巨匠線上真人

資訊安全概論
與
網站軟體安全建構實務

同學，歡迎你參加本課程

- 請關閉你的FB 、Line等溝通工具，以免影響你上課。
- 考量頻寬，請預設關閉麥克風、攝影機，若有需要再打開。
- 隨時準備好，老師會呼叫你的名字進行互動。
- 如果有緊急事情，你必需離開線上教室，請用聊天室私訊給老師，以免老師癡癡呼喚你的名字。
- 先倒好水、上個洗手間，準備上課囉^^

課程檔案下載


巨匠電腦線上真人
開課查詢
免費體驗專區
課程總覽
專業師資
學員專區
講師專區
最新消息
您好!
登出
點數卡產品兌換
APCS檢測專區
公告專區
我的課表
IT真人課程劃位
電腦分校課程劃位
外語真人課程劃位
美語分校課程劃位
取消劃位
課程檔案下載
上課權益查詢
教學平台測試
學習諮詢
常見問題
個資維護
忘記密碼
登出
課程檔案下載
程式語言好難學?
那是因為
你還沒學過Python!
線上老師LIVE直播教學．搶先看
98%
54%
巨匠電腦真人課程

ZOOM 學員操作說明

5 查看選項/共同註記/筆（連連看）

2 共享螢幕（指導演練；點評作品）
老師須先停止共享螢幕
才能請學生共享螢幕

1 聊天

4 解除靜音

3 與會者/舉手

巨匠線上真人

資訊安全概論與網站軟體安全建構實務

第五堂：Web API 安全性設計

本堂教學重點

1. Web API 請求權限設計
2. API 防範惡意請求的對策

- 下堂教學重點

本堂教學重點

1. **Web API 請求權限設計**
2. **API 防範惡意請求的對策**

- **下堂教學重點**

1. Web API 請求權限設計

Web API 請求權限設計

- 驗證 (Authentication)
  - 使用者的身分識別。 例如，使用者帳號和密碼登入，伺服器會使用帳號及密碼驗證登入者身份。
- 授權 (Authorization)
  - 決定使用者是否有被允許執行該功能。 例如只有查詢權限，但沒有新增修改刪除的權限

Web API 請求權限設計

- OAuth 2

下階段開放資訊涉及個資，將採取更嚴格國際資安標準

資安標準上也會朝國際主流標準靠攏，舉例來說，到了第二、第三階段會採用資安要求更高的身分驗證機制，目前偏向採用國際常見的OAuth 2.0，王志峰解釋，原因是，接下來會涉及使用者資料，其中又分為身分證號碼（IDN）或是機敏性資料，像是信用卡卡號，就得考慮到要有加解密的作法。目前，已有銀行開始進行OAuth 2.0的串接驗證，國泰世華就是其中一家。王志峰提到，國泰會慢慢導入這樣的作法，讓自家金融服務能朝國際主流標準前進，他相信，各家銀行也應如此。

https://www.ithome.com.tw/news/133682

Web API 請求權限設計

- OAuth 2

陳恭表示，涉及消費者帳戶與交易資料，除了辨識第三方程式，也不能將消費者的帳號與密碼交給第三方，「目前，國際間慣用的作法是採取OAuth 2委任存取授權方式，讓TSP來存取客戶資料。」

消費者先登入原本銀行的網銀，來進行對第三方程式授權，第三方程式就可以用授權後的Token通行證來存取銀行的API，並且這類Token還需限制API存取範圍和時間，甚至要提供隨時可撤銷授權的機制。授權過程中，還需要讓消費者清楚知道，第三方的程式要求讀取哪些權限。

https://www.ithome.com.tw/news/133707

Web API 請求權限設計

- OAuth 2
  - 2007 年 10 月 OAuth Core 1.0 正式發佈
  - 讓一個應用程式在獲得用戶的授權下，訪問用戶所授權的資源
  - Oauth 旨在提供一種認證程序的規範，並不負責有關金鑰等資訊的管理
  - APP 無法取得用戶端帳號/密碼
  - Facebook Graph API、Google API

Web API 請求權限設計

- OAuth 2
  - 1) 3rd APP向銀行註冊合作，APP取得銀行提供的授權Key (表示銀行3rd API允許APP來呼叫)
  - 2) 使用者使用3rd APP進行登入作業，3rd APP向銀行API發出登入請求(銀行API 授權Key以驗證APP的呼叫)
  - 3) 銀行API將登入請求導向銀行登入作業頁面，並告知使用者3rd APP會存取哪些資料(使用者決定是否同意)
  - 4) 使用者登入後，銀行API會向3rd APP提供一個授權碼(auth code)
  - 5) 3rd APP以授權碼向銀行API換取存取金鑰(Access Token)
  - 6) 後續使用者在使用3rd APP時，3rd APP就會以該存取金鑰(Access Token)向銀行API發出請求並驗證

Web API 請求權限設計

- OAuth 2
  - 1) 3rd APP向銀行註冊合作，APP取得銀行提供的授權Key (表示銀行3rd API允許APP來呼叫)
  - 2) 使用者使用3rd APP進行登入作業，3rd APP向銀行API發出登入請求(銀行API 授權Key以驗證APP的呼叫)
  - 3) 銀行API將登入請求導向銀行登入作業頁面，...用者3rd APP會存取哪些資料(使用者決定是否同意)
  - 4) 使用者登入後，銀...de)
  - 5) 3rd APP以授權碼...
  - 6) 後續使用者在使用...cess Token)向銀行API發出請求並驗證

銀行提供給3rd APP的授權Key必須受到安全性管理

Web API 請求權限設計

- OAuth 2
  - 1) 3rd APP向銀行註冊合作，APP取得銀行提供
  - 2) 使用者使用3rd APP進行登入作業，3rd APP
  - 3) 銀行API將登入請求導向銀行登入作業頁面，
  - 4) 使用者登入後，銀行API會向3rd APP提供一個授權碼(auth code)
  - 5) 3rd APP以授權碼向銀行API換取存取金鑰(Access Token)
  - 6) 後續使用者在使用3rd APP時，3rd APP就會以該存取金鑰(Access Token)向銀行API發出請求並驗證

授權碼(auth code)
時效非常短暫的，並且該作業是透過3rd APP伺服器對銀行API伺服器間進行的溝通

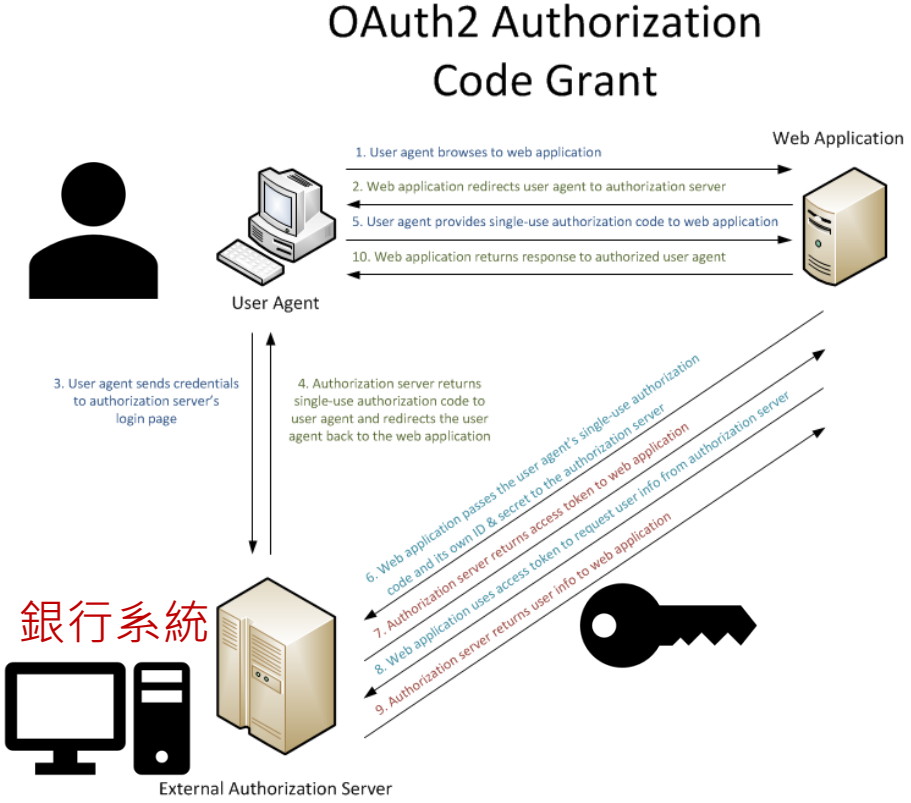
Web API 請求權限設計

- OAuth 2
  - 1) 3rd APP向銀行註冊合作，APP取得銀行提供
  - 2) 使用者使用3rd APP進行登入作業，3rd APP
  - 3) 銀行API將登入請求導向銀行登入作業頁面，
  - 4) 使用者登入後，銀行API會向3rd APP提供一個授權碼(Auth code)
  - 5) 3rd APP以授權碼向銀行API換取存取金鑰(Access Token)
  - 6) 後續使用者在使用3rd APP時，3rd APP就會以該存取金鑰(Access Token)向銀行API發出請求並驗證

存取金鑰(Access Token)
必須具備有效期限，並且可以從伺服器端進行撤銷的，期限到期後重新換發

Web API 請求權限設計

- OAuth 2

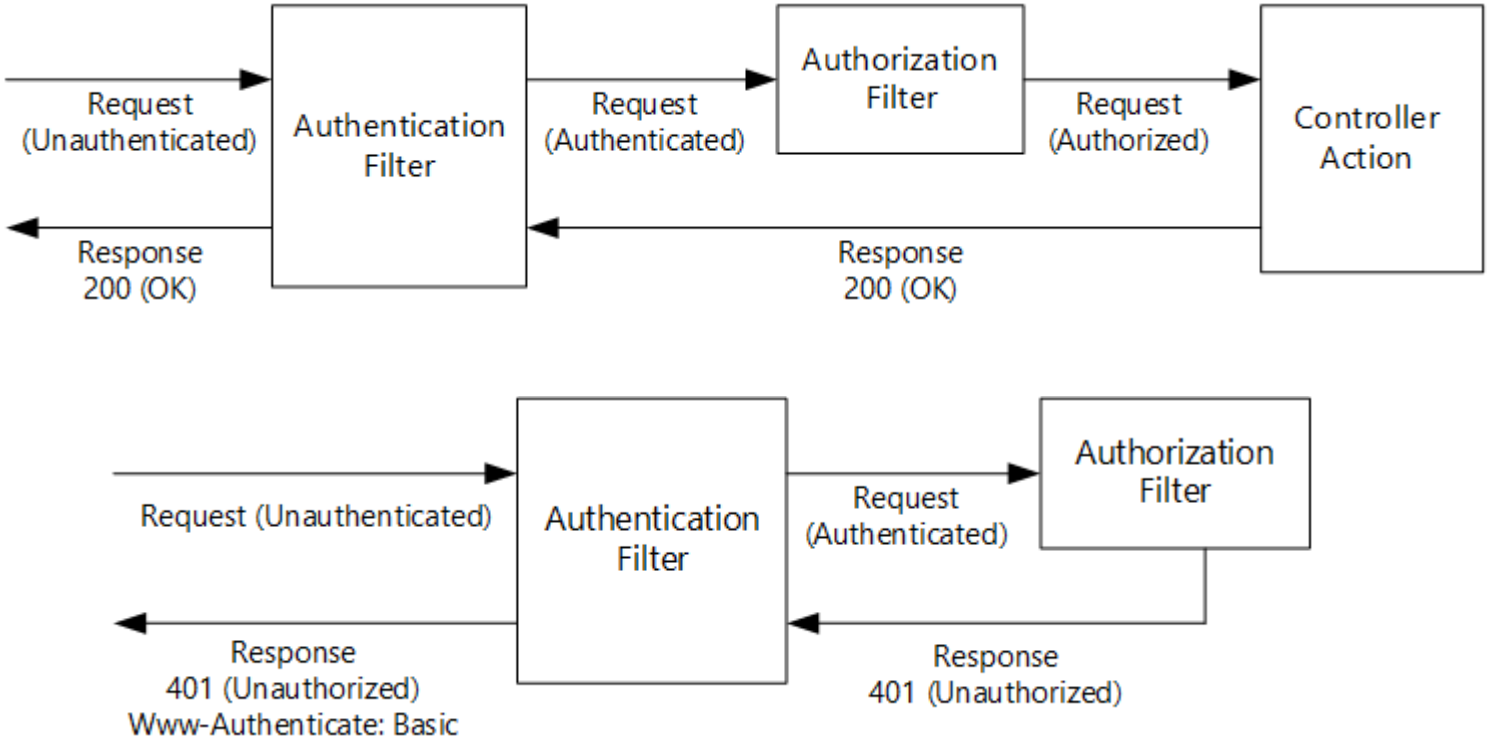


3rd APP

軟體操作示範：

實作：OAuth (Facebook)

Web API 請求權限設計



軟體操作示範：

實作：Web API 驗證與授權

本堂教學重點

1. Web API 請求權限設計
2. API 防範惡意請求的對策

- 下堂教學重點

2. API 防範惡意請求的對策

API 防範惡意請求的對策

- API 成為應用的顯學設計架構
- 根據統計有42%的系統是採用API的方式進行登入作業
- API容易受到攻擊，其中一個重要因素在於，可以大量以程式的方式進行不間斷的請求發起，或是分散到數千個機器人節點上進行攻擊

身份驗證失敗達一定次數，採取暫時遮罩對策，迫使攻擊者降低攻擊頻率和速度，以及部署攻擊上的難度

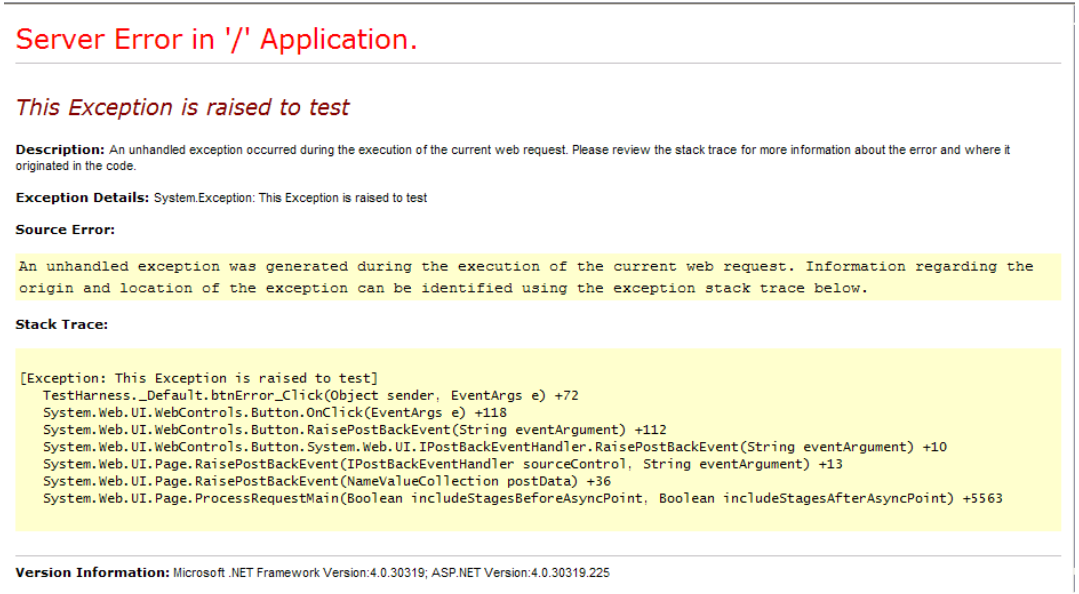
API 防範惡意請求的對策

- API 成為應用的顯學設計架構
- 根據統計有42%的系統是採用API的方式進行登入作業
- API容易受到攻擊，其中一個重要因素在於，可以大量以程式的方式進行不間斷的請求發起，或是分散到數千個機器人節點上進行攻擊

設置請求頻率閥值，例如60秒內連續重覆請求N次，暫停回應

API 防範惡意請求的對策

- API伺服器建構完善的程式異常捕捉機制，進行訊息遮蔽封裝，防止程序堆疊信息暴露



Server Error in '/' Application.

This Exception is raised to test

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Exception: This Exception is raised to test

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the
origin and location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[Exception: This Exception is raised to test]
   TestHarness._Default.btnError_Click(Object sender, EventArgs e) +72
   System.Web.UI.WebControls.Button.OnClick(EventArgs e) +118
   System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +112
   System.Web.UI.WebControls.Button.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +10
   System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +13
   System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +36
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5563
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.225

API 防範惡意請求的對策

- Web API unhandled exception
  - ExceptionFilterAttribute：受限於執行週期，僅能處理較後段的Exception
  - ExceptionLogger / ExceptionHandler：攔截範圍最大
  - ExceptionLogger 用於紀錄攔截到的例外
  - ExceptionHandler 攔截到例外後的處理

軟體操作示範：

實作：Web API unhandled exception

Web API 安全性設計

- 傳輸的安全性
- 身份識別
- 身份授權
- 例外的委善處理

Q&A

問卷

http://www.pcschoolonline.com.tw

巨匠線上真人

www.pcschoolonline.com.tw