還敢拿阿

貢丸文件

富方 鄭

障 CEL

還敢拿阿

Injection

注入攻擊有分很多種，但注入攻擊當中，攻擊者會在特定的地方輸入惡意的代碼，一但 Web 未經查證並且未過濾特定字元，Web 就會誤認為是正常程序，就造成了惡意代碼就能執行在這 Web 當中。

目前 Injection 是 OWASP Top 10 中，他被評比為 Web 當中第一高的安全風險，目前在企業當中 SQL Injection 與 XSS （Cross-Site-Scripting）是最常見的漏洞風險。

SQL Injection

SQL Injection 就是攻擊者輸入 SQL 的語法，輸入到 Web 未經正確查證或過濾的欄位當中，就造成 Web 誤認為你是正確的使用者或管理員，攻擊者就能使用該權限所能做的事情。惡意攻擊者會透過此行為進行資料串改、竊取機密文件、刪除等等的惡意行為來達到威脅公司或販賣各資等等。

SQL Injection 教學

現在假設 user 資料表存在資料如下：

userID	username	password	...
000001	admin	1234	
000002	xxx	zzz	

- 正常輸入狀況

username：admin
password：1234

```
SELECT * FROM user WHERE username='admin' AND password='1234';
```

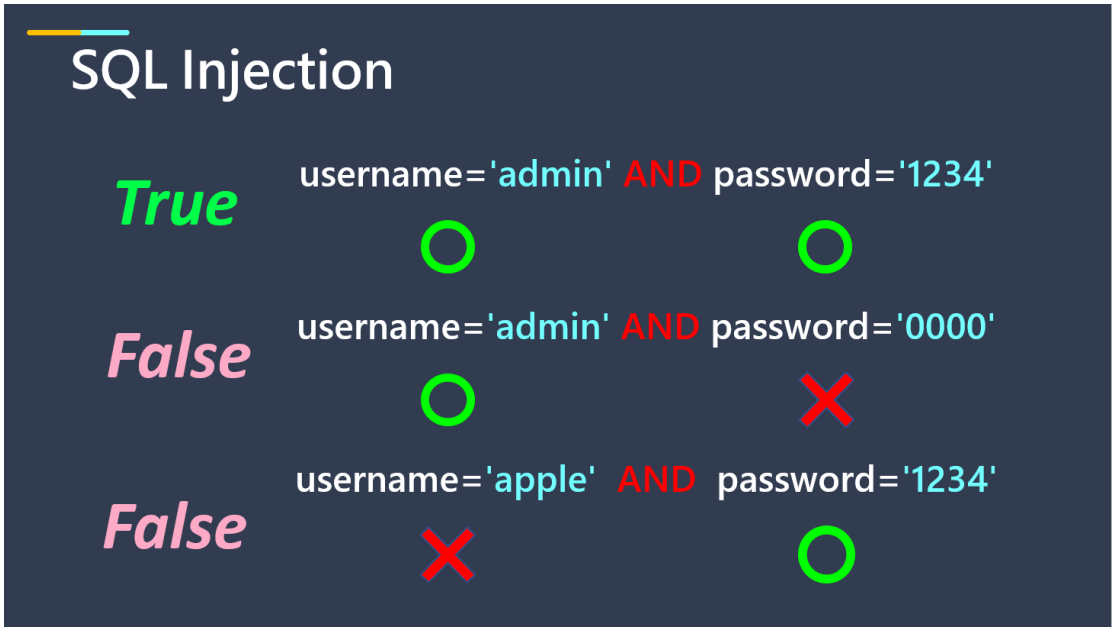
我知道，剛開始看會看的霧傻傻（台語），來讓我慢慢講解

```
SELECT * FROM user
```

先看到前面部分 SELECT * FROM user 就是取出使用者資料，舉個例來說今天要去一間餐廳吃飯，那進去時服務員會拿出『核對表』來查驗你是否有定位子等等的資訊。


```
username='admin' AND password='1234'
```

每個使用者都會對應著每一組密碼，而那個 AND 中文意思可以把它想成『並且』的意思所以說前面 username 並且要等於正確 password，如果對應不正確的密碼或 username 只要其中一個是錯誤的這個式子就不會成立。



如果有學過數位邏輯就可以透過我這張圖了解到概念就是及閘的概念

輸入 A	輸入 B	輸出
0	0	0
0	1	0
1	0	0
1	1	1

說了這麼多，應該了解大概意思是什麼了，那究竟為何攻擊者可以輕鬆繞過呢？那我們繼續看下去

- 不正常輸入

username：' or 1=1 --
password：任意值（也可以不用輸入）

```
SELECT * FROM user WHERE username='' or 1=1 -- AND password='666';//灰色代表被我註解掉
```

前面觀念我就不再提了直接跳到後面

or 1=1 就是等於 Ture 當把這個條件加入到了 username 而後面又被我用--『註解符號』下去註解掉導致後 AND(包含)以後都被我註解掉了，所以這條式子永遠成立。
稍微解釋一下密碼為什麼不用輸入或輸入任意值，由上面了解到，我透過註解符號把後面的 Password 給註解掉，所以不管我輸入什麼值進去或是不輸入值都會被註解掉。

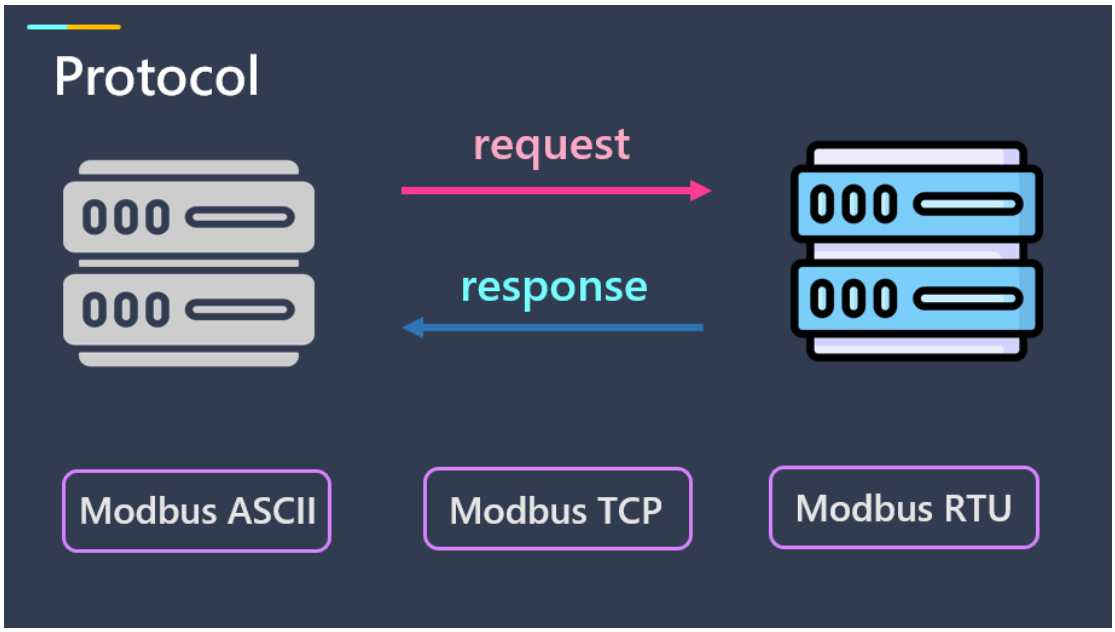
- 額外補充
  問：會有人會問說，為什麼看到很多人註解會有很多樣式
  答：因為不同資料庫有不同的註解方法

SQL Injection

資料庫名稱	
Oracle	--comment
PostgreSQL	--comment /*comment*/
Microsoft	--comment /*comment*/
MySQL	--comment ps.有空白 #comment /*comment*/

Modbus

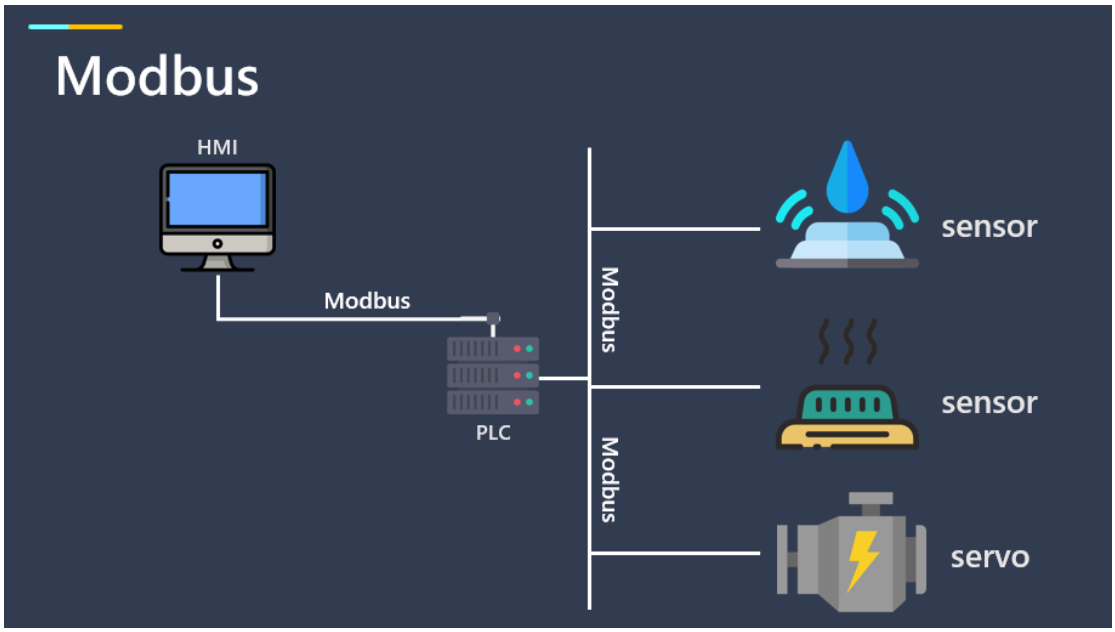
什麼是『Protocol』?
讓我娓娓道來，中文名稱為『協定』，它的功用是建立雙方的溝通模式，而 Protocol 不只有一個溝通方式，例如常見的 Protocol 有 FTP、HTTP、HTTPS...，而每個 Protocol 都有自己獨特的溝通方式，就好比你與朋友聊天和媽媽聊天會有所不同，而 Protocol 最主要的功能就是統一溝通模式，而為什麼需要統一呢？假設今天你媽媽講『台語』，而我講『英語』，這就會造成一件事情就是無法溝通，而 Protocol 就是規定你與媽媽之間只能講『國語』，這樣就可以解決你與媽媽之間的溝通問題。



Modbus 協定

目前在工業控制上，Modbus 為最常見的 Protocol，簡單來說 Modbus 可細分為 Modbus ASCII、Modbus TCP、Modbus RTU。

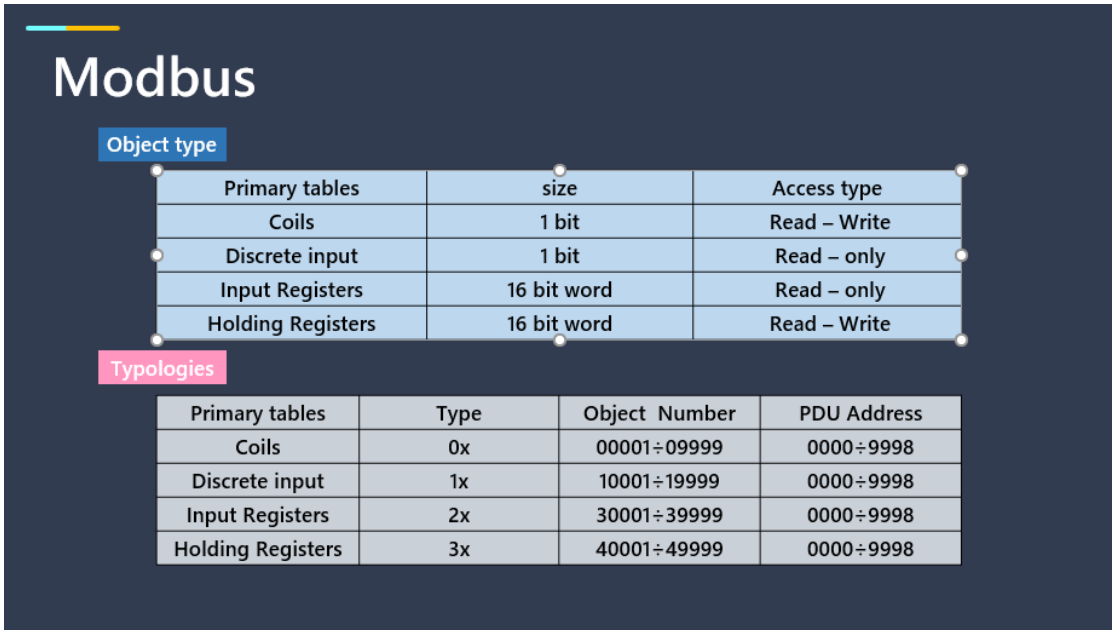
以下是正常工控的簡易流程圖



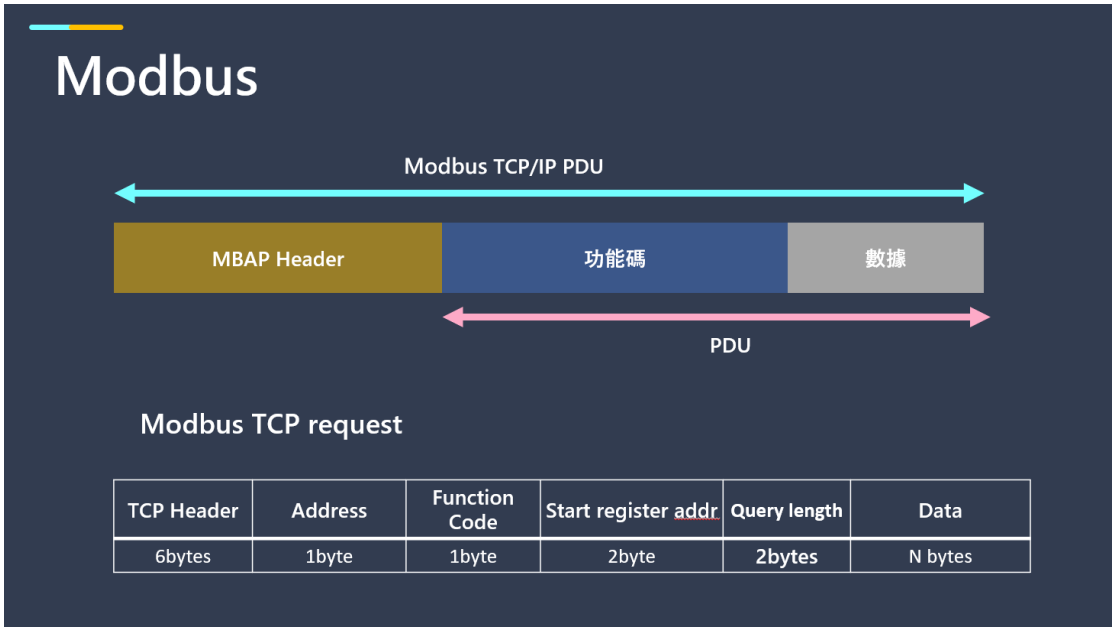
Modbus TCP

那我為了避免讓大家搞混，我就單講 Modbus TCP 的協定，其他想去了解可以上網查詢
什麼是 Modbus TCP 呢？就是透過客戶端／server 藉由 TCP/IP 的方式來傳輸資料，這就是 Modbus TCP，而 Modbus TCP port 預設是 502 port。

Modbus Typologies



Modbus TCP request 格式



1. TCP Header
   (byte 0 ~ 1)：本次通訊識別碼
   (byte 2 ~ 4)：通常為 0
   (byte 5)：資料長度（從 Address ~ data 的總長度)
2. Address
   (byte 6)：slave 端位址

3. Function code
   (byte 7)：操作碼 常見 Function code 分為這幾種
   01: 讀取當前 digital out status
   02: 讀取當前 digital input status
   03: 讀取當前 analog out status
   04: 讀取當前 analog input status
   05: 寫入單個 digital out value
   06: 寫入單個 analog out value
   15: 寫入多個 digital out value
   16: 寫入多個 analog out value
4. Start register addr
   (byte 8 ~ 9)：詢問暫存器起始位址
5. Query length
   (byte 10 ~ 11)：詢問資料長度
6. Data
   (byte 12 ~ N)：所要傳遞的資料