗證機構，進行定期稽核驗證。

2. 建議網站負責的最高主管，可以參加"ISO27001 資安管理系統主導稽核員"的課程，可有效建立資訊安全的管理知識，包含從技術面、管理制度面、政策面、法規面等等。

3. 建議網站管理的負責主管，請教熟悉網路安全的學者專家，進行網站安全設計的整體檢視，並且調查是否有個資因傳輸沒有加密或者密碼沒有加密儲存，造成相關的衝擊。

4. 建議清查儲存資料庫的密碼資料，是否為明碼。或者雖有加密，但並沒有採用無法還原的密碼學技術（Hash function + Salt 機制）。

資訊安全管理，是一門很艱深的學問。不只需要懂理論，也需要懂實做技術。

大型電信商有導入ISO 27001是很值得鼓勵的事，但是驗證通過 ISO 27001不代表系統就絕對安全。 因為也發現到有大型電信商網站出現上述這類的資安問題 ：(a) 重要會員個資帳密網頁，沒有傳輸加密、(b) 寄送密碼信時，信件出現明碼。

建議大型電信商定期檢查會員個資服務.....比對隱私權政策，以及實做系統上是否說寫做一致...

感恩各位政府公務員，具有專業技術的電信商、以及所有在產學界默默奉獻資安教育、網路通訊教育的學者們，一同守護中華民國所有公民的的個資與通訊保障安全。

感恩那些年輕的孩子們，謝謝您們為社會大眾的努力！感恩再感恩！