自定義評估結果 12/7/2022

問題一

tb787631.CISSPPT3E.c08.053

軟件開發人員通常使用以下哪一種工具來與存儲在代碼存儲庫中的代碼進行交互和管理？

A.grep _

B.git _

C.lsof _

D. 海灣合作委員會

你回答正確！

`git` 是一種版本管理工具，開發人員經常使用它來與代碼存儲庫（例如 GitHub 託管的代碼庫）進行交互。`grep` 是一個命令行工具，用於搜索文件中的特定內容。`lsof` 是用於列出系統上打開的文件的命令。`gcc` 是用於將源代碼轉換為可執行代碼的 C 語言編譯器。

問題 2

tb787631.CISSPPT3E.c08.029

Tom 正在評估與他管理的數據庫相關的安全風險。檢查用戶訪問控制，他確定用戶可以訪問表中與他們的許可相匹配的個人記錄，但如果他們拉取多條記錄，

則該事實集合的分類高於任何單獨的事實的分類，並且超過了允許訪問。Tom 發現了什麼類型的問題？

A. 推論

B、SQL 注入

C. 多級安全

D、聚合

您回答錯誤。

聚合是一個安全問題，當事實集合的分類高於任何獨立事實的分類時，就會出現這種情況。當攻擊者可以將不太敏感的信息拼湊在一起並使用它們來導出更敏感的信息時，就會出現推理問題。SQL 注入是一種 Web 應用程序漏洞。多級安全是一種系統控制，允許同時處理不同分類級別的信息。

問題三

tb787631.CISSPPT3E.c08.072

Miguel 最近完成了對其組織用於處理敏感信息的應用程序的滲透測試。在測試期間，他發現了一種情況，攻擊者可以利用計時條件來操縱軟件，從而允許他執行未經授權的操作。以下哪一種攻擊類型適合這種情況？

A、SQL 注入

B. 跨站腳本

C.傳遞哈希

D. TOC/TOU

你回答正確！

檢查時間到使用時間 (TOC/TOU) 攻擊利用系統驗證授權和軟件使用該

授權執行操作之間的時間差異。這是競爭條件攻擊的一個例子。提到的其

他三種攻擊不依賴於精確的時間。

問題四

tb787631.CISSPPT3E.c08.068

Tareck 的組織使用了大量的 COTS 軟件。他最近在對他的業務至關重要的 COTS 軟件包的代碼中發現了一個重大的緩衝區溢出漏洞。Tareck 最有可能糾正這個問題的方法是什麼？

A. 與他的軟件開發團隊一起修改代碼。

B. 通知供應商並請求補丁。

C. 部署入侵防禦系統。

D. 更新防火牆規則。

你回答正確！

在使用現成的商業 (COTS) 軟件時，客戶通常無法訪問源代碼，必須依

靠供應商發布安全補丁來糾正漏洞。其他控制措施，如入侵防禦系統和防

火牆，可能能夠幫助緩解問題，具體取決於缺陷的性質，但它們不會糾正

它。

問題 5

tb787631.CISSPPT3E.c08.049

Chris 正在審查他計劃在其組織中使用的開源應用程序的代碼。他找到了此處顯示的代碼摘錄：

```
int myarray[10];
```

```
myarray[10] = 8;
```

正在發生什麼類型的攻擊？

A. 不匹配的數據類型

B、溢出

C、SQL 注入

D、隱蔽通道

你回答正確！

這是稱為差一錯誤的特定類型緩衝區溢出的示例。代碼的第一行定義了一

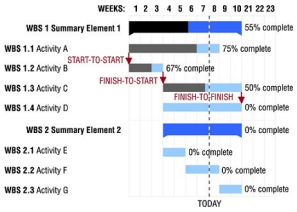
個包含 10 個元素的數組，編號為 0 到 9。代碼的第二行嘗試將一個值放

入數組的第 11 個元素（記住，數組從 0 開始計數！），這會導致溢出 。

問題 6

tb787631.CISSPPT3E.c08.070

David 正在為軟件開發工作制定項目進度表，他看到了此處顯示的圖表。這是什麼類型的圖表？



A. 工作分解結構

B、功能需求

C. PERT 圖

D、甘特圖

您回答錯誤。

圖中顯示的圖表是甘特圖，顯示了不同活動的建議開始和結束日期。它是

基於工作分解結構（WBS）開發的，工作分解結構是基於功能需求開發

的。計劃評估審查技術 (PERT) 圖表將項目進度表顯示為一系列編號的

節點。

問題 7

tb787631.CISSPPT3E.c08.078

以下哪一項變更管理流程是由用戶而不是開發人員發起的？

A. 變更請求
B. 變更控制
C. 釋放控制
D. 設計審查

你回答正確！

請求過程以用戶發起的功能請求開始。變更和發布控制由尋求實施變更的

開發人員發起。設計審查是開發人員在完成設計後啟動的變更批准流程的

一個階段。

問題 8

tb787631.CISSPPT3E.c08.069

下列關於軟件測試的陳述，哪一項是正確的？

A. 靜態測試適用於運行時環境。

B. 靜態測試執行代碼分析。

C. 動態測試使用自動化工具，而靜態測試則不用。

D. 靜態測試是比動態測試更重要的測試技術。

你回答正確！

靜態測試以離線方式執行代碼分析，而不實際執行代碼。動態測試在運行時環境中評估代碼。靜態和動態測試都可能使用自動化工具，並且都是重要的安全測試技術。

問題 9

tb787631.CISSPPT3E.c08.062

Tomas 在他的應用程序日誌中發現了一行，該行似乎與進行目錄遍歷攻擊的嘗試相對應。他認為攻擊是使用 URL 編碼進行的。該行內容如下：

%252E%252E%252F%252E%252E%252Fetc/密碼

%252E 值代表什麼字符？

一種。 。

B、

C。；

D. /

你回答正確！

在 URL 編碼中，. 字符替換為 %252E，/ 字符替換為 %252F。您可以在

日誌條目中看到這一點，其中 ../../ 的預期模式被替換為%252E%252E

%252F%252E%252E%252F。

問題 10

tb787631.CISSPPT3E.c08.064

以下哪一項不是敏捷軟件開發過程的原則？

A. 歡迎不斷變化的需求，即使是在開發過程的後期。

B. 最大限度地減少未完成的工作量是必不可少的。

C. 清晰的文件記錄是衡量進展的主要措施。

D. 圍繞有動力的個人構建項目。

你回答正確！

敏捷宣言包括 12 條軟件開發原則。其中三個被列為答案選擇：最大限度

地減少未完成的工作量是必不可少的，圍繞積極的個人構建項目，並在整

個開發過程中歡迎不斷變化的需求。然而，敏捷並不認為清晰的文檔是衡

量進展的主要標準。相反，工作軟件是衡量進展的主要標準。

問題 11

tb787631.CISSPPT3E.c08.016

Kayla 最近完成了對她的團隊開發的軟件的全面風險分析和緩解審查，並確定了三個持續存在的問題：

1. 跨站腳本
2. SQL 注入
3. 緩衝區溢出

這些問題確定了她的團隊工作中最嚴重的缺陷是什麼？

A. 缺乏 API 安全性

B.錯誤處理不當

C. 不正確或缺少輸入驗證

D. 源代碼設計問題

你回答正確！

這些問題中的每一個都是由不正確或缺少輸入驗證引起的，可以通過正確處理輸入來解決。在許多情況下，這可以使用已經內置到開發人員正在使用的語言或框架中的庫或方法來完成。

問題 12

tb787631.CISSPPT3E.c08.045

Alexis 的組織最近轉向軟件開發的 CI/CD 方法，他們打算在這種方法中加速支持其網站的代碼部署。他們使用這種方法可以期望達到的最合理的頻率是多少？

A. 每月部署

B. 每週部署

C. 日常部署

D. 數百次日常部署

您回答錯誤。

當組織採用持續集成/持續交付 (CI/CD) 方法進行軟件開發時，他們可能會非常快速地部署代碼。事實上，一些組織每天使用這種方法將新代碼部署到生產環境中數百次甚至數千次。

問題 13

tb787631.CISSPPT3E.c08.006

阿什莉 (Ashley) 正在調查一次攻擊，該攻擊破壞了她的一個用戶的帳戶。在攻擊中，攻擊者利用用戶瀏覽器中的信任關係，強制向第三方站點提交經過身份驗證的請求。最有可能發生什麼類型的攻擊？

A、XSS

B、CSRF

C、SQL 注入

D.會話劫持

你回答正確！

跨站點請求偽造（XSRF 或 CSRF）攻擊通過嘗試強制向第三方站點提

交經過身份驗證的請求來利用站點對用戶瀏覽器的信任。會話劫持攻擊試

圖竊取以前經過身份驗證的會話，但不會強制瀏覽器提交請求。SQL 注

入通過 Web 應用程序直接攻擊數據庫。跨站點腳本使用反射輸入誘騙用

戶的瀏覽器執行來自受信任站點的不受信任代碼。

問題 14

tb787631.CISSPPT3E.c08.066

Neal 正在使用 DynamoDB 數據庫。該數據庫的結構不像關係數據庫，但允許 Neal 使用鍵值存儲來存儲數據。DynamoDB 是什麼類型的數據庫？

A.關係數據庫

B、圖數據庫

C. 層次數據庫

D、NoSQL 數據庫

您回答錯誤。

鍵值存儲是 NoSQL 數據庫的一個示例，它不像傳統數據庫那樣遵循關

係或層次模型。圖數據庫是 NoSQL 數據庫的另一個例子，但它使用節

點和邊來存儲數據，而不是鍵和值。

問題 15

tb787631.CISSPPT3E.c08.071

Barry 是一名軟件測試員，他正在使用他的公司開發的新遊戲應用程序。他在智能手機上玩遊戲，以便在最能模擬普通最終用戶的環境中進行測試，但他在進行測試時參考了源代碼。Barry 正在進行什麼類型的測試？

A、白框

B、黑匣子

C、藍框

D、灰盒

你回答正確！

在灰盒測試中，測試人員從用戶的角度評估軟件，但在進行測試時可以訪

問源代碼。白盒測試也可以訪問源代碼，但從開發人員的角度執行測試。

黑盒測試從用戶的角度進行，但無法訪問源代碼。藍盒是一種電話黑客工具，而不是一種軟件測試技術。

問題 16

tb787631.CISSPPT3E.c08.075

從安全角度來看，以下哪一種故障管理方法是最保守的？

A. 失敗打開
B. 失敗緩解
C. 清除故障
D. 失敗關閉

你回答正確！

故障關閉方法可防止在系統安全故障期間發生任何活動，並且是最保守的故障管理方法。故障開放採用相反的理念，在安全控制失敗的情況下允許所有活動。故障清除和故障緩解不是故障管理方法。

問題 17

tb787631.CISSPPT3E.c08.080

Ursula 是一名政府網站開發人員，她最近創建了一個提供財產記錄的公共應用程序。她想讓其他開發人員可以將其集成到他們的應用程序中。Ursula 可以創建什麼來使開發人員能夠最輕鬆地直接調用她的代碼並將輸出集成到他們的應用程序中？

A. 對像模型

B、數據字典

C、原料藥

D、主鍵

你回答正確！

雖然 Ursula 在她的開發工作中肯定會使用對像模型、數據字典和主鍵，

但外部開發人員不能直接使用它們來訪問她的代碼。應用程序編程接口

(API) 允許其他開發人員從他們自己的代碼中調用 Ursula 的代碼，而無

需了解 Ursula 的實現細節。

問題 18

tb787631.CISSPPT3E.c08.058

Haley 正在審查她的組織創建的代碼，以防止其可能暴露於 Web 應用程序漏洞。以下哪種情況可能使應用程序最容易受到跨站點腳本 (XSS) 攻擊？

A. 輸入驗證

B. 反射輸入

C.未打補丁的服務器

D. 混雜的防火牆規則

你回答正確！

跨站點腳本 (XSS) 攻擊可能會利用 Web 應用程序中反射輸入的使用，

其中一個用戶提供的輸入會顯示給另一個用戶。輸入驗證是一種用於防止

XSS 攻擊的控件。XSS 不需要未打補丁的服務器或任何允許訪問 Web

應用程序的防火牆規則。

問題 19

tb787631.CISSPPT3E.c08.031

Vivian 想聘請一名軟件測試員進來，從用戶的角度評估一個新的 Web 應用程序。以下哪項測試最能模擬該觀點？

A、黑匣子

B、灰盒

C、藍框

D、白盒

你回答正確！

黑盒測試從不了解系統實現的先驗知識開始，模擬用戶視角。白盒和灰盒

測試分別在測試之前提供系統的全部和部分知識。藍盒子是一種電話黑客

工具，不用於軟件測試。

問題 20

tb787631.CISSPPT3E.c08.079

Teagan 希望更好地保護他的組織免受數據庫推理攻擊。以下哪一項技術是對抗這些攻擊的有效對策？

A. 輸入驗證
B. 參數化
C. 多實例化
D. 服務器端驗證

你回答正確！

多實例化允許在數據庫中以不同的分類級別存儲多個不同的信息片段，以

防止攻擊者推斷出任何關於信息缺失的信息。輸入驗證、服務器端驗證和

參數化都是用於防止 Web 應用程序攻擊的技術，對推理攻擊無效。

問題 21

tb787631.CISSPPT3E.c08.037

請參考以下場景：

- Linda 正在她公司網站上的一個用戶論壇上查看帖子，當她瀏覽某個帖子時，屏幕上的對話框中會彈出一條消息，上面寫著“提醒”。她查看帖子的源代碼並找到以下代碼片段：

```
<script>alert('Alert');</script>
```

Linda 的留言板上肯定存在什麼漏洞？

A. 跨站腳本

B. 跨站請求偽造

C、SQL 注入

D. 認證不當

你回答正確！

消息論壇顯然容易受到跨站點腳本 (XSS) 攻擊。Linda 在郵件中發現的

代碼是嘗試執行跨站點腳本的明確示例，她收到的警告框表明漏洞存在。

該網站還可能容易受到跨站請求偽造、SQL 注入、不正確的身份驗證和

其他攻擊，但場景中沒有提供這方面的證據。

問題 22

tb787631.CISSPPT3E.c08.039

請參考以下場景：

- Linda 正在她公司網站上的一個用戶論壇上查看帖子，當她瀏覽某個帖子時，屏幕上的對話框中會彈出一條消息，上面寫著“提醒”。她查看帖子的源代碼並找到以下代碼片段：

```
<script>alert('Alert');</script>
```

Linda 與供應商溝通並確定沒有補丁可用於修復此漏洞。以下哪一種設備最能幫助她保護應用程序免受進一步攻擊？

A、VPN

B、WAF

C、DLP

D、入侵檢測系統

你回答正確！

Web 應用程序防火牆 (WAF) 位於 Web 應用程序之前，監視潛在的惡意 Web 攻擊，包括跨站點腳本。然後他們會阻止該流量到達 Web 應用程序。入侵檢測系統 (IDS) 可以檢測到攻擊，但無法採取措施阻止它。

DLP 和 VPN 解決方案無法檢測 Web 應用程序攻擊。

問題 23 #####

tb787631.CISSPPT3E.c08.042

Lauren 想對她正在處理的應用程序使用軟件審查流程。如果她是一名與團隊其他成員工作時間不同的遠程工作者，以下哪個流程最有效？

A、繞過

B.結對編程

C. 團隊審查

D.費根檢查

您回答錯誤。

傳遞審查通常通過電子郵件或使用中央代碼審查系統完成，允許開發人員異步審查代碼。結對編程需要兩名程序員一起工作，一個編寫代碼，另一個審查和跟踪進度。團隊審查通常在一個小組中完成，而 Fagan 檢查是一個正式的審查過程，涉及開發人員和團隊使用正式過程審查代碼。

問題 24

tb787631.CISSPPT3E.c08.084

以下哪種類型的人工智能試圖使用複雜的計算來複製人類思維的部分功能？

A. 決策支持系統

B. 專家系統

C. 知識庫

D. 神經網絡

你回答正確！

神經網絡試圖使用複雜的計算技術來模擬人類思維的行為。知識庫是專家

系統的組成部分，旨在獲取和重新應用人類知識。決策支持系統旨在為執

行標準程序的人員提供建議，並且通常由專家系統驅動。

問題 25 #####

tb787631.CISSPPT3E.c08.085

組織在軟件能力成熟度模型 (SW-CMM) 的哪個級別引入基本生命週期管理流程？

A.初始

B、可重複

C.定義

D、託管

您回答錯誤。

在第 2 級，即 SW-CMM 的可重複級，組織引入了基本的生命週期管理

流程。開始以有組織的方式重用代碼，並且期望從類似項目中獲得可重複

的結果。該級別的關鍵過程域包括需求管理、軟件項目計劃、軟件項目跟

踪和監督、軟件分包合同管理、軟件質量保證和軟件配置管理。

問題 26

tb787631.CISSPPT3E.c08.048

Alyssa 的團隊最近實施了一個新系統，該系統從各種不同的日誌源收集信息，分析這些信息，然後觸發自動行動手冊以響應安全事件。哪個術語最能描述這項技術？

A. SIEM

B. 日誌存儲庫

C、IPS

D.翱翔

您回答錯誤。

安全信息和事件管理 (SIEM) 系統確實會關聯來自多個來源的信息並執行分析，但它們無法提供自動劇本響應。這就是安全編排、自動化和響應 (SOAR) 平台的領域。入侵防禦平台的範圍更有限，允許根據 IPS 本身執行的分析來阻止流量。日誌庫只是收集日誌信息，並不進行分析。

問題 27

tb787631.CISSPPT3E.c08.002

Darren 正在進行威脅搜尋活動，並希望尋找殭屍網絡妥協指標。以下哪些是攻擊者利用殭屍網絡的常見方式？（選擇所有符合條件的。）

A. 挖礦加密貨幣

B. 進行暴力攻擊

C. 掃描易受攻擊的系統

D. 進行中間人攻擊

你回答正確！

殭屍網絡用於各種惡意目的，包括掃描網絡以查找易受攻擊的系統、對其他系統進行暴力攻擊、挖掘加密貨幣以及發送垃圾郵件。它們不常用於進行中間人攻擊，這些攻擊通常是通過 DNS 中毒或類似機制進行的。

問題 28

tb787631.CISSPPT3E.c08.061

Martin 正在檢查用戶報告異常活動的系統，包括系統空閒時的磁盤活動以及 CPU 和網絡使用異常。他懷疑這台機器感染了病毒，但掃描結果是乾淨的。這裡可能使用了什麼惡意軟件技術來解釋乾淨的掃描結果？

A.文件感染病毒

B、MBR 病毒

C. 服務注入病毒

D. 隱形病毒

您回答錯誤。

乾淨掃描結果的一種可能性是該病毒正在使用隱蔽技術，例如攔截來自防

病毒軟件的讀取請求並返回受感染文件的正確版本。該系統也可能是零日

攻擊的受害者，使用的病毒尚未包含在防病毒供應商提供的簽名定義文件

中。

問題 29 #####

tb787631.CISSPPT3E.c08.055

下面哪一項不是對 SQL 注入攻擊的有效控制？

A、逃跑

B. 客戶端輸入驗證

C. 參數化

D. 限制數據庫權限

您回答錯誤。

客戶端輸入驗證不是針對任何類型攻擊的有效控制，因為攻擊者可以通過

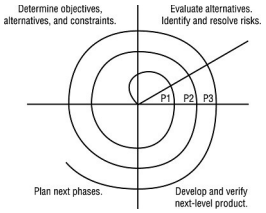
更改客戶端代碼輕鬆繞過驗證。轉義受限字符會阻止它們被傳遞到數據庫 ，

參數化也是如此。限制數據庫權限可防止執行危險代碼。

問題 30

tb787631.CISSPPT3E.c08.076

圖中顯示的是什麼軟件開發模型？



A. 瀑布

B、敏捷

乾淨的

D. 螺旋

你回答正確！

該圖顯示了軟件開發的螺旋模型。在這種方法中，開發人員使用瀑布式軟

件開發過程的多次迭代。這成為通過類似過程進行迭代的“循環”。原始的

瀑布方法不會反复迭代整個過程。一些變體確實允許迭代，但只允許前後

移動一個階段。軟件開發的敏捷方法側重於迭代改進，並不遵循嚴格的

SDLC 模型。精益是一種過程改進方法，而不是軟件開發模型。

問題 31

tb787631.CISSPPT3E.c08.004

Kathleen 正在審查此處顯示的 Ruby 代碼。此代碼使用什麼安全技術？

```
insert_new_user = db.prepare "INSERT INTO users (name, userid, gender,
usertype) VALUES (?, ? ,?,?)"
insert_new_user.execute 'davids', '194567', 'male', 'admin'
```

A. 參數化

B. 類型轉換

C、寶石切割

D、存儲過程

你回答正確！

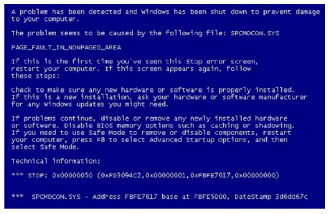
這段代碼是一個參數化的例子，它可以幫助避免 SQL 注入。請注意，每

個參數都有一個佔位符，然後將其傳遞給查詢。

第 32 題

tb787631.CISSPPT3E.c08.008

Jaime 是一名技術支持分析師，他被要求拜訪一位用戶，該用戶的計算機顯示此處所示的錯誤消息。這台電腦進入了什麼狀態？



A. 失敗打開

B、不可恢復的錯誤

C、內存耗盡

D. 故障保護

你回答正確！

圖中顯示的錯誤消息是臭名昭著的“藍屏死機”，它發生在 Windows 系統

遇到危險故障並進入故障安全狀態時。如果系統“無法打開”，它會繼續運

行。所描述的錯誤是內存故障，可能可以通過重新啟動系統來恢復。沒有

跡象表明系統可用內存已用完。

問題 33

tb787631.CISSPPT3E.c08.021

以下哪一個數據庫鍵用於強製表之間的引用完整性關係？

A、主鍵

B、候選鍵

C、外鍵

D、萬能鑰匙

你回答正確！

引用完整性確保記錄在使用另一個表的外鍵引用時存在於輔助表中。外鍵

是用於強制參照完整性的機制。

第 34 題

tb787631.CISSPPT3E.c08.083

Charles 正在開發一個對人類安全有直接影響的任務關鍵型應用程序。時間和成本不如正常運行的軟件重要。鑑於這些要求，他應該選擇以下哪種軟件開發方法？

A、敏捷

B. 開發運營

C. 螺旋

D. 瀑布

你回答正確！

儘管許多組織轉向敏捷、DevOps 或其他更具響應性的開發方法，但當

明確的目標和穩定的需求與防止缺陷的需要以及對開發過程和輸出的高度

控制相結合時，瀑布仍然是一個強有力的競爭者。

問題 35

tb787631.CISSPPT3E.c08.034

Kim 正在對一個應用程序防火牆進行故障排除，該防火牆作為組織的網絡和主機防火牆以及入侵防禦系統的補充，提供針對基於 Web 的攻擊的額外保護。該組織遇到的問題是防火牆技術經常重啟，導致它一次有 10 分鐘不可用。Kim 可能會考慮採用哪種配置來以公司最低的成本維持該期間的可用性？

A. 高可用集群

B.故障轉移設備

C. 故障打開

D. 冗餘磁盤

您回答錯誤。

在這種情況下，故障打開配置可能是合適的。在此配置中，防火牆在重新

啟動時將繼續傳遞流量而不進行檢查。這將最大限度地減少停機時間，並

且流量仍將受到場景中描述的其他安全控制的保護。故障轉移設備和高可

用性集群確實會提高可用性，但可能會付出巨大的代價。冗餘磁盤在這種

情況下無濟於事，因為沒有描述磁盤故障。

問題 36

tb787631.CISSPPT3E.c08.046

Amber 正在進行一個威脅情報項目，她想找到有關她所在組織的 Web 應用程序面臨的威脅的信息源。以下哪個組織被廣泛認為是有關基於 Web 的攻擊媒介的信息的權威來源？

A. (ISC) ^{2}

B. ISACA

C.OWASP

D. Mozilla 基金會

你回答正確！

開放 Web 應用程序安全項目 (OWASP) 被廣泛認為是 Web 應用程序安全問題上最權威的來源。他們發布了 OWASP 十大名單，公佈了最關鍵的 Web 應用程序安全問題。

問題 37

tb787631.CISSPPT3E.c08.051

Belinda 希望更好地保護其組織的 Web 應用程序的用戶免受 cookie 竊取攻擊。以下哪一項是對付此類會話劫持攻擊最有效的控制措施？

A.TLS

B. 複雜會話 cookie

C、SSL

D. 頻繁過期 cookie

你回答正確！

傳輸層安全 (TLS) 提供最有效的會話劫持防禦，因為它加密客戶端和服務器之間的所有流量，防止攻擊者竊取會話憑據。安全套接字層 (SSL) 也對流量進行加密，但它很容易受到對其加密技術的攻擊。複雜且過期的 cookie 是個好主意，但它們不足以防止會話劫持。

問題 38

tb787631.CISSPPT3E.c08.060

關於基於啟發式的反惡意軟件，以下哪項陳述是正確的？

A. 它的誤報率低於簽名檢測。

B. 它需要頻繁的定義更新來檢測新的惡意軟件。

C. 它比簽名檢測更有可能檢測到零日攻擊。

D. 它監視系統以查找包含已知病毒內容的文件。

你回答正確！

與基於簽名的方法相比，基於啟發式的反惡意軟件軟件檢測到零日攻擊的

可能性更高。基於啟發式的軟件不需要頻繁更新簽名，因為它不依賴監控

系統來檢測已知惡意軟件的存在。這種方法的缺點是它比簽名檢測方法具

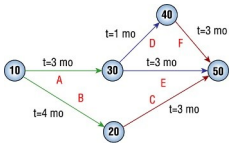
有更高的誤報率。

第 39 題

tb787631.CISSPPT3E.c08.056

Jason 正在審閱軟件開發項目的文檔，偶然發現了此處顯示的圖表。

他正在檢查什麼類型的圖表？



A. WBS 圖表

B. PERT 圖

C、甘特圖

D. 線框圖

你回答正確！

PERT 圖使用節點來表示里程碑或可交付成果，然後顯示里程碑之間移動的估計時間。甘特圖使用不同的格式，每個任務一行，顯示任務的預期持續時間。工作分解結構是一種早期的可交付成果，它將項目工作劃分為可實現的任務。線框圖用於網頁設計。

問題 40

tb787631.CISSPPT3E.c08.087

以下哪一項原則不會在軟件開發的敏捷方法中受到青睞？

A. 個人和互動之上的流程和工具

B. 工作軟件優於綜合文檔

C. 合同談判中的客戶協作

D. 響應變化勝於遵循計劃

您回答錯誤。

軟件開發的敏捷方法包含四個原則。它重視個人和交互勝過流程和工具，

重視工作軟件勝過全面的文檔，重視客戶協作勝過合同談判，響應變化勝

過遵循計劃。

問題 41

tb787631.CISSPPT3E.c08.028

Victor 最近在一家在線約會網站擔任新職位，負責領導一個開發團隊。他很快意識到開發人員在生產代碼方面存在問題，因為他們從事不同的項目，導致對生產代碼的修改相互衝突。Victor 應該投資於改進什麼流程？

A.請求控制

B. 釋放控制

C. 變更控制

D. 配置控制

你回答正確！

變更控制流程負責提供一個有組織的框架，多個開發人員可以在該框架內

創建和測試解決方案，然後再將其部署到生產環境中。請求控件為用戶請

求提供了一個框架。發布控制管理代碼到生產中的部署。配置控制確保根

據變更和配置管理策略對軟件版本進行變更。

問題 42

tb787631.CISSPPT3E.c08.096

當一個事務讀取由從未提交的第二個事務寫入數據庫的信息時，會發生以下哪一個數據庫並發問題？

A. 丟失更新

B、SQL 注入

C. 不正確的總結

D、臟讀

您回答錯誤。

當一個事務從數據庫中讀取由另一個未提交的事務寫入的值時，就會發生

臟讀。當一個事務向數據庫寫入一個值，該值覆蓋了具有較早優先級的事

務所需的值，從而導致這些事務讀取不正確的值時，就會發生更新丟失。

當一個事務使用聚合函數匯總存儲在數據庫中的數據而第二個事務正在修

改數據庫時，會出現不正確的匯總，從而導致匯總包含不正確的信息 。

SQL 注入是 Web 應用程序安全漏洞，而不是數據庫並發問題。

問題 43

tb787631.CISSPPT3E.c08.040

請參考以下場景：

- Linda 正在她公司網站上的一個用戶論壇上查看帖子，當她瀏覽某個帖子時，屏幕上的對話框中會彈出一條消息，上面寫著“提醒”。她查看帖子的源代碼並找到以下代碼片段：

```
<script>alert('Alert');</script>
```

在與供應商的進一步討論中，Linda 發現他們願意解決問題但不知道如何更新他們的軟件。什麼技術可以最有效地減輕應用程序對此類攻擊的脆弱性？

A. 邊界檢查

B. 同行評審

C. 輸入驗證

D.操作系統補丁

你回答正確！

輸入驗證驗證用戶提供的輸入是否違反安全條件，是抵禦跨站點腳本攻擊的最有效方法。邊界檢查是一種輸入驗證形式，但它通常用於確保數字輸

入在可接受的範圍內，不適用於跨站點腳本攻擊。同行評審和操作系統補

丁都是很好的安全實踐，但不太可能有效抵禦跨站點腳本攻擊。

問題 44

tb787631.CISSPPT3E.c08.081

Nathan 最近完成了一個軟件開發項目，他將組織的網絡運營堆棧與其開發流程相集成。因此，開發人員可以根據需要從他們的代碼中修改防火牆規則。哪個術語最能描述這種能力？

A、敏捷

B.IaC

三、安全數據表

D. 開發運營

您回答錯誤。

這是軟件定義的安全性 (SDS) 的一個示例，其中安全基礎設施可以很容

易地被代碼操縱。回答這個問題很棘手，因為其他幾個術語密切相關。軟

件定義的安全性是基礎設施即代碼 (IaC) 的一個示例，但 SDS 是一個更

具描述性的答案，因此也是更好的答案。SDS 通常在敏捷開發框架中使

用。DevOps 方法將開發和運營聯繫在一起，但當它還包括 SDS 時通常

稱為 DevSecOps。

問題 45

tb787631.CISSPPT3E.c08.038

請參考以下場景：

- Linda 正在她公司網站上的一個用戶論壇上查看帖子，當她瀏覽某個帖子時，屏幕上的對話框中會彈出一條消息，上面寫著“提醒”。她查看帖子的源代碼並找到以下代碼片段：

```
<script>alert('Alert');</script>
```

在包含此代碼的論壇上發布消息的用戶的可能動機是什麼？

A. 認可

B. 竊取敏感信息

C. 憑證竊取

D. 社會工程

您回答錯誤。

Linda 發現的腳本只會在用戶屏幕上彈出一條消息，不會再執行任何惡

意操作。這種類型的腳本使用 `alert()` 調用，通常用於探測網站是否存

在跨站點腳本漏洞。

問題 46

tb787631.CISSPPT3E.c08.001

Susan 為其組織的數據提供了一個公共 RESTful API，但希望將其使用限制在受信任的合作夥伴範圍內。她打算使用 API 密鑰。您會給 Susan 什麼其他建議來限制服務的潛在濫用？

A. 限制請求率

B. 強制 HTTP-only 請求

C. 由於帶寬限制避免令牌

D. 將 GET、POST、PUT 等 HTTP 方法列入黑名單

您回答錯誤。

限制請求率可以防止像這樣的 API 被濫用。其他的建議都是不好的建議。

通常，請求應該需要 HTTPS，使用 JSON Web 令牌 (JWT) 等工具將令牌用於安全性，並且 HTTP 方法可能會受到限制，但 GET、POST 和 PUT 是用於 API 訪問的一些最常用方法，並且是更典型的是列入白名單。

問題 47

tb787631.CISSPPT3E.c08.054

在評估潛在的安全事件時，Harry 發現來自 Web 服務器請求的日誌條目顯示用戶在表單字段中輸入了以下內容：

胡蘿蔔'&1=1;--

嘗試了哪種類型的攻擊？

A、緩衝區溢出

B. 跨站腳本

C、SQL 注入

D. 跨站請求偽造

你回答正確！

輸入字段中的單引號是一個明顯的跡象，表明這是一次 SQL 注入攻擊。

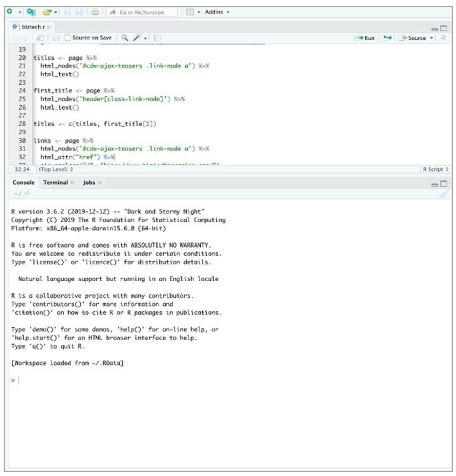
引號用於在 SQL 代碼輸入域外轉義，後面的文字用於直接操作 Web 應

用向數據庫發送的 SQL 命令。

問題 48

tb787631.CISSPPT3E.c08.041

Hannah 是一名軟件開發人員，致力於使用 R 編程語言創建統計軟件。她使用此處顯示的 RStudio 工具來幫助她編寫此代碼。哪個術語最能描述此工具？



一、SDK

B、集成開發環境

C、原料藥

D、DLP

你回答正確！

RStudio 是一種用於協助創建代碼的工具，也稱為集成開發環境 (IDE)。

軟件開發工具包 (SDK) 是可用於幫助開發人員創建代碼的代碼庫和其他

工具。應用程序編程接口 (API) 是一組可供外部開發人員使用的功能，

但代碼不會像代碼庫或其他 SDK 工具那樣在用戶的機器上執行。數據丟

失防護 (DLP) 功能不是軟件開發工具集的組成部分。

問題 49

tb787631.CISSPPT3E.c08.030

Ron 領導著一個軟件開發人員團隊，他們發現自己經常重新創建執行常見功能的代碼。他可以使用什麼軟件開發工具來最好地解決這種情況？

A. 代碼庫

B.代碼庫

C. IDE

D.那個

你回答正確！

代碼庫是可以合併到單個開發項目中的可重用函數包。Ron 可以使用庫輕鬆地在他的團隊中共享代碼。代碼存儲庫可用於管理這些庫的分發和更新，但這是次要用例，使代碼庫成為最佳答案。集成開發環境 (IDE) 是開發人員用來創建軟件的工具，而動態應用程序安全測試 (DAST) 用於驗證代碼的正確實現。

第 50 題

tb787631.CISSPPT3E.c08.092

湯姆正在編寫一個軟件程序，計算來自不同司法管轄區的在線訂單的銷售稅。該應用程序包括一個用戶定義的字段，允許輸入總銷售額。Tom 想確保在此字段中輸入的數據是格式正確的美元金額。他應該使用什麼技術？

A、極限檢查

B、故障打開

C. 故障保護

D. 輸入驗證

你回答正確！

輸入驗證確保作為輸入提供給程序的數據與預期參數匹配。限制檢查是一

種特殊形式的輸入驗證，可確保值保持在預期範圍內，但在此場景中沒有

指定範圍。在規劃可能的系統故障時，故障開放和故障安全是選項。

問題 51

tb787631.CISSPPT3E.c08.010

在此處顯示的表格中，哪個是方法示例？

帳戶

餘額：貨幣 = 0
所有者：字符串
添加資金（存款：貨幣）
RemoveFunds（取款：貨幣）

一、賬戶

B. 所有者

C. 增加資金

D、平衡

你回答正確！

在圖中，Account 是類的名稱。Owner 和 Balance 是該類的屬性 。

AddFunds 和 RemoveFunds 是該類的方法。

問題 52

tb787631.CISSPPT3E.c08.023

Victor 創建了一個數據庫表，其中包含有關其組織員工的信息。該表包含員工的用戶 ID、三個不同的電話號碼字段（家庭、工作和移動電話）、員工的辦公地點和員工的職位。表中有 16 條記錄。這張表的度數是多少？

A.3
B.4
C.6
D. 16

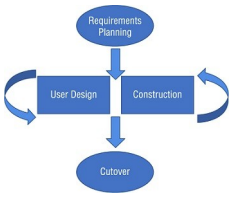
您回答錯誤。

數據庫表的度是表中屬性的數量。Victor 的表有六個屬性：員工的用戶 ID、家庭電話、辦公電話、移動電話、辦公地點和職務。

問題 53

tb787631.CISSPPT3E.c08.011

Wanda 正在審查她的組織使用的應用程序開發文檔，並找到此處顯示的生命週期圖解。她的組織使用什麼應用程序開發方法？



A. 瀑布

B、螺旋形

C、敏捷

D.RAD

你回答正確！

快速應用程序開發 (RAD) 側重於快速開發和快速適應不斷變化的需求的能力。RAD 使用四個階段：需求計劃、用戶設計、構建和切換。

問題 54

tb787631.CISSPPT3E.c08.012

以下哪一種測試方法通常可以在不訪問源代碼的情況下工作？

A.動態測試

B、靜態測試

C. 白盒測試

D、代碼審查

您回答錯誤。

軟件的動態測試通常發生在測試人員無法訪問源代碼的黑盒環境中。靜態

測試、白盒測試和代碼審查方法都需要訪問應用程序的源代碼。

問題 55

tb787631.CISSPPT3E.c08.009

Joshua 正在為他的組織開發軟件威脅建模程序。以下哪些是該計劃的適當目標？（選擇所有符合條件的。）

A. 減少與安全相關的設計缺陷的數量
B. 減少與安全相關的編碼缺陷的數量
C. 降低非安全相關缺陷的嚴重性
D. 減少威脅載體的數量

您回答錯誤。

軟件威脅建模旨在減少與安全相關的設計和編碼缺陷的數量以及其他缺陷

的嚴重性。軟件開發人員或評估人員無法控制威脅環境，因為它在組織外

部。

問題 56

tb787631.CISSPPT3E.c08.082

TJ 正在檢查一個系統，用戶報告了一個奇怪的錯誤消息和無法訪問文件。他看到了圖中所示的窗口。TJ 應該懷疑哪種類型的惡意軟件？

A. 服務注入

B、加密病毒

C、SQL 注入

D. 勒索軟件

你回答正確！

類似於圖中顯示的消息表示勒索軟件攻擊。攻擊者加密用戶硬盤上的文件，然後要求贖金（通常以比特幣支付）以獲取恢復對原始內容的訪問權限所需的解密密鑰。另一方面，加密病毒使用加密來躲避防病毒機制，並且不會更改系統上的其他內容。

問題 57

tb787631.CISSPPT3E.c08.047

Chris 是一名軟件開發人員，他正在積極地為應用程序編寫代碼。他處於敏捷過程的哪個階段？

A. 規劃

B. 衝刺

C.部署

D. 發展

您回答錯誤。

Chris 正處於敏捷衝刺階段，可能正在開發基於用戶故事的代碼。規劃包括涉眾故事，以及設計和測試用例準備。部署包括應用程序的實際部署，以及額外的驗證和測試。

問題 58

tb787631.CISSPPT3E.c08.043

Alan 正在他的環境中將 Java 代碼部署到各種機器上，並且必須首先在這些機器上安裝 JVM。在這種情況下，哪個術語最能描述 JVM？

A. 儲存庫

B. 變更經理

C、運行時

D、沙盒

你回答正確！

JVM 是允許在設備上執行 Java 代碼的運行時虛擬機。JVM 實現了 Java 沙箱，但這只是其眾多功能之一。JVM 本身不是變更管理器或代碼存儲庫。

問題 59

tb787631.CISSPPT3E.c08.036

Greg 正在與組織中爆發的惡意軟件作鬥爭。他使用專門的惡意軟件分析工具從三個不同的系統中捕獲惡意軟件樣本，並註意到代碼在不同感染之間略有變化。格雷格認為，這就是殺毒軟件難以抗擊疫情的原因。Greg 應該懷疑哪種類型的惡意軟件導致了此安全事件？

A. 隱形病毒
B、多態病毒
C. 多方病毒
D. 加密病毒

你回答正確！

每次感染系統時，多態病毒都會通過調整代碼來幫助它們逃避簽名檢測機制，從而發生變異。加密病毒也會從感染變異到感染，但通過在每台設備上使用不同的密鑰對自身進行加密來實現。

問題 60

tb787631.CISSPPT3E.c08.017

請參考以下場景：

- Robert 是一名顧問，幫助組織創建和開發成熟的軟件開發實踐。他更喜歡使用軟件能力成熟度模型 (SW-CMM) 通過獨立審查和自我評估來評估組織的當前和未來狀態。他目前正在與兩個不同的客戶合作。
- Acme Widgets 的軟件開發實踐組織得不是很好。它確實有一個專門的開發人員團隊，他們“不惜一切代價”將軟件推出市場，但它沒有任何正式的流程。
- Beta Particles 是一家在使用正式的、文檔化的軟件開發流程開發軟件方面擁有多年經驗的公司。它使用軟件開發的標準模型，但沒有對這些過程進行量化管理。

Robert 應該將 SW-CMM 的哪個階段報告為 Acme Widgets 的當前狀態？

A. 定義

B、可重複

C.初始

D、託管

您回答錯誤。

Acme Widgets 顯然處於 SW-CMM 的初級階段。這個階段的特點是沒有正式的過程。公司可能仍然會生產工作代碼，但它是以一種雜亂無章的方式進行的。

問題 61

tb787631.CISSPPT3E.c08.090

以下哪一項是軟件開發瀑布模型中正確的步驟順序？

A. 需求、設計、測試、編碼、維護
B. 需求、設計、編碼、測試、維護
C. 設計、需求、編碼、測試、維護
D. 設計、需求、測試、編碼、維護

你回答正確！

在瀑布模型中，軟件開發過程遵循五個順序步驟，依次是：需求、設計、編碼、測試和維護。

第 62 題 #####

tb787631.CISSPPT3E.c08.019

請參考以下場景：

- Robert 是一名顧問，幫助組織創建和開發成熟的軟件開發實踐。他更喜歡使用軟件能力成熟度模型 (SW-CMM) 通過獨立審查和自我評估來評估組織的當前和未來狀態。他目前正在與兩個不同的客戶合作。
- Acme Widgets 的軟件開發實踐組織得不是很好。它確實有一個專門的開發人員團隊，他們“不惜一切代價”將軟件推出市場，但它沒有任何正式的流程。
- Beta Particles 是一家在使用正式的、文檔化的軟件開發流程開發軟件方面擁有多年經驗的公司。它使用軟件開發的標準模型，但沒有對這些過程進行量化管理。

羅伯特應該將 SW-CMM 的哪個階段報告為 Beta 粒子的當前狀態？

A. 定義

B、可重複

C、優化

D、託管

你回答正確！

SW-CMM 的已定義階段以存在基本生命週期管理流程和代碼重用為標誌 。

它包括需求管理、軟件項目規劃、質量保證和配置管理實踐的使用。

問題 63

Olivia 正在對她的組織從第三方獲得的 Web 應用程序進行風險分析，並擔心它可能包含漏洞。她可能採取以下哪一項活動來最好地降低風險？

A. 部署 WAF。

B. 實施強加密。

C. 購買保險單。

D. 停止使用該軟件。

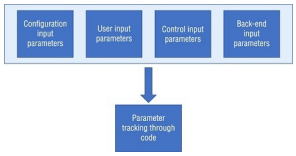
您回答錯誤。

部署 Web 應用程序防火牆 (WAF) 可以降低 Web 應用程序漏洞的可能性或影響，因此是降低風險的一個很好的例子。加密也是一種風險緩解控制，但它不太可能對 Web 應用程序安全漏洞有效。購買保單是風險轉移的一個例子，而不是減輕風險的例子。

第 64 題

tb787631.CISSPPT3E.c08.073

圖中顯示的輸入參數用於安全審查過程的哪一部分？



A. SQL 注入回顧

B. 衝刺回顧

C.費根檢查

D. 攻擊面識別

你回答正確！

這些輸入參數中的每一個都構成了應用程序攻擊面的一部分。攻擊者可以

選擇以其中任何一個為目標來攻擊代碼或其支持基礎設施。

問題 65

tb787631.CISSPPT3E.c08.013

Lucca 正在分析他的組織從第三方供應商處獲得的 Web 應用程序。Lucca 確定該應用程序包含一個缺陷，該缺陷會導致登錄的用戶能夠執行他們在其角色中不應執行的操作。這應該歸類為哪種類型的安全漏洞？

A. 數據驗證

B、會話管理

C、授權

D、錯誤處理

您回答錯誤。

鑑於這裡的選項列表，根本原因很可能是授權檢查的問題，它沒有正確地

限制用戶獲得他們應該擁有的授權。數據驗證問題更有可能允許注入攻擊

或允許輸入錯誤數據，而會話管理問題將允許會話劫持或實際上可能導致

他們以其他用戶身份登錄。最後，錯誤處理會在發生錯誤時顯示為問題，

而此問題並未表明。

第 66 題

tb787631.CISSPPT3E.c08.098

Frank 正在努力選擇一種新的雲服務，為他的團隊正在開發的應用程序提供對象存儲。Frank 計劃使用哪類雲服務？

A、SaaS

B、基礎設施即服務

C、FaaS

D、PaaS

您回答錯誤。

存儲是一個基礎設施組件，因此，對象存儲服務是基礎設施即服務

(IaaS) 雲服務的一個示例。軟件即服務 (SaaS) 模型提供由提供商管理的

完整應用程序。平台即服務 (PaaS) 和功能即服務 (FaaS) 方法允許開發

人員在提供商管理的基礎設施平台上運行他們自己的代碼。

問題 67

tb787631.CISSPPT3E.c08.091

Renee 是一名軟件開發人員，她為她的組織編寫 Node.js 代碼。該公司正在考慮從一個自託管的 Node.js 環境轉移到一個 Renee 將在雲供應商管理的應用程序服務器上運行她的代碼的環境。Renee 的公司正在考慮哪種類型的雲解決方案？

A. 基礎設施即服務

B、CaaS

C、PaaS

D、軟件即服務

你回答正確！

在平台即服務解決方案中，客戶提供供應商然後在其自己的基礎設施上執行的應用程序代碼。

第 68 題

tb787631.CISSPPT3E.c08.050

當一個事務寫入數據庫的值覆蓋了具有較早優先級的事務所需的值時，會發生以下哪一項數據庫問題？

A、臟讀

B. 不正確的總結

C. 丟失更新

D、SQL 注入

您回答錯誤。

當一個事務向數據庫寫入一個值，該值覆蓋了具有較早優先級的事務所需的值，從而導致這些事務讀取不正確的值時，就會發生更新丟失。當一個事務從數據庫中讀取由另一個未提交的事務寫入的值時，就會發生臟讀。當一個事務使用聚合函數匯總存儲在數據庫中的數據而第二個事務正在修改數據庫時，會出現不正確的匯總，從而導致匯總包含不正確的信息 。

SQL 注入是 Web 應用程序安全漏洞，而不是數據庫並發問題。

第 69 題

tb787631.CISSPPT3E.c08.077

Mark 正在考慮用雲中可用的新產品替換其組織的客戶關係管理 (CRM) 解決方案。這個新的解決方案完全由供應商管理，Mark 的公司將不必編寫任何代碼或管理任何物理資源。Mark 正在考慮哪種類型的雲解決方案？

A. 基礎設施即服務

B、CaaS

C、PaaS

D、軟件即服務

你回答正確！

在軟件即服務解決方案中，供應商管理物理基礎設施和完整的應用程序堆

棧，為客戶提供對完全託管應用程序的訪問。

第 70 題

tb787631.CISSPPT3E.c08.052

在軟件配置管理程序中，CAB 的主要作用是什麼？

A. 批准開發人員的憑據。

B. 促進經驗教訓會議。

C. 審核並批准/拒絕代碼更改。

D. 優先考慮軟件開發工作。

你回答正確！

變更顧問委員會 (CAB) 的目的是審查然後批准或拒絕提議的代碼變更。

CAB 通常不參與開發人員證書的批准、經驗教訓會議的開展或軟件開發

工作的優先級排序。

第 71 題

tb787631.CISSPPT3E.c08.088

API 開發人員最常使用什麼技術來將對 API 的訪問限制為授權個人和應用程序？

A. 加密

B. 輸入驗證

C. API 密鑰

D. IP 過濾器

您回答錯誤。

API 開發人員通常使用 API 密鑰來限制對授權用戶和應用程序的訪問。

加密為使用 API 交換的信息提供機密性，但不提供身份驗證。輸入驗證

是一種用於防止惡意輸入的應用程序安全技術。IP 過濾器可用於限制對

API 的訪問，但它們並不常用，因為隨著端點的變化，過濾器需要不斷

修改和維護，因此很難使用 IP 過濾器部署 API。

第 72 題

tb787631.CISSPPT3E.c08.093

Brian 正在幫助他的組織實施一種新的軟件測試方法，他想審查他的工具包的完整性。以下哪項將被視為動態應用程序安全測試 (DAST) 工具？（選擇所有符合條件的。）

A. 代碼審查

B. 模糊測試

C、靜態分析

D. Web 應用程序漏洞掃描

你回答正確！

動態應用程序安全工具通過實際執行代碼來進行測試。模糊測試和 Web

應用程序漏洞掃描都是這種情況。代碼審查和靜態分析包分析代碼本身但

不執行它，使它們成為靜態應用程序安全測試 (SAST) 工具。

第 73 題

tb787631.CISSPPT3E.c08.003

以下哪一項關於代碼審查的陳述是不正確的？

A. 代碼審查應該是一個包括多個開發人員的同行驅動的過程。

B. 代碼審查可以自動化。

C. 代碼審查發生在設計階段。

D. 代碼審查者可能期望每小時審查幾百行代碼。

你回答正確！

代碼審查發生在代碼開發之後，發生在系統開發生命週期 (SDLC) 的設

計階段之後。代碼審查可以結合使用手動和自動技術，或者僅依賴其中一

種技術。它應該是一個同行驅動的過程，包括沒有編寫代碼的開發人員。

開發人員應該期望平均每小時完成大約 300 行的審查。

第 74 題

tb787631.CISSPPT3E.c08.022

Brynn 認為她組織中的系統可能已被宏病毒破壞。以下哪個文件最有可能是罪魁禍首？

A.投影.doc

B 、command.com

C、命令.exe

D.loopmaster.exe _

您回答錯誤。

宏病毒最常見於辦公文檔，例如以 .doc 或 .docx 擴展名結尾的

Microsoft Word 文檔。它們通常不存在於擴展名為 .com 或 .exe 的可執

行文件中。

第 75 題

tb787631.CISSPPT3E.c08.015

Taylor 希望更好地保護她的組織開發的應用程序免受緩衝區溢出攻擊。以下哪項控制最能提供這種保護？

A. 加密

B. 輸入驗證

C、防火牆

D. 入侵防禦系統

您回答錯誤。

防止緩衝區溢出攻擊的最佳保護是服務器端輸入驗證。該技術將用戶輸入限制在適合已分配緩衝區的認可值範圍內。雖然防火牆和入侵防禦系統可能包含限制緩衝區溢出的控件，但在應用程序服務器上執行過濾會更有效。加密無法防止緩衝區溢出攻擊。

第 76 題

tb787631.CISSPPT3E.c08.044

Christine 已接近測試新軟件包的最後階段。以下哪一種類型的軟件測試通常最後發生並針對測試場景執行？

A、單元測試

B、集成測試

C. 用戶驗收測試

D、系統測試

你回答正確！

用戶驗收測試 (UAT) 通常是測試過程的最後階段。它驗證開發的解決方

案是否滿足用戶要求並根據用例對其進行驗證。單元測試、集成測試和系

統測試都在 UAT 之前的過程中進行。

第 77 題

tb787631.CISSPPT3E.c08.074

這三個主要步驟可以描述什麼應用程序安全過程？

1. 分解應用程序
2. 確定和排序威脅
3. 確定對策和緩解措施

A.費根檢查

B. 威脅建模

C. 滲透測試

D、代碼審查

你回答正確！

威脅建模通常涉及分解應用程序以了解它以及它如何與其他組件或用戶交互。接下來，識別威脅並對其進行排序可以讓您專注於應該優先考慮的威脅。最後，確定如何減輕這些威脅完成了這個過程。一旦完成，組織就可以採取行動來處理通過適當的控制措施識別出的威脅。

第 78 題

tb787631.CISSPPT3E.c08.018

請參考以下場景：

- Robert 是一名顧問，幫助組織創建和開發成熟的軟件開發實踐。他更喜歡使用軟件能力成熟度模型 (SW-CMM) 通過獨立審查和自我評估來評估組織的當前和未來狀態。他目前正在與兩個不同的客戶合作。
- Acme Widgets 的軟件開發實踐組織得不是很好。它確實有一個專門的開發人員團隊，他們“不惜一切代價”將軟件推出市場，但它沒有任何正式的流程。
- Beta Particles 是一家在使用正式的、文檔化的軟件開發流程開發軟件方面擁有多年經驗的公司。它使用軟件開發的標準模型，但沒有對這些過程進行量化管理。

Robert 正在與 Acme Widgets 合作制定一項戰略，以推進他們的軟件開發實踐。他們的下一個目標里程碑應該是哪個 SW-CMM 階段？

A. 定義

B、可重複

C.初始

D、託管

您回答錯誤。

可重複階段是 SW-CMM 中繼初始階段之後的第二個階段。它應該是 Acme Widgets 的下一個里程碑目標。可重複階段的特點是基本的生命週期管理流程。

第 79 題 #####

tb787631.CISSPPT3E.c08.065

Gavin 是一名內部審計員，負責檢查其組織的變革管理實踐。他想審查對軟件包所做的一系列更改，以確定它們是否已正確記錄。他應該從哪裡獲得對每項提議變更的描述？

A.駕駛室

B.RFC

C.翱翔

D、SIEM

您回答錯誤。

每個更改都應該是經過審查和批准的更改請求 (RFC) 的結果。這些 RFC

可能會得到變更諮詢委員會 (CAB) 的批准。組織使用的安全信息和事件

管理 (SIEM) 以及安全編排、自動化和響應 (SOAR) 平台通常不會包含

有關變更管理流程的信息。

問題 80 #####

tb787631.CISSPPT3E.c08.027

什麼術語用於描述軟件沒有漏洞的置信度，無論是有意設計到軟件中還是在其生命週期的任何時候意外插入，並且軟件以預期的方式運行？

A. 驗證
B. 認證
C. 置信區間
D. 保險

您回答錯誤。

就軟件而言，保證是指軟件沒有漏洞的置信度，無論是有意設計到軟件中

還是在其生命週期的任何時候意外插入，並且軟件以預期的方式運行。這

是一個通常用於軍事和國防環境的術語。

問題 81

tb787631.CISSPPT3E.c08.086

盧卡斯為他的公司運行會計系統。一個重要的東西被解僱後的第二天早上，系統開始莫名其妙地丟失信息。盧卡斯懷疑被解僱的員工在離職前篡改了系統。Lucas 應該懷疑哪種類型的攻擊？

A. 權限提升

B、SQL 注入

C、邏輯炸彈

D. 遠程代碼執行

你回答正確！

這個問題的關鍵事實是盧卡斯懷疑篡改發生在員工離開之前。這是邏輯炸彈的特徵：在滿足特定條件之前處於休眠狀態的惡意代碼。此處列出的其他攻擊類型——權限提升、SQL 注入和遠程代碼執行——更有可能實時發生。

問題 82

tb787631.CISSPPT3E.c08.094

哪種技術管理方法集成了圖中所示的技術管理的三個組成部分？

A、敏捷

B、精益

C. 開發運營

D、ITIL

你回答正確！

DevOps 技術管理方法尋求以無縫方法集成軟件開發、運營和質量保證 ，

從而在三個學科之間建立協作。

問題 83

tb787631.CISSPPT3E.c08.063

攻擊者向公共討論論壇發布了一條消息，其中包含一個嵌入的惡意腳本，該腳本不會向用戶顯示，但在閱讀後會在用戶系統上執行。這是什麼類型的攻擊？

A. 持久性 XSRF

B. 非持久性 XSRF

C. 持久性 XSS

D. 非持久性 XSS

您回答錯誤。

惡意用戶通過使用第三方站點誘騙受害者的 Web 瀏覽器執行腳本的攻擊

稱為跨站點腳本 (XSS) 攻擊。這種特殊的攻擊是一種持久性 XSS 攻擊 ，

因為它一直保留在論壇上，直到管理員發現並刪除它，從而能夠影響許多

用戶。

問題 84

tb787631.CISSPPT3E.c08.032

參考此處顯示的數據庫事務，如果帳戶號為 1001 的帳戶表中不存在帳戶，會發生什麼情況？

開始交易

更新帳戶

設置餘額 = 餘額 + 250

WHERE 賬號 = 1001;

更新帳戶

設置餘額 = 餘額 - 250

WHERE 賬戶號碼 = 2002 ;

結束交易

A. 數據庫會用這個賬號創建一個新賬戶，並給它一個 250 美元的餘額。

B. 數據庫將忽略該命令並仍然將第二個帳戶的餘額減少 250 美元。

C. 數據庫將回滾事務，忽略兩個命令的結果。

D. 數據庫會產生一條錯誤信息。

您回答錯誤。

在此示例中，這兩個 SQL 命令確實捆綁在一個事務中，但發出不匹配任

何行的更新命令並不是錯誤。因此，第一個命令將“成功”更新零行，不會

產生錯誤或導致事務回滾。然後將執行第二個命令，將第二個帳戶的餘額

減少 250 美元。

問題 85 #####

tb787631.CISSPPT3E.c08.059

Roger 正在對其公司開發的報稅應用程序進行軟件測試。最終用戶將通過網絡訪問應用程序，但羅傑在後端進行測試，評估網絡服務器上的源代碼。Roger 正在進行什麼類型的測試？

A、白框

B、灰盒

C、藍框

D、黑匣子

您回答錯誤。

在白盒測試中，攻擊者可以在開始測試之前訪問系統的完整實現細節，包括源代碼。在灰盒測試中，攻擊者擁有部分知識。在黑盒測試中，攻擊者對系統一無所知，站在用戶的角度進行測試。藍盒子是一種電話黑客工具，不用於軟件測試。

問題 86

tb787631.CISSPPT3E.c08.024

Carrie 正在分析她基於 Web 的應用程序的應用程序日誌，並遇到以下字符串：

```
../../../../../../../../../etc/passwd
```

可能針對 Carrie 的應用程序嘗試了哪種類型的攻擊？

A. 命令注入

B、會話劫持

C、目錄遍歷

D、蠻力

你回答正確！

日誌中顯示的字符串是目錄遍歷攻擊的特徵，攻擊者試圖強制 Web 應用程序向上導航文件層次結構並檢索通常不應提供給 Web 用戶的文件，例

如密碼文件。“雙點”系列表示目錄遍歷攻擊，因為它是用於引用層次結構

中上一級目錄的字符串。

問題 87

tb787631.CISSPPT3E.c08.026

Tracy 正準備為其組織的企業資源規劃系統應用補丁。她擔心補丁可能會引入之前版本中不存在的缺陷，因此她計劃進行一項測試，將之前對輸入的響應與新打補丁的應用程序產生的響應進行比較。Tracy 計劃進行哪種類型的測試？

A、單元測試

B.驗收測試

C. 回歸測試

D. 漏洞測試

你回答正確！

回歸測試是針對應用程序運行一組已知輸入，然後將結果與軟件早期版本

產生的結果進行比較的軟件測試。它旨在捕獲在將新代碼版本引入生產環

境之前部署新代碼版本的意外後果。

問題 88

tb787631.CISSPPT3E.c08.097

國防部在 1990 年代率先提出了什麼軟件開發概念，以努力將不同的產品開發團隊聚集在一起？

A. 綜合產品團隊

B. 敏捷方法

C. Scrum 方法

D、用戶故事

您回答錯誤。

集成產品團隊 (IPT) 方法彙集了跨職能團隊，由國防部於 1995 年設計。

它是敏捷方法的前身，它使用 scrum 方法和用戶故事等工具來進行軟件開發工作。

問題 89

tb787631.CISSPPT3E.c08.035

當攻擊者可以通過分析分類在較低級別的幾條信息來推斷出一條更敏感的信息時，會出現什麼類型的安全問題？

A、SQL 注入

B. 多級安全

C. 參數化

D. 推理

你回答正確！

當攻擊者可以將不太敏感的信息拼湊在一起並使用它們來導出更敏感的信息時，就會出現推理問題。SQL 注入是一種 Web 應用程序漏洞。多級安全是一種系統控制，允許同時處理不同分類級別的信息。參數化是一種安全控制，用於降低依賴於不當用戶輸入的攻擊的可能性。

問題 90

tb787631.CISSPPT3E.c08.007

Arnold 正在創建一個新的軟件包並使用 OpenSSL 庫。哪個術語最能描述他正在使用的庫？

A. 開源
B.COTS
C、第三方
D、託管

你回答正確！

OpenSSL 包是廣泛使用的 TLS 加密實現，可作為開源包使用。它不是現成的商業軟件 (COTS)。雖然它可能是由第三方開發的，但將其描述

為開源更為準確。該庫可作為免費使用的代碼使用，但不能作為託管服務使用。

問題 91

tb787631.CISSPPT3E.c08.067

在這裡顯示的事務中，如果數據庫在第一個和第二個更新語句之間失敗，會發生什麼情況？

開始交易

更新帳戶

設置餘額 = 餘額 + 250

WHERE 賬號 = 1001;

更新帳戶

設置餘額 = 餘額 - 250

WHERE 賬戶號碼 = 2002；

結束交易

A. 數據庫會將 250 美元的資金存入第一個賬戶，但不會減少第二個賬戶的餘額。

B. 數據庫將忽略第一個命令，只將第二個帳戶的餘額減少 250 美元。

C. 數據庫將回滾事務，忽略兩個命令的結果。

D. 數據庫會成功執行這兩個命令。

您回答錯誤。

事務中間的數據庫故障會導致整個事務的回滾。在這種情況下，數據庫不會執行任何命令，因為這樣做會違反事務的原子性屬性。

問題 92

tb787631.CISSPPT3E.c08.014

Bobby 正在調查授權的數據庫用戶如何獲得對超出其正常許可級別的信息的訪問權限。Bobby 認為用戶正在使用一種匯總數據的功能。什麼術語描述了這種類型的功能？

A. 推論
B、多態
C、骨料
D、模塊化

您回答錯誤。

聚合函數匯總大量數據，結果僅提供匯總信息。如果精心設計，聚合函數可能會無意中洩露敏感信息。

問題 93

tb787631.CISSPPT3E.c08.033

Brandon 是一名軟件開發人員，希望將他的軟件與流行的社交媒體網站集成。該站點為他提供了軟件庫，他可以使用這些軟件庫更好地集成他的代碼以及其他使他的工作更輕鬆的工具。哪個術語最能描述他正在使用的服務？

一、SDK

B、DLP

C. 去

D、原料藥

你回答正確！

軟件開發工具包 (SDK) 是可用於幫助開發人員創建代碼的代碼庫和其他工具。集成開發環境 (IDE) 可能是 SDK 的一個組件，但不一定是每個 SDK 的一部分。應用程序編程接口 (API) 是一組可供外部開發人員使用的功能，但代碼不會像代碼庫或其他 SDK 工具那樣在用戶的機器上執行。

數據丟失防護 (DLP) 功能不是軟件開發工具集的組成部分。

問題 94

tb787631.CISSPPT3E.c08.025

當遵循軟件開發的 SDLC 方法時，何時應該進行設計評審？

A.代碼審查後

B. 用戶驗收測試後

C.功能需求開發後

D.單元測試完成後

您回答錯誤。

設計評審應在功能和控制規範開發之後但在代碼創建之前進行。代碼審查、

單元測試和功能測試都發生在代碼創建之後，因此也發生在設計審查之後。

問題 95

tb787631.CISSPPT3E.c08.089

Reggie 最近收到了他公司內部審計員的一封信，他安排召開啟動會議以評估他的團隊。Reggie 不希望在那次會議中學到以下哪項？

A. 審計範圍

B. 審計目的

C. 預計時限

D. 預期結果

您回答錯誤。

審計啟動會議應清楚地描述審計的範圍和目的以及預期的時間框架。審計

師不應該對他們會發現什麼有任何期望來進行審計，因為審計結果只能根

據審計檢查的結果來製定

問題 96

tb787631.CISSPPT3E.c08.005

Jessica 正在審查她所在組織的變更管理流程，並希望驗證軟件變更是否包括驗收測試。哪個過程負責實現這個目標？

A.請求控制

B. 變更控制

C. 釋放控制

D. 配置控制

您回答錯誤。

發布控製過程的職責之一是確保該過程包括驗收測試，以確認在代碼發布之前對最終用戶工作任務的任何更改都已被理解並起作用。請求控制、變更控制和配置控製過程不包括驗收測試。

問題 97

tb787631.CISSPPT3E.c08.020

請參考以下場景：

- Robert 是一名顧問，幫助組織創建和開發成熟的軟件開發實踐。他更喜歡使用軟件能力成熟度模型 (SW-CMM) 通過獨立審查和自我評估來評估組織的當前和未來狀態。他目前正在與兩個不同的客戶合作。

- Acme Widgets 的軟件開發實踐組織得不是很好。它確實有一個專門的開發人員團隊，他們“不惜一切代價”將軟件推出市場，但它沒有任何正式的流程。
- Beta Particles 是一家在使用正式的、文檔化的軟件開發流程開發軟件方面擁有多年經驗的公司。它使用軟件開發的標準模型，但沒有對這些過程進行量化管理。

Robert 還與 Beta Particles 合作制定推進其軟件開發實踐的戰略。他們的下一個目標里程碑應該是哪個 SW-CMM 階段？

A. 定義

B、可重複

C、優化

D、託管

您回答錯誤。

託管階段是 SW-CMM 中繼定義階段之後的第四個階段。這應該是 Beta Particles 的下一個里程碑目標。管理階段的特點是使用量化的軟件開發措施。

問題 98

tb787631.CISSPPT3E.c08.057

在什麼軟件測試技術中，評估者在每次軟件更改時重新測試大量場景以驗證結果是否與標準基線一致？

A. 正交陣列測試

B. 模式測試

C. 矩陣測試

D. 回歸測試

你回答正確！

在開發人員對應用程序進行更改後執行回歸測試。它重新運行大量測試用

例並將結果與基線結果進行比較。正交陣列測試是一種基於統計分析生成

測試用例的方法。模式測試使用過去軟件錯誤的記錄來為分析提供信息。

矩陣測試開發了一個包含所有可能輸入和輸出的矩陣，以告知測試計劃。