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
巨匠電腦真人課程

ZOOM 學員操作說明


www.pcschool.com.tw
您正在觀看蘇世宗的螢幕
查看選項
原始大小
請求遠端控制
共同註記
退出全螢幕
5 查看選項/共同註記/筆（連連看）
滑鼠
文字
筆
箭頭
擦除
格式
撤銷
重做
清除
與會者 (15)
查找參會者
張齡月 (我)
婷婷
解除靜音
舉手
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
解除靜音
啟動視訊
邀請
與會者
共享螢幕
聊天
錄影
4 解除靜音
3 與會者/舉手

講師簡介

- 陳葵懋 (Ian Chen)
  - 高師大資訊教育所碩士
  - 15年業界軟體開發與架構設計經驗
  - HTML5 & JavaScript程式開發實戰作者
  - 連續8屆獲選 Microsoft MVP 最有價值技術專家
  - Microsoft TechDays 大型技術研討會講師
  - 巨匠人工智慧及程式開發課程講師
  - **http://codeian.idv.tw/**

本課程各堂教學主題

- 第一堂： SQL資料庫個資保護對策
- 第二堂：雲端網站安全性設計
- 第三堂：雲端網站安全性設計
- 第四堂：Web API安全性設計
- 第五堂：Web API安全性設計

巨匠線上真人

資訊安全概論與網站軟體安全建構實務

第一堂：SQL資料庫個資保護對策

本堂教學重點

1. 雲端資料庫與本地端資料庫的差別
2. 動態資料遮罩
3. 透明資料加密

◆ 下堂教學重點

本堂教學重點

1. 雲端資料庫與本地端資料庫的差別
2. 動態資料遮罩
3. 透明資料加密

◆ 下堂教學重點

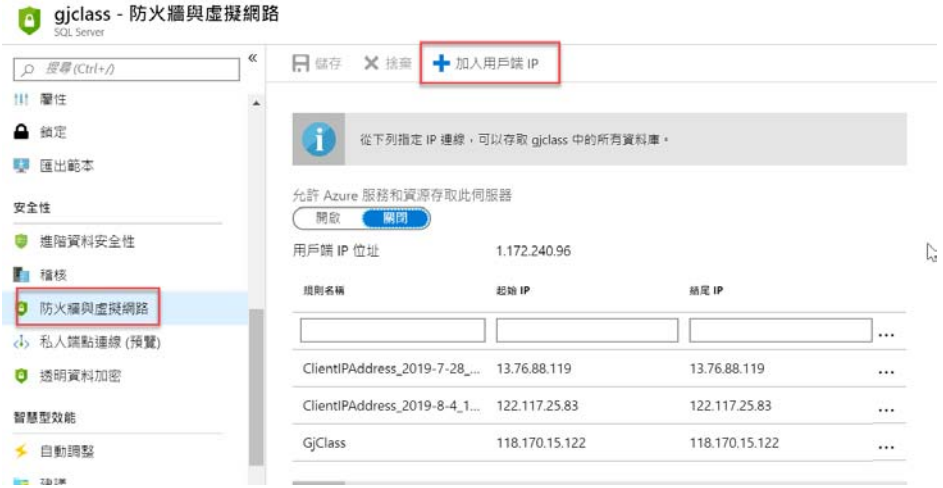
1.雲端資料庫與本地端資料庫的差別

雲端資料庫與本地端資料庫的差別

- Azure SQL Database
  - 雲端資料庫服務 - 關聯式資料庫即服務 (DBaaS)
  - 自動處理所有的 SQL 和作業系統程式碼修補和更新
- SQL Database VM
  - 虛擬機器
- 支援透明資料加密
- 支援動態資料遮罩

雲端資料庫與本地端資料庫的差別

- IP 防火牆規則
  - 伺服器層級 IP 防火牆規則
  - 資料庫層級 IP 防火牆規則



本堂教學重點

1. 雲端資料庫與本地端資料庫的差別
2. 動態資料遮罩
3. 透明資料加密

◆ 下堂教學重點

2.動態資料遮罩

動態資料遮罩

- Dynamic Data Masking
- 非資料加密處理
- 防止未經授權存取敏感性資料
- 針對未經授權的使用者遮罩機密資料
- 簡化應用程式安全性的設計和編碼
- 資料庫中的資料不會變更

動態資料遮罩

- 資料欄位建立遮罩並不會防止資料欄位更新
  - 查詢看到遮罩後的資料，但一樣可以進行資料更新
- 未經授權(UNMASK)使用者進行敏感資料遮罩
  - (sysadmin 、 db_owner 除外)
  - UNMASK 權限可擷取未遮罩的資料
- SQL Server 2016 (13.x) 、Azure SQL Database 支援

動態資料遮罩

- default()
  - 依指定欄位的資料類型進行完整遮罩
  - 字串 - XXXX
  - 數值 - 0
  - 日期 - 01.01.1900
  - ALTER COLUMN [Gender] ADD MASKED WITH (FUNCTION = 'default()')

動態資料遮罩

- email()
  - aXXX@XXXX.com
  - ALTER COLUMN Email ADD MASKED WITH (FUNCTION = 'email()')

動態資料遮罩

- Random()
  - 隨機遮罩
  - 用於任何數值類型
  - ALTER COLUMN [salary] ADD MASKED WITH (FUNCTION = 'random(1, 12)')

動態資料遮罩

- Partial
  - 自訂字串
  - 公開前N個及最後N個字母，其餘自訂填補字串
  - ALTER COLUMN [mobileno] ADD MASKED WITH (FUNCTION = 'partial(1,"XXXXXXX",1)')

動態資料遮罩

- 查詢目前資料庫有哪些資料欄位已設定遮罩
  - SELECT c.name, tbl.name as table_name, c.is_masked, c.masking_function FROM sys.masked_columns AS c JOIN sys.tables AS tbl ON c.[object_id] = tbl.[object_id] WHERE is_masked = 1;

動態資料遮罩

- 遮罩並非加密，使用推斷手法，仍可以推論出實際資料值

SQLQuery1.sql - l...ind (webuser (53))*

```
select FirstName,Salary from Employees where Salary>=5000 and Salary<=10000
```

100 %

結果 訊息

	FirstName	Salary
1	Nancy	9518
2	Andrew	9817
3	Margaret	3494
4	Steven	7093
5	Michael	8500
6	Robert	9671
7	Laura	2666
8	Anne	4551

動態資料遮罩

- Azure SQL Database

軟體操作示範：

實作：動態資料遮罩

本堂教學重點

1. 雲端資料庫與本地端資料庫的差別
2. 動態資料遮罩
3. 透明資料加密

- 下堂教學重點

3.透明資料加密

透明資料加密

- 透明資料加密 (Transparent Data Encryption,TDE)
- 加密資料檔和記錄檔
- 發生實體檔案 (如磁碟機或備份磁帶) 遭竊的狀況時，惡意人士無法採用還原或附加資料庫方式瀏覽資料
- 執行資料和記錄檔即時 I/O 加密和解密
- 寫入磁碟前先加密，並在讀入記憶體時進行解密
- TDE 並不會讓加密之資料庫的大小增加

透明資料加密

- SQL 2008 支援
- Enterprise Edition支援
- Database Encryption Key (DEK)
  - DEK 對稱金鑰，用儲放在master中的憑證或EKM所保護的非對稱金鑰所加密而建立
  - Extensible Key Management(EKM)，外部金鑰管理模組

透明資料加密

- 系統管理員或 dbmanager 角色的成員，才能啟用透明資料加密 (TDE)
- ALTER DATABASE [AdventureWorks] SET ENCRYPTION ON;
- ALTER DATABASE [AdventureWorks] SET ENCRYPTION OFF;
- SELECT [name], [is_encrypted] FROM sys.databases;
  - 1 表示加密的資料庫
  - 0 表示未加密的資料庫

透明資料加密

- Azure SQL Database
  - 設所有新部署的 Azure SQL 資料庫會啟用 TDE
  - 舊版資料庫必須手動啟用 TDE
  - 預設設定是以內建伺服器憑證保護資料庫加密金鑰(加密演算法是 AES 256)

透明資料加密

- Azure SQL Database

透明資料加密

- Azure SQL Database

透明資料加密

- SQL Database
  - USE master
  - 建立資料庫主要金鑰
    - CREATE MASTER KEY ENCRYPTION BY PASSWORD = ‘your pwd’

透明資料加密

- SQL Database
  - USE master
  - 建立保護 TDE Key的憑證
    - CREATE CERTIFICATE MySQLServerCert　WITH SUBJECT = 'Certificate to protect TDE key'

透明資料加密

- SQL Database
  - USE master
  - 建立伺服器憑證的備份
    - BACKUP CERTIFICATE certname TO FILE ='path_to_file' WITH PRIVATE KEY (FILE ='path_to_private_key_file', ENCRYPTION BY PASSWORD ='encryption_password')
    - TO FILE = '*path_to_file*' , FILE= 'path_to_private_key_file'
      指定儲存憑證的檔案之完整路徑，包括檔案名稱。 此路徑可以是本機路徑或通往網路位置的 UNC 路徑。 如果只指定檔案名稱，檔案將會儲存在執行個體的預設使用者資料夾

透明資料加密

- SQL Database
  - USE your db
  - 建立加密金鑰
    - CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_128 ENCRYPTION BY SERVER CERTIFICATE MySQLServerCert;
  - 預設加密演算法AES_128

透明資料加密

- SQL Database
  - USE your db
  - 啟用加密
    - ALTER DATABASE Northwind SET ENCRYPTION ON
  - 關閉加密
    - ALTER DATABASE Northwind SET ENCRYPTION OFF

透明資料加密

- 搬移加密資料庫
  - 憑證與私鑰必須一併搬移

```
--Other Server Create CERTIFICATE from source file
--CERTIFICATE name 可以不同
--DECRYPTION BY PASSWORD 密碼必須和備份時指定的密碼一樣
CREATE CERTIFICATE SQLServerCertAnother
FROM FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\DATA\your certificate file '
WITH PRIVATE KEY
(
    FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\your priveate key file',
    DECRYPTION BY PASSWORD = 'your backup pwd'
);
GO
```

軟體操作示範：

實作：透明資料加密

資料欄位加密

- 資料欄位加密
  - SQL 2005 支援
  - 加密資料表中的特定資料欄位

資料欄位加密

- 使用內建加密函數
  - EncryptByPassPhrase
    - Triple DES(TDEA)

```
DECLARE @EncryptKey nvarchar(128);
SET @EncryptKey = 'ian!01';

--加密
update Employees set EncryptSalary=EncryptByPassPhrase(@EncryptKey, CONVERT(varchar(50),salary));

--解密
select EncryptSalary,CONVERT(varchar(50),DecryptByPassphrase(@EncryptKey,EncryptSalary)) as DecryptSalary,Salary from Employees
```

資料欄位加密

- 憑證（Certicate）加密金鑰（Key）
- 利用金鑰（Key）加密欄位資料（Data）

資料欄位加密

- 建立Database Master Key

```
--建立Database Master Key
IF EXISTS(SELECT * FROM sys.symmetric_keys WHERE name = '##MS_DatabaseMasterKey##')
  DROP MASTER KEY ;
ELSE
  CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'your pwd';
GO
```

資料欄位加密

- 建立憑證

```
-- 建立憑證
CREATE CERTIFICATE MyColumnCert
   WITH SUBJECT = 'Column Data Protect',
   START_DATE = '2019/1/1',
   EXPIRY_DATE = '2029/12/31'
GO
```

資料欄位加密

- 建立用憑證加密的對稱金鑰

```
-- 建立用憑證加密的對稱金鑰
CREATE SYMMETRIC KEY MyColumnKey
  WITH ALGORITHM = AES_256                -- 加密演算法
  ENCRYPTION BY CERTIFICATE MyColumnCert;    -- 利用憑證加密MyColumnKey
GO
```

資料欄位加密

- 欄位加密
  - 透過憑證開啟對稱金鑰
  - 使用金鑰進行資料加密
  - 關閉對稱金鑰

```
--透過憑證開啟對稱金鑰
OPEN SYMMETRIC KEY MyColumnKey DECRYPTION BY CERTIFICATE MyColumnCert
GO

--使用金鑰進行資料加密
UPDATE Employees
SET encryptsalary = EncryptByKey(Key_GUID('MyColumnKey'),convert(varchar(20),salary))
GO

--關閉對稱金鑰
CLOSE ALL SYMMETRIC KEYS
GO
```

資料欄位加密

- 欄位解密
  - 透過憑證開啟對稱金鑰
  - 使用金鑰進行資料解密
  - 關閉對稱金鑰

```
--透過憑證開啟對稱金鑰
OPEN SYMMETRIC KEY MyColumnKey DECRYPTION BY CERTIFICATE MyColumnCert
GO

--使用金鑰進行資料解密
select salary,encryptsalary,convert(varchar(20),DecryptByKey(encryptsalary)) from Employees


--關閉對稱金鑰
CLOSE ALL SYMMETRIC KEYS
GO
```

軟體操作示範：

實作：資料欄位加密

Q&A

下堂教學重點

- 雲端服務與雲端虛擬機器的差別
- 雲端網站安全性設計與OWASP防範對策

問卷

http://www.pcschoolonline.com.tw

巨匠線上真人

www.pcschoolonline.com.tw