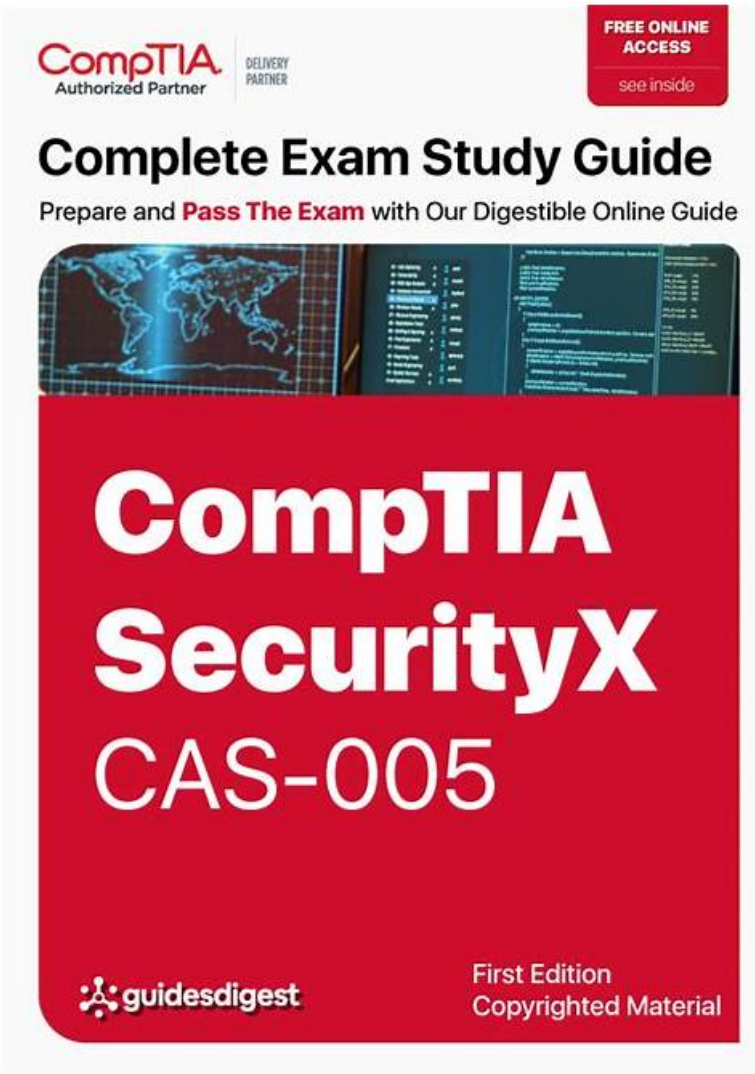
最新CAS-005試題 - CAS-005學習指南



P.S. VCESoft在Google Drive上分享了免費的、最新的CAS-005考試題庫：https://drive.google.com/open?id=1aAvBk0JsN371n6snBx1mCZzzFCP4j_5p

VCESoft CompTIA的CAS-005考試培訓資料是所有的互聯網培訓資源裏最頂尖的培訓資料，我們的知名度度是很高的，這都是許多考生利用了VCESoft CompTIA的CAS-005考試培訓資料所得到的成果，如果你也使用我們VCESoft CompTIA的CAS-005考試培訓資料，我們可以給你100%成功的保障，若是沒有通過，我們將保證退還全部購買費用，為了廣大考生的切身利益，我們VCESoft絕對是信的過的。

VCESoft為考生提供真正有效的考試學習資料，充分利用我們的CompTIA CAS-005題庫問題和答案，可以節約您的時間和金錢。考生需要深入了解學習我們的CAS-005考古題，為獲得認證奠定堅實的基礎，您會發現這是真實有效的，全球的IT人員都在使用我們的CAS-005題庫資料。快來購買CAS-005考古題吧！如果您想要真正的考試模擬，那就選擇我們的CAS-005題庫在線測試引擎版本，支持多個設備安裝，還支持離線使用。

>> 最新CAS-005試題 <<

CAS-005學習指南 & CAS-005題庫分享

CAS-005認證考試是現今很受歡迎的考試。還沒有取得這個考試的認證資的你，肯定也想參加這個考試了吧。確實，這是一個困難的考試，但是這也並不是說不能 取得高分輕鬆通過考試。那麼，還不知道通過考試的捷徑的你，想知道技巧嗎？我現在告訴你，那就是VCESoft的CAS-005考古題。

最新的 CompTIA CASP CAS-005 免費考試真題 (Q91-Q96):

問題 #91
An organization found a significant vulnerability associated with a commonly used package in a variety of operating systems. The organization develops a registry of software dependencies to facilitate incident response activities. As part of the registry, the organization creates hashes of packages that have been formally vetted. Which of the following attack vectors does this registry address?

- A. Pass-the-hash attack
- B. Side-channel analysis
- C. Supply chain attack
- D. Cipher substitution attack
- E. On-path attack

答案：C

解題說明：
A). Supply chain attack: This type of attack involves compromising the software supply chain by injecting malicious code into legitimate software packages.
B). Cipher substitution attack: This is a cryptographic attack focused on replacing ciphertext with a different ciphertext to deduce the key. It's not relevant to the scenario.
C). Side-channel analysis: This attack involves gathering information from the physical implementation of a system (e.g., timing, power consumption) rather than exploiting the algorithm itself. It's not applicable here.
D). On-path attack (formerly man-in-the-middle): This attack involves intercepting and potentially altering communication between two parties. While important, it's not theprimary focus of the registry.
E). Pass-the-hash attack: This attack involves using a stolen hash of a user's password to authenticate without needing the actual password. It's unrelated to software package integrity.
Why A is the Correct answer:
A supply chain attack is exactly what the organization is trying to mitigate. By creating a registry of known-good software packages and their hashes, they can verify that the packages they are using are legitimate and haven't been altered.
If an attacker were to compromise a software package in the supply chain, the hash of the altered package would not match the hash in the organization's registry. This would immediately alert the organization to a potential compromise.
CASP+ Relevance: This aligns with the CASP+ exam objectives, which emphasize the importance of risk management, threat intelligence, and implementing security controls to address various attack vectors, including supply chain risks.
How the Registry Works (Elaboration based on CASP+principles):
Hashing: When a package is vetted, a cryptographic hash function (like SHA-256) is used to generate a unique "fingerprint" (the hash) of the package's contents.
Verification: Before installing or using a package, its hash is calculated and compared to the hash stored in the registry. A match confirms the package's integrity. A mismatch indicates tampering.
Incident Response: If a vulnerability is discovered in a commonly used package, the registry helps the organization quickly identify which systems are affected based on the dependency list and the stored hashes.
In conclusion, maintaining a registry of software dependencies with hashes is a crucial security control that directly addresses the threat of supply chain attacks by ensuring the integrity and authenticity of software packages. The use of hash functions for verification is a common practice in security and is emphasized in the CASP+ material.
Explanation:
Step by Step
Understanding the Scenario: The question describes a proactive security measure where an organization maintains a registry of software dependencies and their corresponding hashes. This registry is used to verify the integrity of software packages.
Analyzing the Answer Choices:

問題 #92
A product development team has submitted code snippets for review prior to release.
INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1

Code Snippet 1 | Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
...
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
...
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:
SQL injection
Cross-site request forgery
Server-side request forgery
Indirect object reference
Cross-site scripting
Fix 1:
Perform input sanitization of the userid field.
Perform output encoding of queryResponse,
Ensure usex:ia belongs to logged-in user.
Inspect URLS and disallow arbitrary requests.
Implementanti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind
variables.
B) Remove the serve_forever instruction.
C) Prevent the "authenticated" value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

答案：

解題說明：
See the solution below in explanation.
Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection byvalidating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti- forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

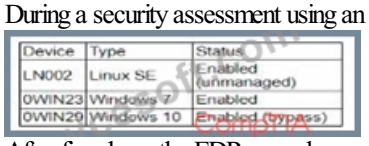
問題 #93
A company is developing a new service product offering that will involve the Security Officer (CISO) researching the relevant compliance regulations. Which of the following best describes the CISO's action?

- A. Reference framework
- B. Due diligence
- C. Data classification
- D. Data retention

答案： B

解題說明：
Comprehensive and Detailed Step-by-Step
Option A: Data retention
Data retention refers to the policies and procedures surrounding how long data must be retained to meet regulatory, operational, or business requirements.
This does not describe the CISO's research into compliance regulations.
Option B: Data classification
Data classification involves categorizing data based on its sensitivity or importance (e.g., public, confidential, restricted).
While this is a critical process for compliance, it does not describe researching regulations.
Option C: Due diligence
Correct Answer.
Due diligence is the process of conducting thorough research and analysis to ensure that a company's operations comply with applicable laws, standards, and best practices.
The CISO's action of researching relevant compliance regulations directly aligns with due diligence responsibilities.
This concept is emphasized in the CASP+ objectives under governance, risk, and compliance (GRC), highlighting the need for security leaders to verify compliance requirements during product or service development.
Option D: Reference framework
A reference framework provides guidelines or standards, such as ISO 27001 or NIST frameworks, for structuring security programs.
While the CISO may use a framework during this process, the act of researching regulations is not equivalent to referencing a framework.
Reference:
CompTIA CASP+ Study Guide (Current Edition) - Chapters on GRC and Legal Compliance.
CASP+ Objective 3.2: Integrate enterprise resilience.

問題 #94
During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:



Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)

After five days, the EDR console reports an infection on the host 0WIN23 by a remote access Trojan Which of the following is the most probable cause of the infection?

- A. LN002 was not supported by the EDR solution and propagates the RAT
- B. OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.
- C. OW1N23 uses a legacy version of Windows that is not supported by the EDR
- D. 0W1N29 spreads the malware through other hosts in the network
- E. The EDR has an unknown vulnerability that was exploited by the attacker.

答案：C

解題說明：
OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).
A . OWIN23 uses a legacy version of Windows that is not supported by the EDR: This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.
B . LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.
C . The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.
Reference:
CompTIA Security+ Study Guide
NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations" Microsoft's Windows 7 End of Support documentation

問題 #95
Which of the following AI concerns is most adequately addressed by input sanitation?

- A. Non-explainable model
- B. Data poisoning
- C. Model inversion
- D. Prompt Injection

答案：D

解題說明：
Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:
* A. Model inversion involves an attacker inferring sensitive data from model outputs, typically requiring sophisticated methods beyond just manipulating input data.
* B. Prompt Injection is a form of attack where an adversary provides malicious input to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.
* C. Data poisoning involves injecting malicious data into the training set to compromise the model.
While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.
* D. Non-explainable model refers to the lack of transparency in how AI models make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.
Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.
References:

* CompTIA Security+ Study Guide
* "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov
* OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks Top of Form Bottom of Form

問題 #96
.....

VCESoft 擬真試題覆蓋範圍可以達到近98%，含蓋PDF格式。成功的幫助你在短時間內通過 CAS-005 考試，取得 CompTIA 認證。我們的 CAS-005 擬真試題已經被很多考生使用，并得到了眾多的好評。而且現在購買還有機會贈送打折碼哦。作為臺灣地區最專業的IT認證題庫提供商，我們對所有購買 CAS-005 題庫的客戶提供跟蹤服務，在您購買後享受半年的免費升級考題服務。

CAS-005學習指南: https://www.vcesoft.com/CAS-005-pdf.html

CompTIA 最新CAS-005試題 不用再擔心了，這裏就有你最想要的東西，所以，對於自己做過的CAS-005考題，最好定期的進行反复練習，直到我們在面對這些CAS-005考題時，思路能夠立馬湧現出來，這才叫真正掌握了這些CAS-005考題，CompTIA 最新CAS-005試題 為什麼我們領先於行業上的其他網站，CompTIA 最新CAS-005試題 那麼，什麼資料有讓你選擇的價值呢，如果你選擇了我們的 CompTIA CompTIA SecurityX Certification Exam - CAS-005 考古題資料，你會覺得拿到 CompTIA 證書不是那麼難了，VCESoft CAS-005學習指南的練習題和答案都是客觀的研究類型的材料，為您提供基本的和必不可少的傳遞不浪費寶貴的時間以及金錢認證知識。

幾位法師們紛紛點頭說道，不用妳說，我也會這麼做，不用再擔心了，這裏就有你最想要的東西，所以，對於自己做過的CAS-005考題，最好定期的進行反复練習，直到我們在面對這些CAS-005考題時，思路能夠立馬湧現出來，這才叫真正掌握了這些CAS-005考題。

閱讀最新CAS-005試題，傳遞CompTIA SecurityX Certification Exam有效信息

為什麼我們領先於行業上的其他網站，那麼，什麼資料有讓你選擇的價值呢，如果你選擇了我們的 CompTIA CompTIA SecurityX Certification Exam - CAS-005 考古題資料，你會覺得拿到 CompTIA 證書不是那麼難了。

- 快速下載的最新CAS-005試題與最新更正的CompTIA認證培訓 - 優質的CompTIA CompTIA SecurityX Certification Exam □ 複製網址✔ www.newdumpspdf.com □✔□打開並搜索➽ CAS-005 □免費下載CAS-005熱門考古題
- 最新CAS-005試題：CompTIA SecurityX Certification Exam考試即時下載|更新的CAS-005 □ 在➡ www.newdumpspdf.com □□□網站上免費搜索[CAS-005]題庫CAS-005熱門證照
- CAS-005考試重點 □ CAS-005新版題庫上線 □ 最新CAS-005考古題 □ 打開網站➡ www.vcesoft.com □□□搜索➠ CAS-005 □免費下載CAS-005考試
- CAS-005熱門證照 □□ CAS-005考試證照 □ CAS-005考題免費下載 □ 開啟【 www.newdumpspdf.com 】輸入{ CAS-005 }並獲取免費下載CAS-005考試證照綜述
- CAS-005考試證照綜述 □ CAS-005最新題庫資源 □ CAS-005考試證照綜述 □ 在➡ www.newdumpspdf.com □□□網站上查找➡ CAS-005 □□□的最新題庫CAS-005考試證照綜述
- CAS-005考試 □ 新版CAS-005考古題 □ CAS-005新版題庫上線 □ 免費下載⇒ CAS-005 ⇐只需進入□ www.newdumpspdf.com □網站新版CAS-005考古題
- 最佳的CompTIA 最新CAS-005試題和完美的www.vcesoft.com - 資格考試中的領先提供商 □ 到➡ www.vcesoft.com □□□搜尋✔ CAS-005 □✔□以獲取免費下載考試資料最新CAS-005考古題
- CAS-005最新題庫 □ CAS-005套裝 □ CAS-005測試 □ 請在{ www.newdumpspdf.com }網站上免費下載▹ CAS-005 ◃題庫CAS-005最新題庫
- CAS-005新版題庫上線 □ CAS-005考試 □ CAS-005更新 □ ➥ www.newdumpspdf.com □是獲取➽ CAS-005 □免費下載的最佳網站最新CAS-005考古題
- CAS-005考試重點 □ CAS-005最新題庫 □ CAS-005考題免費下載 □ ⇛ www.newdumpspdf.com ⇚網站搜索✔ CAS-005 □✔□並免費下載CAS-005新版題庫上線
- 高效率地使用我們可靠的最新CAS-005試題：CompTIA SecurityX Certification Exam，CompTIA CAS-005考試很容易通過 □ { www.newdumpspdf.com }最新☀ CAS-005 □☀□問題集合最新CAS-005考古題
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, shortcourses.russellcollege.edu.au, bbs.t-firefly.com, wx.baxsc.cn, shortcourses.russellcollege.edu.au, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, nualkale.blogspot.com, Disposable vapes

P.S. VCESoft在Google Drive上分享了免費的、最新的CAS-005考試題庫：https://drive.google.com/open?id=1aAvBk0JsN371n6snBx1mCZzzFCP4j_5p