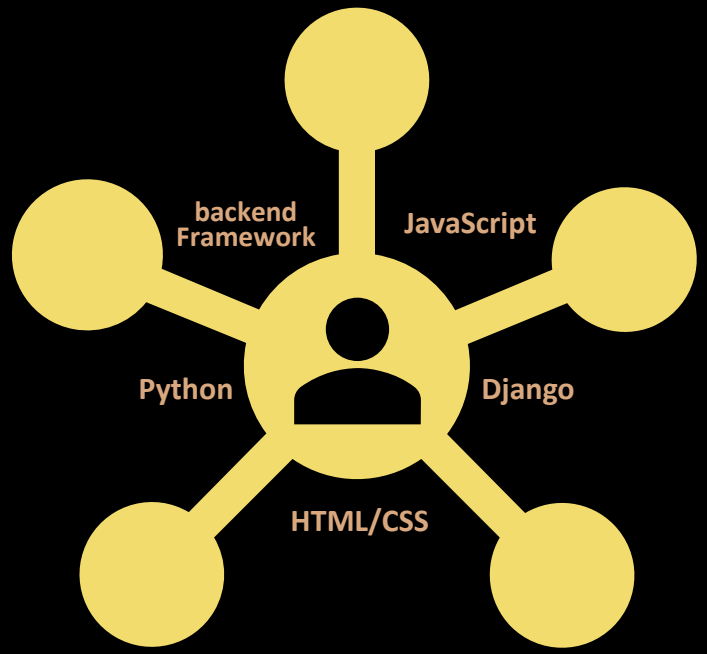
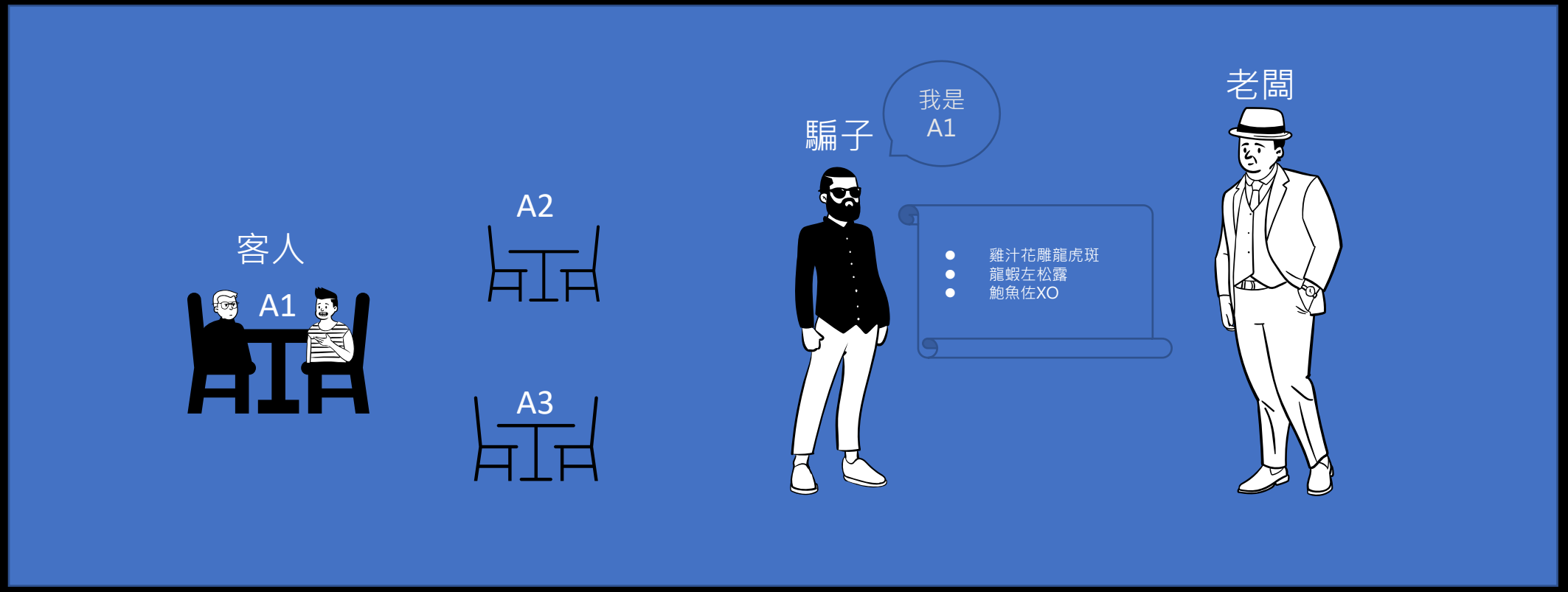


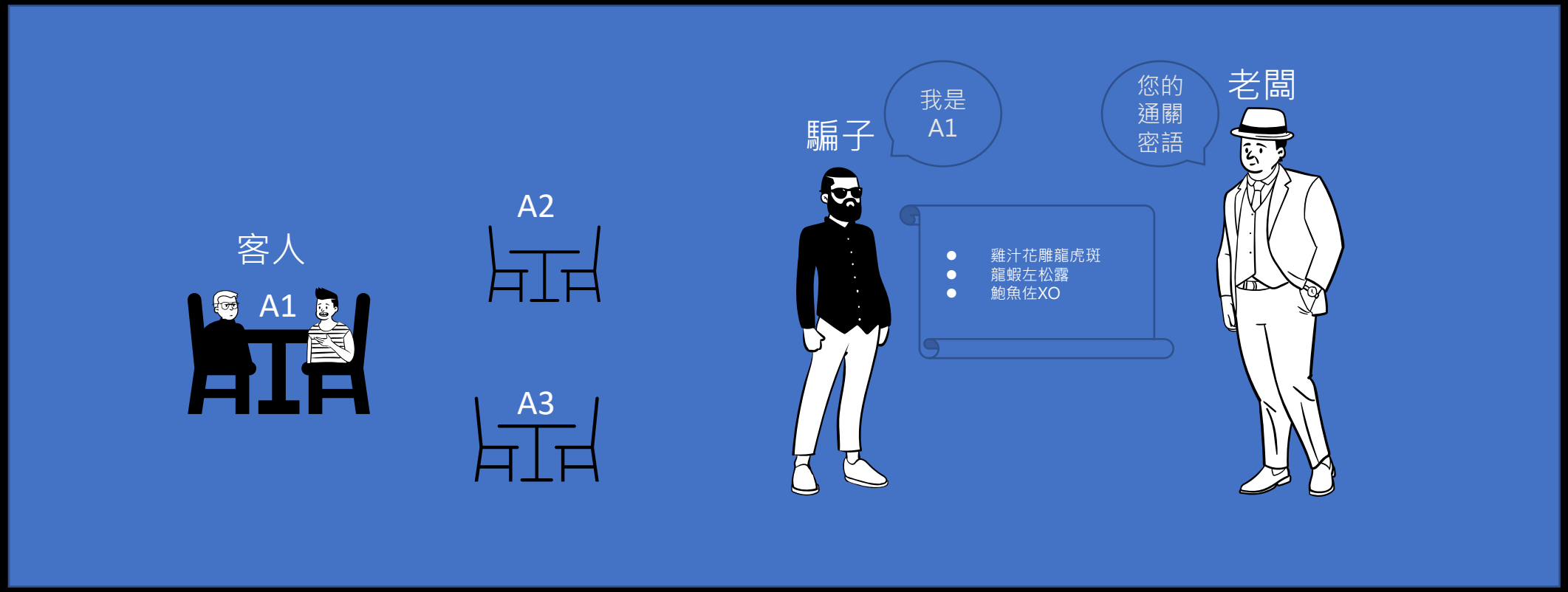
Cross Site Request Forgery
跨站請求偽造保護

Python Django網站框架與資料庫於伺服器端程式設計實務| 許季秦 | 113.03.23

CSRF 概說



CSRF 概說



CSRF 概說

- 跨站請求偽造保護是一種重要的安全機制。
- 用於防止惡意網站利用已認證用戶的流覽器發送未經授權的請求。
- CSRF 攻擊利用了用戶的身份驗證憑據（如 session cookie 等）來執行可能具有破壞性的操作。

CSRF 概說

- CSRF 保護機制透過在每個表單中包含一個 CSRF Token來實現。
- 此Token是一種隨機生成的唯一識別碼，用於驗證請求的合法性。
- 當使用者首次訪問包含表單的頁面時，Django 會在用戶的會話中生成 CSRF Token ，並將其嵌入到表單中。
- 當用戶提交表單時，Django 將檢查請求中的 CSRF Token是否與用戶會話中的Token匹配。
- 只有當這兩個權杖匹配時，請求才會被視為合法，否則將被拒絕。

https://docs.djangoproject.com/en/4.1/ref/csrf/

CSRF 概說

為了啟用CSRF 保護，需要確定以下設置已正確配置：

Settings.py

```
MIDDLEWARE = [
    'django.middleware.security.SecurityMiddleware',
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django.contrib.messages.middleware.MessageMiddleware',
    'django.middleware.clickjacking.XFrameOptionsMiddleware',
]
```

CSRF 概說

- 在每個包含表單的頁面或模板中，都要包含 {% csrf_token %} 模板標籤，以便為每個表單生成 CSRF 權杖。

例如：

```
<form action="" method="post">
    {% csrf_token %}
    <input type="text" name="username" placeholder="帳號" ><br>
    <input type="password" name="password" placeholder="密碼" ><br>
    <input type="submit" value="LOGIN" ><br>
</form>
```

{% csrf_token %}模板標籤將在表單中生成一個隱藏的 input 元素，其中包含了 CSRF Token。當用戶提交表單時，這個權杖將被包含在請求中，並由 Django 進行驗證。


Thank You