# 資訊安全概論與實務
# 期末報告

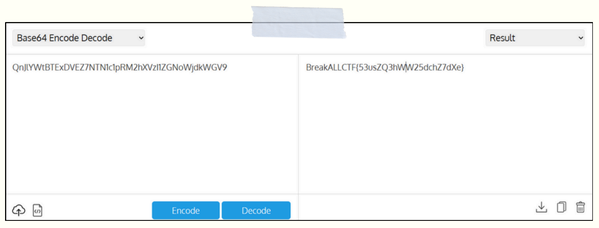
一公 26黃宣柔、一公 35蘇媞芸、
一誠 37聶宜帆、一愛 7李欣恬、一愛 10林涵瀠

**課程簡介**：培養正確的資安觀念 、了解資安事件常見的手法，並在課堂中實作資安攻防作業。

## 課程內容介紹

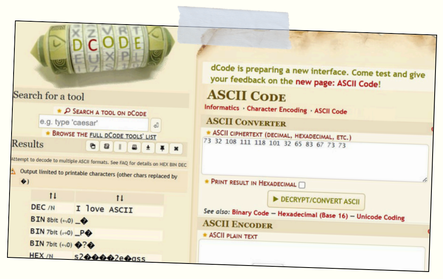
### 編碼與解碼

了解ASCII、Base64、Morse code摩斯密碼概念後，使用線上工具解開亂碼，最後利用生成式AI生成可用於解碼的python程式，用google colab執行。



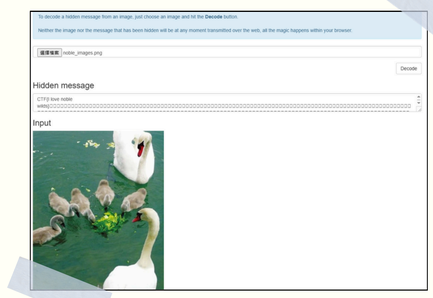

### 密碼學概論

透過學習不同類型的密碼，例如:古典密碼及現代密碼差異、Caesar Cipher等，了解密碼的使用情形，再使用線上工具，將文字加密解密，進行身分驗證、隱藏訊息。



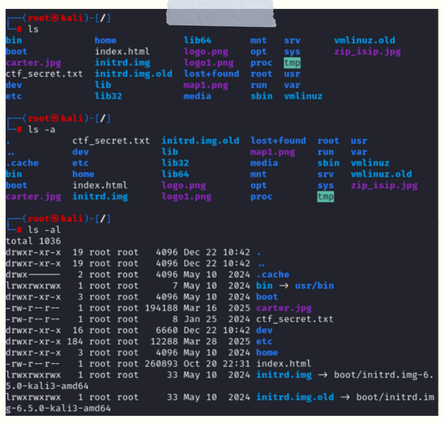

### 隱寫術

學習文件隱寫和圖片隱寫的技術，並且利用線上網站解密圖片中的文字。




### Linux簡介

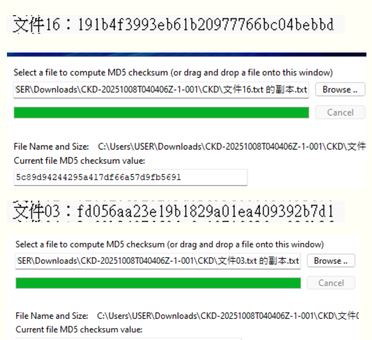
Linux是自由和開放原始碼(open sourse)的UNIX-like作業系統,可利用CDX終端機進行指令操作,如: ls(list 清單) cat(檔案名稱) less(文件) ,利用這些可以去尋找資料或是寫程式,甚至可以去問候其他電腦看它有沒有生命跡象!:-D




CDX終端機實作

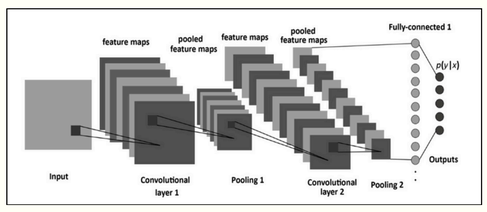
### 參加高中跨校資安實務素養挑戰賽-個人賽與團體賽



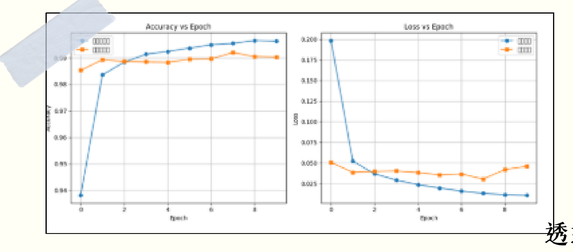



在比賽過程中，我們利用題目提供的參考網站，以及團體賽中以團隊合作的方式解題。這個比賽經驗也讓我們體會到資安題目的困難部分--判斷要使用的工具：網路上的工具有千百種，要挑出能夠解出題目的工具，才是解題的關鍵。

### 人工智慧AI簡介



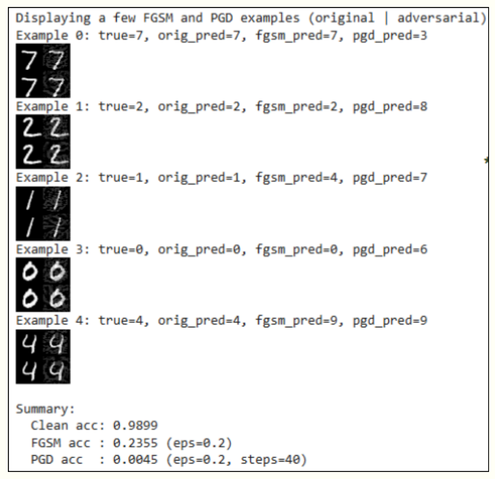

透過學習多種經典神經網路(神經網路、卷積神經網路、遞歸神經網路)，理解人工智慧的運作方式，並運用問題實作，建立對AI的基本認識。




透過AI實作成果

### 模型逆向攻擊 MNIST訓練模型

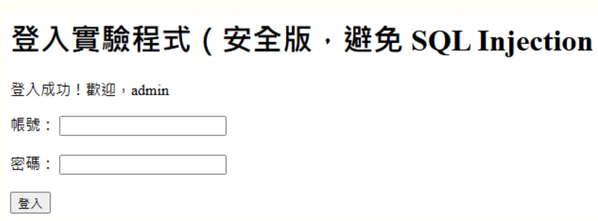
模型逆向攻擊是一種嘗試「從模型推回輸入資料」的攻擊方式。
也就是說：
攻擊者利用模型的輸出（例如：機率、分類結果），反推原本用來訓練模型的資料長什麼樣子。
在了解其相關的知識理論後，
透過Chat GPT生成模型逆向攻擊的程式，貼到google colab上執行，觀察其準度。




實際執行成果

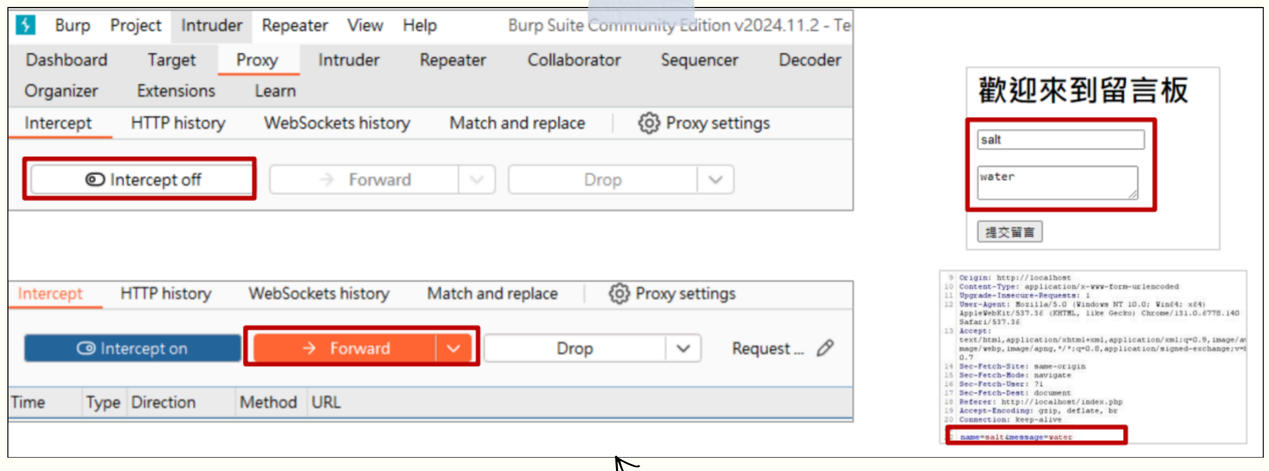
### SQL injection 實作

了解SQL injection是透過輸入惡意SQL指令改變資料庫查詢語句，可能導致登入繞過、刪除資料表，並進行實作




### 封包攔截-Burp Suite攔截

所謂的封包攔截是指在「使用者端（瀏覽器）」和「伺服器」之間，暫停、查看、分析傳輸中的資料封包的過程。而我們運用Burp Suite這個程式來協助分析與檢查網站弱點。




利用Burp Suite進行封包攔截實作

**心得**：這門課程介紹許多有趣的資訊技術，並帶我們從專業知識認識資安問題，SQL injection和封包攔截即為我們透過實作認識到可能的資安問題的例子。而密碼學和其他編譯、解譯的有趣技術都讓我們學到了很多。