

109年公務人員特種考試司法人員、法務部
調查局調查人員、國家安全局國家安全情報
人員、海岸巡防人員及移民行政人員考試試題

考試別：司法人員

等別：三等考試

類科組：檢察事務官電子資訊組

科目：資通安全

考試時間：2小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

一、資料隱碼 (SQL Injection) 仍是至今常見的網路攻擊，此攻擊包含很多種手法，請回答下列問題：

- (一)請說明顛覆邏輯 (Subverting Logic) 以及盲目注入 (Blind Injection) 兩種手法的意義。(15分)
- (二)參數化查詢 (Parameterized Query) 是公認防禦 SQL Injection 攻擊的有效方法，請說明其防禦原理。(10分)

二、SSL (Secure Socket Layer) 協定是非常重要的網際網路安全協定，請回答：

- (一)SSL 的工作原理為何？請詳細說明之。(10分)
- (二)請解釋何謂 SSL VPN (Virtual Private Network)？和 IPsec VPN 相比，其優缺點為何？(10分)
- (三)現今網站多採用 SSL 協定，此對資通安全管理造成那些安全威脅？試申論之。(5分)

三、資料外洩防護 (Data Loss Prevention / Data Leak Prevention, DLP) 是近年來受到重視的資訊安全議題，請問：

- (一)DLP 的意義為何？請詳細說明。(5分)
- (二)實現 DLP 的技術有那些？請詳細說明。(10分)
- (三)請比較 DLP 和 DRM (Digital Right Management) 功能的異同。(10分)

四、數位鑑識 (Digital Forensics) 是網路安全防禦的重要手段之一，請回答：

- (一)何謂數位鑑識？請詳細說明其意義，然後列出並解釋從事數位鑑識時該遵循那些原則？(15分)
- (二)電腦犯罪者為了避免被偵測，常會採取反鑑識作為。反鑑識的方法可分為幾類？請各舉例說明之。(10分)