This page was exported from - New Lead2pass Dumps PDF Version Released For Free Downloading
Export date: Fri Mar 29 6:16:45 2024 / +0000 GMT

[April 2018 Free Sharing Of Updated CAS-002 VCE And PDF Dumps From Lead2pass 900q

Free Updated Lead2pass CAS-002 Exam Dumps Download: https://www.lead2pass.com/cas-002.html QUESTION 21A company is developing a new web application for its Internet users and is following a secure coding methodology. Which of the following methods would BEST assist the developers in determining if any unknown vulnerabilities are present? A. Conduct web server load tests.B. Conduct static code analysis.C. Conduct fuzzing attacks.D. Conduct SQL injection and XSS attacks.Answer: C QUESTION 22A project has been established in a large bank to develop a new secure online banking platform. Half way through the development it was discovered that a key piece of software used as part of the base platform is now susceptible to recently published exploits. Who should be contacted FIRST by the project team to discuss potential changes to the platform requirements? A. EngineersB. Facilities ManagerC. StakeholdersD. Human Resources Answer: C QUESTION 23The security administrator has been tasked with providing a solution that would not only eliminate the need for physical desktops, but would also centralize the location of all desktop applications, without losing physical control of any network devices. Which of the following would the security manager MOST likely implement? A. VLANsB. VDIC. PaaSD. IaaS Answer: B QUESTION 24A number of security incidents have been reported involving mobile web-based code developed by a consulting company. Performing a root cause analysis, the security administrator of the consulting company discovers that the problem is a simple programming error that results in extra information being loaded into the memory when the proper format is selected by the user. After repeating the process several times, the security administrator is able to execute unintentional instructions through this method. Which of the following BEST describes the problem that is occurring, a good mitigation technique to use to prevent future occurrences, and why it a security concern? A. Problem: Cross-site scripting Mitigation Technique. Input validation Security Concern: Decreases the company's profits and cross-site scripting can enable malicious actors to compromise the confidentiality of network connections or interrupt the availability of the network.B. Problem: Buffer overflow Mitigation Technique: Secure coding standardsSecurity Concern: Exposes the company to liability buffer overflows and can enable malicious actors to compromise the confidentiality/availability of the data.C. Problem: SQL injection Mitigation Technique: Secure coding standardsSecurity Concern: Exposes the company to liability SQL injection and can enable malicious actors to compromise the confidentiality of data or interrupt the availability of a system.D. Problem: Buffer overflow Mitigation Technique: Output validationSecurity Concern: Exposing the company to public scrutiny buffer overflows can enable malicious actors to interrupt the availability of a system. Answer: B QUESTION 25A security architect is assigned to a major software development project. The software development team has a history of writing bug prone, inefficient code, with multiple security flaws in every release. The security architect proposes implementing secure coding standards to the project manager. The secure coding standards will contain detailed standards for: A. error handling, input validation, memory use and reuse, race condition handling, commenting, and preventing typical security problems.B. error prevention, requirements validation, memory use and reuse, commenting typical security problems, and testing code standards.C. error elimination, trash collection, documenting race conditions, peer review, and typical security problems.D. error handling, input validation, commenting, preventing typical security problems, managing customers, and documenting extra requirements. Answer: A QUESTION 26The sales division within a large organization purchased touch screen tablet computers for all 250 sales representatives in an effort to showcase the use of technology to its customers and increase productivity. This includes the development of a new product tracking application that works with the new platform. The security manager attempted to stop the deployment because the equipment and application are non-standard and unsupported within the organization. However, upper management decided to continue the deployment. Which of the following provides the BEST method for evaluating the potential threats? A. Conduct a vulnerability assessment to determine the security posture of the new devices and the application.B. Benchmark other organization's that already encountered this type of situation and apply all relevant learning's and industry best practices.C. Work with the business to understand and classify the risk associated with the full lifecycle of the hardware and software deployment.D. Develop a standard image for the new devices and migrate to a web application to eliminate locally resident data. Answer: C QUESTION 27A security audit has uncovered a lack of security controls with respect to employees' network account management. Specifically, the audit reveals that employee's network accounts are not disabled in a timely manner once an employee departs the organization. The company policy states that the network account of an employee should be disabled within eight hours of termination. However, the audit shows that 5% of the accounts were not terminated until three days after a dismissed employee departs. Furthermore, 2% of the accounts are still active.Which of the following is the BEST course of action that the security officer can take to avoid repeat audit findings? A. Review the HR termination process and ask the software developers to review the identity management code.B. Enforce the company policy by conducting monthly account reviews of

inactive accounts.C. Review the termination policy with the company managers to ensure prompt reporting of employee terminations.D. Update the company policy to account for delays and unforeseen situations in account deactivation. Answer: C QUESTION 28The Chief Executive Officer (CEO) has decided to outsource systems which are not core business functions; however, a recent review by the risk officer has indicated that core business functions are dependent on the outsourced systems. The risk officer has requested that the IT department calculates the priority of restoration for all systems and applications under the new business model. Which of the following is the BEST tool to achieve this? A. Business impact analysisB. Annualized loss expectancy analysisC. TCO analysisD. Residual risk and gap analysis Answer: A QUESTION 29A company has decided to relocate and the security manager has been tasked to perform a site survey of the new location to help in the design of the physical infrastructure.The current location has video surveillance throughout the building and entryways.The following requirements must be met:Able to log entry of all employees in and out of specific areas Access control into and out of all sensitive areas Tailgating preventionWhich of the following would MOST likely be implemented to meet the above requirements and provide a secure solution? (Select TWO). A. Discretionary Access controlB. Man trapC. Visitor logsD. Proximity readersE. Motion detection sensors Answer: BD QUESTION 30The Chief Executive Officer (CEO) of a corporation purchased the latest mobile device and connected it to the internal network. The CEO proceeded to download sensitive financial documents through their email. The device was then lost in transit to a conference. The CEO notified the company helpdesk about the lost device and another one was shipped out, after which the helpdesk ticket was closed stating the issue was resolved.This data breach was not properly reported due to insufficient training surrounding which of the following processes? A. E-DiscoveryB. Data handlingC. Incident responseD. Data recovery and storage Answer: C **CAS-002 dumps full version (PDF&VCE):** https://www.lead2pass.com/cas-002.html Large amount of free **CAS-002** exam questions on Google Drive: https://drive.google.com/open?id=13j5iOL_XYuK24xlefcIzTQtqmeQfLY7K