《資訊管理與資通安全》

一、金融科技（Fintech）已掀起全球熱潮，其運用資訊科技讓金融服務變得更有效率。請說明何謂行動支付？何謂第三方支付？並分別舉例現有應用加以說明。（25分）

試題評析	金融科技是這一兩年竄起的當紅題目，同學除了對於基本理論要有掌握外，每次看到新出現的金融相關議題要思考其屬於哪一種分類。 此題算是中規中矩，針對每種支付方式要能夠盡可能詳述其差異，包含監管單位、優缺點……等，除了基本的名詞解釋外，需要對於所舉的例子有更進一步的說明，才可以在此題拿到不錯的分數。
考點命中	《高點‧高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁56-57。

答：

(一)行動支付

1.監管單位：金管會。

2.指目前可以透過行動裝置進行付款的服務。根據2012年國際清算銀行（Bank for International Settlements）所發表的零售支付工具創新報告中，對於行動支付的定義為：「舉凡以行動存取設備（如：手機及平板電腦等）透過無線網路，採用語音、簡訊或近場無線通訊（NFC）等方式所啟動的支付行為均屬之」。

3.例如：Apple pay即為一種行動支付。銀行會和蘋果公司溝通，透過Apple的手機當做載具，把銀行的信用卡資訊內嵌到手機載具上，其支付還是透過銀行自己的信用卡，故交易流程與付款方式還是一樣，只是銀行需要額外給蘋果公司手續費。

對銀行而言，除了可以透過此方法吸引更多iPhone用戶使用自己家的信用卡外，銀行也可以取得更多消費者有關的資訊，例如：使用哪支手機支付、App store的交易頻率……等。日後銀行可以透過此資訊當做行銷的參考資料。而目前Apple pay是台灣少數採用NFC技術的行動支付之一。

(二)第三方支付

1.監管單位：經濟部。

2.存在於買家與賣家間的第三方業者，在中間進行收款與付款的交易模式。在第三方支付中，其交易方式為當進行交易時，買家會先把錢交給第三方業者，等到買家收到貨品且確認無誤時，第三方業者才會將款項交給賣家。

其優缺點為：

優點	缺點
1. 付款與退款方便且快速。 2. 具有交易擔保之功能（買方收到貨品且確認後才會將款項交給賣家），可降低詐騙發生機率。 3. 減少個人資料外洩。 4. 有些會提供個人化的帳務管理機制。 5. 透過國際型的第三方支付公司，可以降低中小型賣家進行跨國交易之門檻。	1. 目前礙於法令，許多第三方支付都有許多實際執行上之限制，例如：支付寶目前買家支付上限是每日3萬元。 2. 第三方支付提供者成為駭客覬覦之對象。 3. 有可能變成洗錢的溫床。

3.由中國竄起的支付寶所提供的其中一項功能即為第三方支付，而此類的支付其利潤主要有兩個：

(1)交易手續費：通常此類支付，當交易完成後，會對商家收取一定額度的手續費，但是當此手續費太高時，商家會將此類費用轉嫁給消費者。

(2)利息收入：從消費者手中獲取的款項到在付給商家的這段期間，可以賺取利息費用，時間越久，利息越多。

二、(一)請試舉出7種資料庫安全威脅。（10分）

(二)伺服器虛擬化已成為企業建置機房的趨勢。請說明何謂虛擬化（Virtualization）？並舉出4

項虛擬化的優點。（15分）

試題評析	資料庫的安全威脅一直是長青題，需要對資料庫的基本架構與部署方式有基本認知，考題會從各種角度去考學生的理解度，但是只要圍繞在基本觀念上，即可得到高分。 此題的第一部分屬於基本題型，考生可能一開始會無法想到這麼多點，但是只要從資料庫的建置到最後的部署一一把流程記起來，針對每個流程都有可能產生對應的威脅，在答題上需要把對應的解決方法也提出會比較適當。 第二題的虛擬化則是只要把握基本概念即可，答題上如果只回答定義會略顯不足，盡量詳細描述虛擬化技術，才可獲得較好的分數。
考點命中	《高點‧高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁2-5（課堂補充）、51。

答：

(一) 常見之資料庫安全威脅：

1.不當的部署

在開發過程中不當的程序與不適合的測試方式都是造成資料庫漏洞的常見原因。有些企業在建置資料庫時，會針對其功能進行優化，有時候反而在優化的過程中暴露出更多的漏洞，所以在建置完到部署之前需要對資料庫進行全面性的安全檢查，來避免資料庫的漏洞與找出攻擊者可能使用的非預期行為。

2.伺服器資料洩漏

大部分的資料庫都需要具有隨時連網功能，故也成為駭客最想要攻擊的目標之一，而在傳遞資料時若沒有加密，則可能造成資料在傳遞時洩漏重要資訊，甚至是與資料庫伺服器有關的設定資訊。

3.SQL注入

攻擊者在網頁可以輸入資料的地方嘗試填入不合法的語法，其目的為猜測網頁設計者背後撰寫語法的邏輯，利用該欄位搭配自己的語法組合成一個可以造成對網頁有害的攻擊指令，像是推測欄位數，table的名字，SQL的版本資訊，試著去拼湊輸入一條SQL指令，輕則刪掉資料庫，重則竊取全部的個資。系統在開發時需要注意：

(1)不要將錯誤訊息給管理者以外的人看到，以避免攻擊者獲得更多的攻擊資訊。

(2)對於使用者個人帳號權限需要有控管機制。

(3)需要對使用者所有輸入的字串進行合法性檢查。

4.權限控管問題

權限的設置上常見的問題為：

(1)員工被賦予過多的權則

(2)合法的權限未被授權或是濫用

要避免以上兩種事情發生，應讓每個員工帳號在權限分發時，採用最小權限原則，應只給每個層級的員工其基本的訪問權限，嚴格控管員工對於資料存取的能力。

5.基礎設施問題

當資料庫所使用的基礎設施有問題時，就會造成駭客利用此漏洞進行攻擊，最危險的情況可能會讓整台主機的控制權都被駭客奪取。要解決基礎設施問題最好的辦法是定期更新，讓系統保持在最新的版本上。

6.濫用資料庫工具

在開發過程中有可能為了測試或是功能開發到一半而終止，造成資料庫中有不需要的套件或工具，而因為其主要功能沒有在繼續使用，導致沒有定期更新，此時這種工具類的程式最有可能變成駭客攻擊的目標。最好的解決辦法是要定期的把不必要的套件與工具刪除。

7.資料庫中的不當行為

資料庫的不一致性有可能導致漏洞的產生，故開發人員要非常清楚各種可能影響到資料庫正常運作的威脅，然後透過日誌與資訊的追蹤來防止類似的事件發生。

(二) 為一種資源管理的方式與技術，指將電腦的硬體資源（CPU、記憶體、磁碟、網路……等），抽象化後呈現出來並可以分割或組合成一個或多個電腦組態環境，並藉由此方法來打破實體結構間不可分割的障礙，使用者可以用更有運算力的組態設定來計算，且這些資源的虛擬化是不受資源的限制，可以隨時擴充與移除。

虛擬化的技術大致上分為：

1.全虛擬化：虛擬機器完整的模擬硬體底層，包含CPU、記憶體……等，透過事先設定的硬體溝通介面，可以讓作業系統與虛擬硬體間的互動有如跟真正的硬體互動般執行工作。

2.超虛擬化：透過修改操作系統部分訪問權限的程式碼以便讓系統與虛擬機器監視器直接互動。在此技術中部分硬體介面以軟體的形式提供給使用者的操作系統。

3.部分虛擬化：相對於全虛擬化，只虛擬化部分的硬體，在使用此技術時如果使用者的操作系統沒有經過特定的修改是無法直接在此虛擬化技術上執行。

4.操作系統虛擬化：在伺服器端使用輕量級的虛擬技術，透過創建多個虛擬的系統操作實例來隔離不同的線程，線程間彼此不知道對方的存在。

其好處有：

1.降低成本：虛擬化技術可以讓一台機器有如多台機器一樣提供給不同使用者操作，也可以充分的使用到沒有被完整利用的資源，使用者在初期可以減少採購成本。

2.管理簡化：虛擬化技術的使用者可以依照市場與業務的需求，即時的增加或減少機器量，因而提高使用率，在管理上不用維護過多的不必要硬體。而且透過主控台還可以看到所有實體機器與虛擬機器的狀態與組態，方便系統管理者一次管理多台機器。

3.提升效率：可以減少伺服器的數量，降低管理人員的負擔，增加IT的管理效率。

4.環保：減少伺服器數量與增加機器使用率，讓整體資源的效率更好，可以幫助企業節省消耗支出。

三、請說明虛擬實境（Virtual Reality, VR）與擴增實境（Augmented Reality, AR）。請說明透過各種體感元件來模擬各種人類的動作，這種以假亂真是屬於上面那一種應用？另請說明寶可夢（Pokemon GO）是屬於上面那一種應用？（25分）

試題評析	實境技術隨著科技發展，近幾年是商業發展的重點，可想而知也會變成考題常出的方向，此題除了需要了解各種實境的基本定義外，對於常出現的遊戲、應用……等，都要多思考其所代表的意義與分類，像是此題的寶可夢就是結合實例的一個例子。 答題上掌握兩個原則，第一是對基本概念的闡述要完整，第二是針對每種題目所問到的例子除了分類外，還要盡可能描述其概念與對應實境的原因，即可為整題拿到不錯的分數。

答：

(一)虛擬實境：

透過電腦技術模擬出一個高度真實感的空間，讓穿戴特殊顯示裝置的使用者感覺好像身處在現實生活一般，使用者可以藉由操作控制器來與此虛擬空間互動，但目前的技術在觸覺上有非常大的瓶頸，無法讓人的腦波與電腦結合，達到人可以感覺出電腦所模擬的任何知覺。

目前較常見的虛擬實境技術之一為結合智慧型手機，主要的原因為智慧型手機效能明顯提高、螢幕加大與畫質提升。其使用方式為將手機插入到頭戴式裝置中，而目前最大的瓶頸除了硬體效能外，最大的問題為互動方面缺乏額外的控制器輔助，導致無法有高度的沉浸效果。

而題目所說的模擬人體動作，達到以假亂真即是此分類，透過模擬人類的動作，並在虛擬世界中呈現與互動即是此類技術的重點。

(二)擴增實境：

由虛擬實境所衍生出來的技術，指將電腦的資訊疊合到現實世界中，其目的是希望在現實的世界中添加虛擬的物件，讓人們可以在現實世界中與虛擬的物件互動，此技術也是最早應用在行銷與商業領域中。

虛擬的互動也僅限於遊戲中，現在題目所說的寶可夢即是此類，透過在現實世界中抓虛擬的神奇寶貝，並且只在遊戲中互動，即是擴增實境的主軸。

而此兩者的差異為虛擬實境企圖透過電腦技術來取代現實世界，而擴增實境則是基於現實世界中創造虛擬的物件來與使用者互動。

四、請回答下列有關瀏覽器相關的資訊安全問題：

(一)請舉出五項瀏覽器對採用SSL網站的安全檢查措施。（15分）

(二)請說明XSS攻擊，並說明可防範的方式。（10分）

試題評析	此題目的第一題為較少見的題型，考生需要對於SSL的檢查措施在實務上有基本的認知才會比較容易作答，考試當下把握住SSL的基本概念與驗證方式，套用在瀏覽器上即可。 第二題的攻擊方式也是常會出現的考題，對於防範方法除了課堂所說的之外，也要對網站的架設有一定的認知，才可以答出較為不一樣的答案，也是此題拿到高分的訣竅。

答：

(一)

1.網站的網址開頭是否為「https://」，如果有s，代表使用者與網站間已經有加密過，傳輸的內容較難被得知。

2.檢查網頁裡面的連結是否都是用https來傳輸。

3.針對SSL憑證做相對應的檢查，像是「憑證的有效期限」、「憑證名稱是否有誤」與「憑證的發送者是否是合格的發行者」。

4.使用者也可以針對網站自行檢查已獲得驗證的組織名稱，若組織名稱不符合或是憑證過期，其會顯示錯誤與警告。

5.網站會向瀏覽器證明其身分，瀏覽器會要求網站使用可信任機構所核發的憑證。

(二)跨站腳本攻擊（Cross-Site Scripting, XSS）

惡意使用者將程式碼注入到網頁中（常發生在有類似留言板功能的網頁），其他使用者在觀看此網頁時就會受到惡意程式碼的影響。這些惡意網頁程式碼通常是JavaScript，但實際上也可以包括Java，VBScript，ActiveX，Flash，或者甚至是普通的HTML。攻擊成功後，攻擊者可能得到更高的權限、私密網頁內容、對談和cookie等各種內容。

其防護方法有：

1.檢查使用者的輸入是否有特殊字元：不要直接使用用戶所輸入的資料，要先確認其內容是否合法，甚至加密後再儲存起來。

2.針對每個欄位皆有最大長度的限制：避免攻擊者在欄位內存入相關攻擊語法。

3.對cookie資料加密：如果直接拿取cookie中的值，並直接使用，則非常有可能造成漏洞。

4.不要把網頁的"ValidateRequest"屬性設定為false：一般的論壇因為可以允許使用者輸入html的tag，所以會將此欄位設定成false。此值如果是true時，當送出的資料中有html tag，則會出現錯誤，故論壇形式的網頁如果沒有特別的判斷機制，很容易被當成攻擊的目標。

5.了解駭客的攻擊手法，針對各種攻擊手法個別防範。