**IOT 安全期末報告**

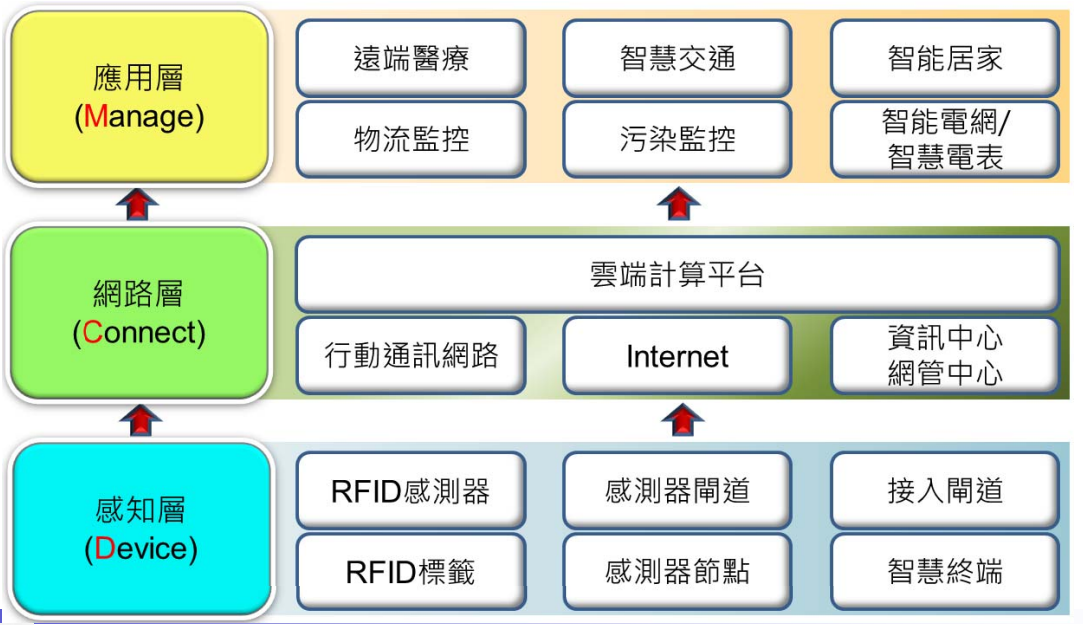
1. **IOT架構**

物聯網(Internet of Things, IoT)架構可分為三個階層，如下：

1.感知層(Device)：針對不同的場景進行感知與監控，主要可分為感測技術與辨識技術。感測技術是使智慧物件具有感測環境變化或物體移動的能力。常被用來嵌入物體的感測元件，包括紅外線、溫度、濕度、亮度、壓力、三軸加速度等感測器；辨識技術如RFID的元件，將RFID的標籤嵌入於物體，便使物體可以記錄及回報自己的身份或狀態。

2.網路層(Connect)：將感知層收集到的資料傳輸至網際網路，建構無線通訊網路上。可分為語音傳輸為主的｢電信網路｣ (TeleCom)與資料傳輸為主的｢數據網路｣ (DataCom)。

3.應用層(Manage)：物聯網與行業間的專業進行技術融合，會根據不同的需求開發出相應的應用軟體，如智慧電表。

****

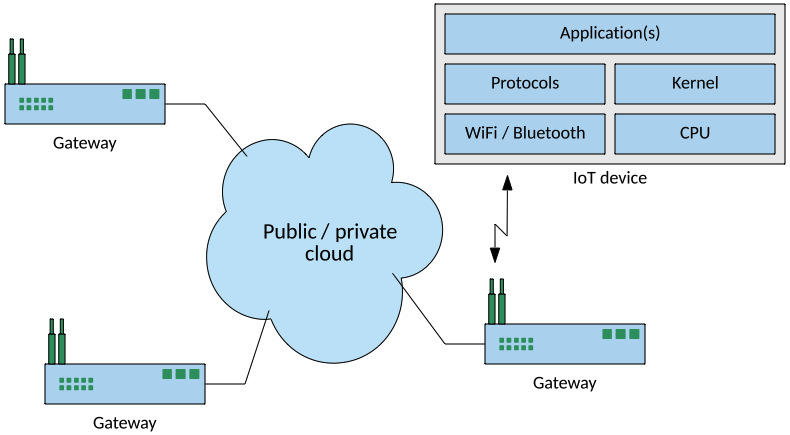
**IOT架構**

IoT 生態系統劃分為 3 個層級（參見）：

數據中心（公有或私有）

網關（中間通信網關）

端點設備（分佈式 IoT 設備）



**IOT生態系統提供多個攻擊層級**

1. **IOT安全挑戰**

IOT十大威脅

1. 不安全的網頁介面

**情境1:** Web界面顯示“忘記密碼”功能，在輸入無效賬戶時會通知攻擊者該賬戶不存在。一旦識別出有效賬戶，如果沒有賬戶鎖定控制存在，則密碼猜測可以無限期地開始。

Account john@doe.com does not exist.

**情境2:**  Web界面受跨站腳本攻擊。

http://xyz.com/index.php?user=<script>alert(123)</script> ... Response from browser is an alert popup.

在上述情況下，攻擊者能夠輕鬆確定帳戶是否有效，並且還能夠確定該網站受跨站點腳本影響

1. 憑證或授權不足

**情境1:** 界面只需要簡單的密碼。

Username = Bob; Password = 1234

**情境2:** 通過網絡傳輸時，用戶名和密碼保護不佳。

Authorization: Basic YWRtaW46MTIzNA==

在上述情況下，攻擊者能夠輕鬆猜出密碼，或者能夠在憑證跨越網絡並對其進行解碼時捕獲憑證，因為憑證僅受Base64編碼保護。

1. 不安全的網路服務

**情境1:** 模糊攻擊導致網絡服務和設備崩潰.

GET %s%s%s%s%s%s%s%s%s%s%s%s%s%s%s HTTP/1.0

**情境2:**可能在用戶不知情的情況下通過UPnP向互聯網打開端口

Port 80 and 443 exposed to the internet via a home router.

在上述情況下，攻擊者可以通過HTTP GET完全禁用設備或通過port 80或port443通過互聯網訪問設備。

1. 缺少傳輸加密或完整性的驗證

**情境1:**雲端介面只使用HTTP.

http://www.xyzcloudsite.com

**情境2:**用戶名和密碼通過發送網路發送

http://www.xyzcloud.com/login.php?userid=3&password=1234

在上述情況下，由於缺少傳輸加密，攻擊者有能力清晰地查看敏感數據。

1. 隱私問題考量

**情境1:** 收集個人數據。

Date of birth(生日), home address(地址), phone number(電話號碼), etc.

**情境2:** 收集財務信用卡或銀行資訊.

Credit card data(新用卡資料) and bank account information(銀行帳戶資訊).

在上述情況下，任何數據的暴露都可能導致身份盜用或賬戶損害。

1. 不安全的雲端服務介面

**S情境1:** 密碼重置指示帳戶是否有效

Password Reset "That account does not exist."

**情境2:** 通過網絡傳輸時，用戶名和密碼保護不佳.

Authorization: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3

在上述情況中，攻擊者能夠確定一個有效的用戶帳戶，或者能夠在他們通過網絡並對其進行解碼時捕獲憑證，因為憑證只使用Base64編碼進行保護。

1. 不安全的行動裝置應用介面

**情境1:** 密碼重置表示帳戶是否存在.

Password Reset "That account does not exist."

**情境2:** 通過網絡傳輸時，用戶名和密碼保護不佳.

Authorization: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3

在上述情況中，攻擊者能夠確定一個有效的用戶帳戶，或者能夠在他們通過網絡並對其進行解碼時捕獲憑證，因為憑證只使用Base64編碼進行保護。

1. 安全組態的不足

**情境1:**無法執行較強密碼強度策略

Admins and users are allowed to create passwords for their accounts.

(管理員和用戶可以為其帳戶創建密碼)

**情境2:**無法啟用靜態數據加密

Password or other sensitive data stored on the device may not be encrypted.

(存儲在設備上的密碼或其他敏感數據可能未被加密。)

In the cases above, the attacker is able to use the lack of these controls to get access to user accounts with weak passwords or access data at rest which has protection.

在上述情況中，攻擊者能夠使用缺少這些資訊的設備，用於訪問具有較弱密碼強度的用戶帳戶或訪問具有保護的靜止數據。

1. 不安全的軟體和硬體

**情境1:**更新文件透過HTTP.

http://www.xyz.com/update.bin

**情境2:** 更新文件未加密，可以查看人可讀的數據。

�v�ñ]��Ü��Qw�û]��ˇ3DP�Ö�∂]��ˇ3DPadmin.htmadvanced.htmalarms.htm

在上述情況下，攻擊者能夠捕獲更新文件或捕獲文件並查看其內容。

10. 缺乏實體安全措施

**情境1:** 該設備可以很容易地拆卸，存儲是用未加密的SD卡。

SD card can be removed and inserted into a card reader to be modified or copied.

(可以取出SD卡並將其插入讀卡器進行修改或複制)

**情境2:** 設備上有USB port。

Custom software could be written to take advantage of features such as updating via the USB port to modify the original device software.

(可以編寫自定義軟體利用如通過USB port更新等功能來修改原始設備軟件)

在這兩種情況下，攻擊者都可以訪問原始設備軟體並進行修改或簡單地複製特定目標數據。

2018年將面臨物聯網的10種安全威脅。

1. 殭屍網絡和DDoS攻擊

2016年9月Mirai殭屍網絡時才首次意識到物聯網安全威脅。據一些人估計，Mirai感染了約250萬個物聯網設備，包括打印機、路由器和聯網攝像頭。殭屍網絡的創建者用它來發動分佈式拒絕服務(DDoS)攻擊，包括攻擊網絡安全博客KrebsonSecurity。實際上，攻擊者利用被Mirai感染的所有設備，企圖同時連接到目標網站，希望搞垮服務器，防止任何人訪問網站。

自Mirai首次見諸媒體以來，攻擊者已發動了其他物聯網殭屍網絡攻擊，包括Reaper和Hajime。專家表示，未來可能會有更多的此類攻擊。

2. 遠程拍錄

黑客有可能在主人毫不知情的情況下，黑入物聯網設備，拍錄主人的活動。

維基解密網站披露的文檔表明，這個情報機構早就知道物聯網設備的眾多零日攻擊，但沒有透露這些漏洞，原因是希望利用這些漏洞祕密錄下會揭露美國敵人的活動的對話。除了Android和iOS智能手機的漏洞外，文檔還提到了智能電視的漏洞。很顯然，犯罪分子也可能會利用這些漏洞實施不法勾當。

3. 垃圾郵件

2014年1月發生了有史以來已知針對物聯網設備的一起攻擊，攻陷了10多萬個聯網設備，包括電視機、路由器和至少一台智能電冰箱，每天發送30萬封垃圾郵件。攻擊者從任何一個設備發送的消息也就10條，因而很難阻止或查明攻擊源頭。

這起早期的攻擊絕非最後一起。由於Linux.ProxyM物聯網殭屍網絡，去年秋天物聯網垃圾郵件攻擊繼續肆虐。

4. APT

近年來，高級持續性威脅(APT)已經成為安全專業人員關注的一大問題。APT的背後是一羣本領高超的攻擊者，比如國家或企業，它們發動複雜的網絡攻擊，難以預防或對付。比如説，摧毀伊朗核離心機的Stuxnet蠕蟲和2014年索尼影業黑客事件就歸咎於敵對國家。

隨着更多的關鍵基礎設施接入互聯網，許多專家警告，APT可能會對電網、工業控制系統或其他聯網系統發起物聯網攻擊。有人甚至警告，恐怖分子可能會發動使全球經濟陷於癱瘓的物聯網攻擊。

5. 勒索軟件

勒索軟件在家用PC和企業網絡上已變得非常普遍。現在專家表示，勒索軟件攻擊者開始盯上智能設備只是個時間問題。安全研究人員已經演示了能夠將勒索軟件安裝到智能恆温器上。比如説，他們可以將温度調高到95度，拒絕調回到正常温度，除非受害者同意支付用比特幣支付的贖金。他們還能夠對聯網的車庫門、車輛甚至家電發動類似的攻擊。

6. 數據竊取

獲取敏感數據仍然是網絡攻擊的主要目標之一，比如客户名稱、信用卡號碼、社會保障號碼及其他個人身份信息。據波耐蒙研究所聲稱，數據泄露事件讓公司平均損失362萬美元，相當於每條被竊取的記錄141美元。在想方設法入侵企業網絡或家庭網絡的犯罪分子看來，物聯網設備就是一條全新的攻擊途徑。比如説，如果一個保護不當的物聯網設備或傳感器連接到企業網絡，這可能為攻擊者提供了進入網絡的新方法，有可能找到他們覬覦的寶貴數據。

7. 入侵住宅

隨着智能鎖和智能車庫開門器變得更常見，網絡犯罪分子也更有可能成為現實世界中的小偷。面對手頭擁有高級工具和軟件的犯罪分子，如果沒有得到妥善的保護，家庭系統可能岌岌可危。令人不安的是，安全研究人員已證明，很容易黑入幾家不同廠商的智能鎖，智能車庫門的安全性似乎並沒有大大提高。

8. 偷偷與孩子溝通

物聯網安全最令人不安的故事之一就是黑入嬰兒監視器。一對夫婦曾發現，一個陌生人不僅用他們的嬰兒監視器窺視其三歲大的兒子，還一直通過監視器與孩子説話。這位母親曾聽到陌生的聲音説：“醒來，小男孩，爸爸在找你”，孩子説他嚇壞了，因為有人在晚上通過監視器與他説話。

隨着更多的兒童設備和玩具連接到互聯網，這種可怕的情景可能會變得更司空見慣。

9. 遙控車輛

由於車輛變得更智能，並連接到互聯網，它們也容易受到攻擊。黑客已證明，他們可以控制吉普車，將空調設到最高數值、換廣播電台、開啟雨刷器，最終讓車輛停下來。這個新聞導致車企召回了140萬輛車，但是這個漏洞背後的白帽研究人員表示，他們發現了另外的安全漏洞，克萊斯勒為召回車輛所打的補丁堵不了這些漏洞。雖然專家表示，汽車業在確保車輛安全方面有所改進，但幾乎可以肯定的是，攻擊者會在聯網汽車中發現新的漏洞。

10. 人體攻擊

有時候物聯網不僅僅包含對象，還包括聯網醫療設備植入到體內的人。電視連續劇《Homeland》的劇集圍繞利用植入體內的醫療設備搞暗殺活動展開，美國前副總統Dick Cheney對於這種場景深為擔憂，於是他關閉了植入其體內的除顫器的無線功能。這種類型的攻擊在現實生活中還沒有發生，但隨着更多的醫療設備成為物聯網的一部分，這種可能性仍然存在。

IoT 資安威脅的例子:

在特定的街景地形，無人機莫名自動墜機砸傷甚至砸死人。

劫持廠房工業用 IoT 裝置：去年夏天，美國研究人員對發力發電公司進行資安演習，以物理入侵方式（破壞門鎖）輕鬆進入該公司旗下一風力發電廠的網路機房，以小小一台Raspberry PI 電腦，關掉五個風力發電廠的所有風力發電機電力輸配異常。

讓特定有慢性病的重要人物失能甚至遇害— 駭入印表機而印出錯誤的醫療指示與病歷，使得一個人被醫死在手術台上。

SCADA （supervisory control and data acquisition）工控系統

 Stuxnet：利用 Simens WinCC/PCS7系统的4個 漏洞， 2010年國

際頭條新聞。其專門針對鈾濃縮設施，使離心機失控從而造成納坦

茲的工廠遭受物理破壞，成功使正在用來濃縮鈾的1000台離心機癱

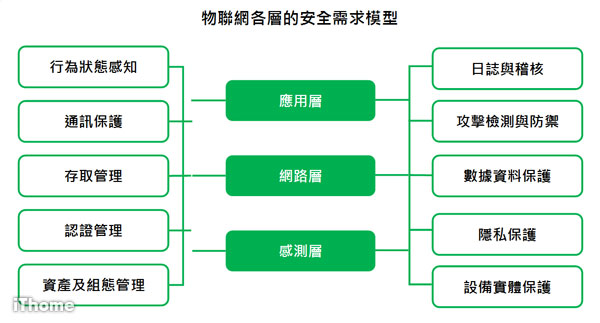
瘓。

 Havex： 感染SCADA系統的工業控制系統，這種惡意代碼可能通

過使用一個按鍵就能夠使水電大壩停運、核電站過載，甚至關閉一

個國家的電網。7/16， 駭客操控工控系統，攻擊歐洲能源公司，偷

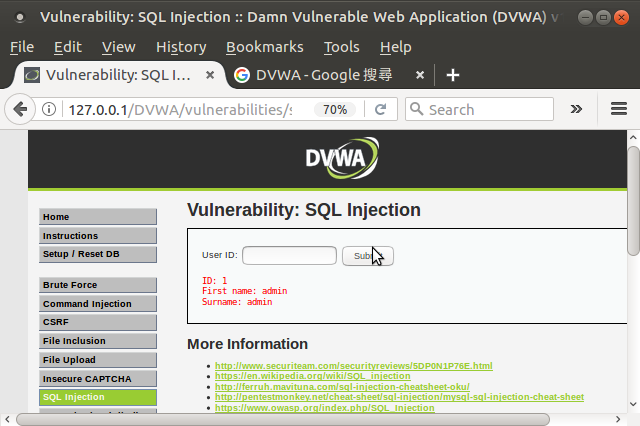
走汽油及燃煤。

****

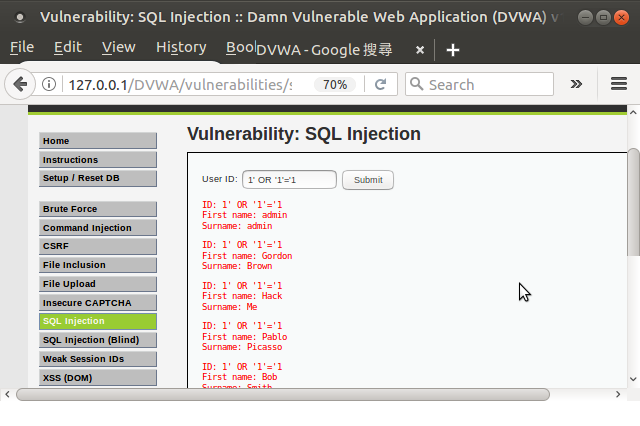
**IOT安全需求模型**

1. **IOT安全演示**

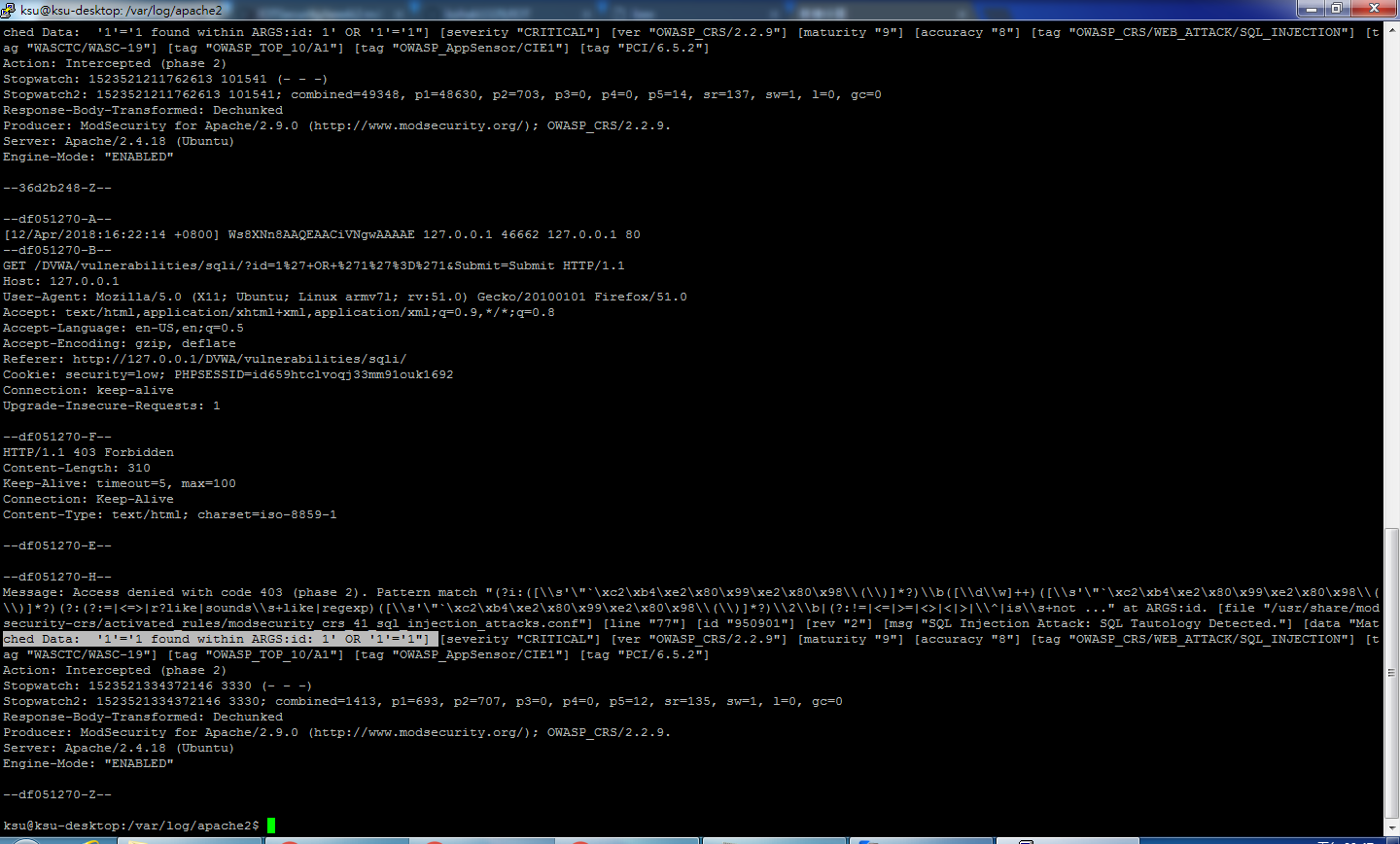
**SQL injection演示**

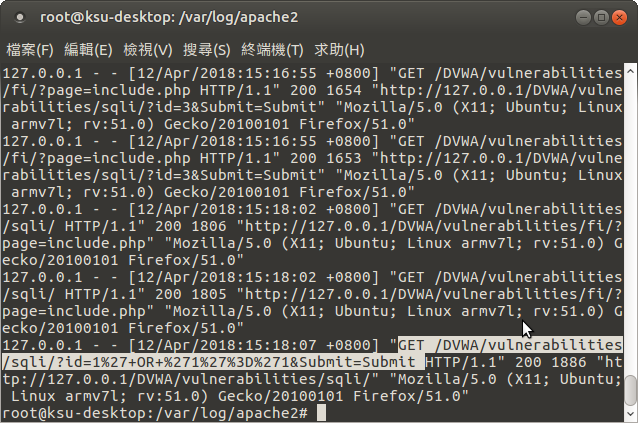
****

**輸入1後呈現**

****

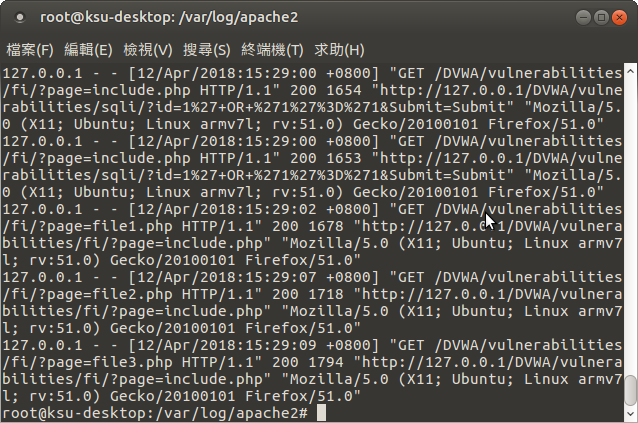
**SQL注入攻擊**

****

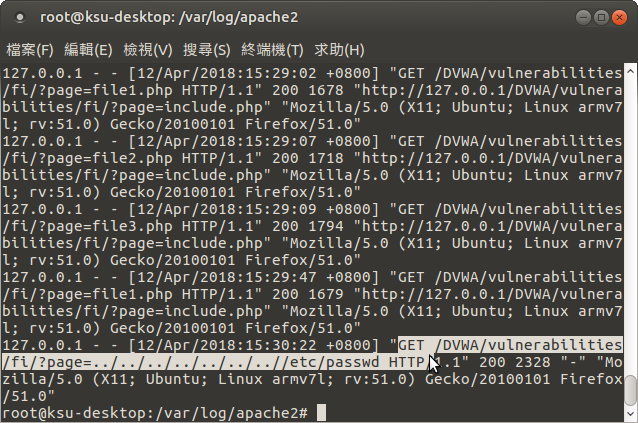
**找到sql injection攻擊**

**sql injection\_log access**

**File Inclusion演示**

****

**File Inclusion**

****

**File Inclusion密碼**

**4.未來方向**

IOT安全議題將越來越聚焦在裝置和資料的管理和分析，隨著裝置監控和偵測需求的成長，雲端資安服務也將成為IOT安全的一環。

在未來一定都是跟IOT息息相關，所以我們可以去了解資訊安全中各項議題

並且在雲端資安服務也要去做各項研究。

**為何需要SecureSDLC？**

資安事件頻傳

作業系統漏洞

資料庫配置錯誤

SQL Injection

XSS

軟體漏洞導致資安風險

漏洞年年成長

修補措施及中後期處理、被動反應，且越後期修補成本越高

**SSDLC 機制具些許差異性，仍可歸納出一致性的重點，摘述如下：**

**SSDLC 整合骨幹**: SSDLC 周期中，涉及許多工具，CI（Continuous Integration，持續整合）扮演核心整合平台的角色，Jenkins 為金融企業中普遍採用的一種 CI 工具。

**版本管理機制**: 版本管理平台已為金融產業必備的平台，而政府機關這方面卻顯不足，採用 SVN 版控工具為較大宗，而近年 GIT 有明顯增加趨勢。

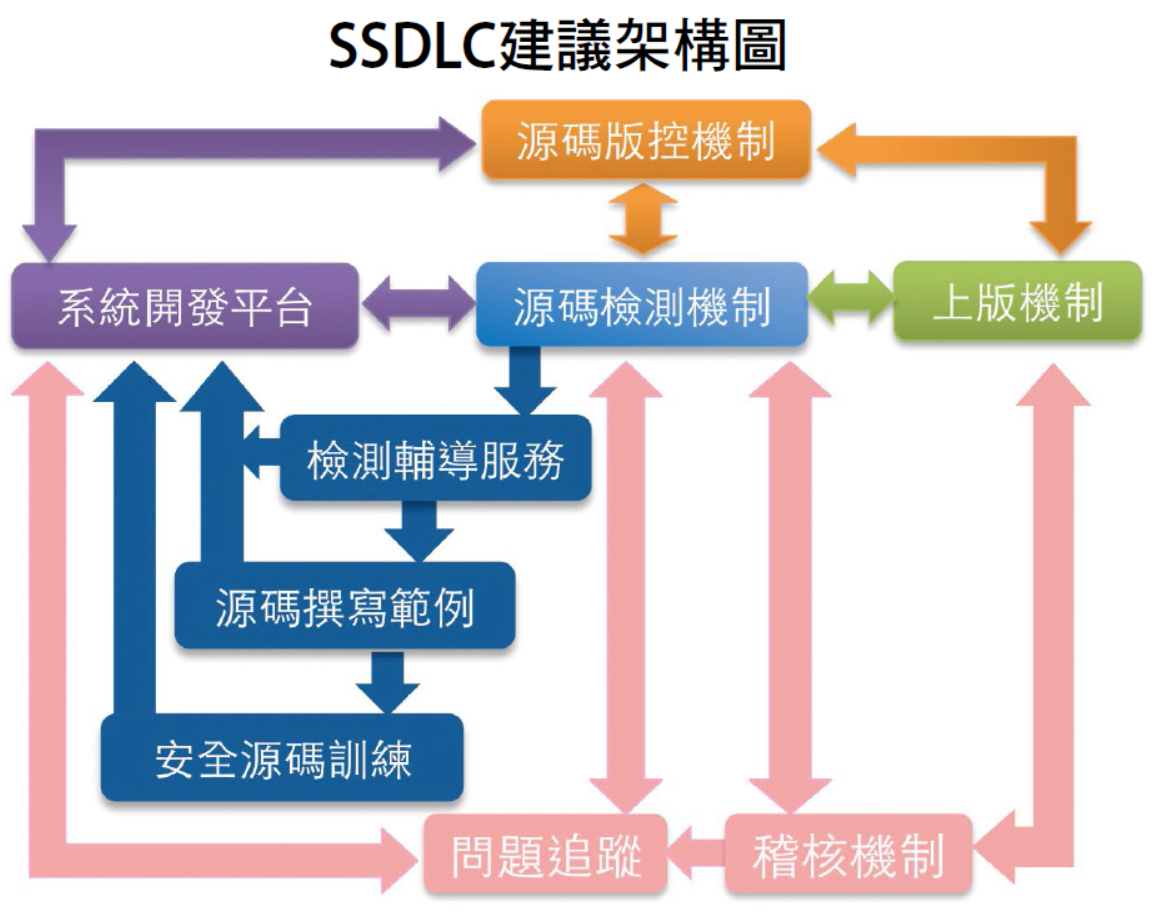
**源碼檢測(白箱)與弱點掃描(黑箱)工具**:

黑白箱檢測工具已是金融企業必備的工具，同時整合上述工具，構成自動化檢測機制。由於近年來，對行動 APP 應用系統的黑白箱檢測需求有快速增加趨勢。

不分版本均可檢測：企業內部與委外廠商的應用系統開發環境版本差異，某些檢測工具與環境版本息息相關，造成系統檢測與建置時困擾，建議選擇不分版本均可檢測的工具。

**自動上版作法**: 當應用系統風險已可完整監控時，上版流程自動化已成為精簡人力與減少人力疏失的利器，惟上版失敗復原及無瑕上版機制應謹慎規劃。

**變更管理:**營運期間，掌握需求變更項目對程式的衝擊程度，重要卻耗時耗力，金融銀行以需求變更系統與版控機制的整合，達成這個管理需求，同時利用版本系統的特性，動態掌握前後版程式更替情形，滿足主管機關合規要求。

****

**SSDLC架構**