312-50v13 Dumps PDF 2025 Strategy Your Preparation Efficiently [Q95-Q115

312-50v13 Dumps PDF 2025 Strategy Your Preparation Efficiently
Latest Verified & Correct ECCouncil 312-50v13 Questions

NO.95 You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

- Use the cloud service provider&#8217;s encryption services but store keys on-premises.
- Use the cloud service provider&#8217;s default encryption and key management services.
- Rely on Secure Sockets Layer (SSL) encryption for data at rest.
- Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

The best practice to meet the client&#8217;s requirement is to encrypt data client-side before uploading to the cloud and retain control of the encryption keys. This practice is also known as client-side encryption or end-to-end encryption, and it involves encrypting the data on the client&#8217;s device using a software or hardware tool that generates and manages the encryption keys. The encrypted data is then uploaded to the cloud service, where it remains encrypted at rest. The encryption keys are never shared with the cloud service provider or any third party, and they are only used by the client to decrypt the data when needed. This way, the client can maintain full control over the encryption keys and the security of the data, even when the data is stored on a public cloud service12.

The other options are not as optimal as option D for the following reasons:

* A. Use the cloud service provider&#8217;s encryption services but store keys on-premises: This option is not feasible because it contradicts the client&#8217;s requirement of maintaining full control over the encryption keys. Using the cloud service provider&#8217;s encryption services means that the client has to rely on the cloud service provider to generate and manage the encryption keys, even if the keys are stored on- premises. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Moreover, storing the keys on-premises may introduce additional challenges, such as key distribution, synchronization, backup, and recovery3.

* B. Use the cloud service provider&#8217;s default encryption and key management services: This option is not desirable because it violates the client&#8217;s requirement of maintaining full control over the encryption keys. Using the cloud service provider&#8217;s default encryption and key management services means that the client has to trust the cloud service provider to encrypt and decrypt the data on the server-side, using the cloud service provider&#8217;s own encryption keys and mechanisms. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Furthermore, the cloud service provider&#8217;s default encryption and key management services may not meet the regulatory requirements or the security standards of the client4.

* C. Rely on Secure Sockets Layer (SSL) encryption for data at rest: This option is not sufficient because SSL encryption is not designed for data at rest, but for data in transit. SSL encryption is a protocol that encrypts the data as it travels over the internet between the client and the server, using certificates and keys that are exchanged and verified by both parties. SSL encryption can protect the data from being intercepted or modified by unauthorized parties, but it does not protect the data from being accessed or decrypted by the cloud service provider or any third party who has access to the server. Moreover, SSL encryption does not provide the client with any control over the encryption keys or the security of the data.

References:

* 1: Client-side encryption &#8211; Wikipedia

* 2: What is Client-Side Encryption? | Definition, Benefits & Best Practices | Kaspersky

* 3: Cloud Encryption Key Management: What You Need to Know | Thales

* 4: Cloud Encryption: How It Works and How to Use It | Comparitech

* : What is SSL Encryption and How Does it Work? | Norton

NO.96 Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?
* Advanced SMS phishing
* Bypass SSL pinning
* Phishing
* Tap &#8216;n ghost attack

NO.97 To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?
* Randomizing

* Bounding
* Mutating
* Fuzzing

NO.98 Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url:externaIsile.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed In the above scenario?
* website defacement
* Server-side request forgery (SSRF) attack
* Web server misconfiguration
* web cache poisoning attack
Server-side request forgery (also called SSRF) is a net security vulnerability that allows an assaulter to induce the server-side application to make http requests to associate arbitrary domain of the attacker&#8217;s choosing.

In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services among the organization&#8217;s infrastructure, or to external third-party systems.

Another type of trust relationship that often arises with server-side request forgery is where the application server is able to interact with different back-end systems that aren&#8217;t directly reachable by users. These systems typically have non-routable private informatics addresses. Since the back-end systems normally ordinarily protected by the topology, they typically have a weaker security posture. In several cases, internal back-end systems contain sensitive functionality that may be accessed while not authentication by anyone who is able to act with the systems.

In the preceding example, suppose there&#8217;s an body interface at the back-end url https://192.168.0.68/admin.

Here, an attacker will exploit the SSRF vulnerability to access the executive interface by submitting the following request:

POST /product/stock HTTP/1.0

Content-Type: application/x-www-form-urlencoded

Content-Length: 118

stockApi=http://192.168.0.68/admin

NO.99 What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?
* 110
* 135
* 139
* 161
* 445
* 1024

NO.100 You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee&#8217;s device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

* Provide employees with corporate-owned devices for work-related tasks.
* Implement a mobile device management solution that restricts the installation of non-approved applications.
* Require all employee devices to use a company-provided VPN for internet access.
* Conduct regular cybersecurity awareness training, focusing on phishing attacks.

The best measure to prevent similar attacks without overly restricting the use of personal devices is to conduct regular cybersecurity awareness training, focusing on phishing attacks. Cybersecurity awareness training is a process of educating and empowering employees on the best practices and behaviors to protect themselves and the organization from cyber threats, such as phishing, malware, ransomware, or data breaches. Cybersecurity awareness training can help the organization mitigate the risk of phishing incidents by providing the following benefits12:

* It can increase the knowledge and skills of employees on how to identify and avoid phishing emails, messages, or links, such as by checking the sender, the subject, the content, the attachments, and the URL of the message, and by verifying the legitimacy and authenticity of the message before responding or clicking.

* It can enhance the attitude and culture of employees on the importance and responsibility of cybersecurity, such as by encouraging them to report any suspicious or malicious activity, to follow the security policies and guidelines, and to seek help or guidance when in doubt or trouble.

* It can reduce the human error and negligence that are often the main causes of phishing incidents, such as by reminding employees to update their devices and applications, to use strong and unique passwords, to enable multi-factor authentication, and to backup their data regularly.

The other options are not as optimal as option D for the following reasons:

* A. Provide employees with corporate-owned devices for work-related tasks: This option is not feasible because it contradicts the BYOD policy, which allows employees to use their personal devices for work- related tasks. Providing employees with corporate-owned devices would require the organization to incur additional costs and resources, such as purchasing, maintaining, and securing the devices, as well as training and supporting the employees on how to use them. Moreover, providing employees with corporate-owned devices would not necessarily prevent phishing incidents, as the devices could still be compromised by phishing emails, messages, or links, unless the organization implements strict security controls and policies on the devices, which may limit the user autonomy and productivity3.

* B. Implement a mobile device management solution that restricts the installation of non-approved applications: This option is not desirable because it violates the user autonomy and privacy under the BYOD policy, which allows employees to use their personal devices for both personal and professional purposes. Implementing a mobile device management solution that restricts the installation of non- approved applications would require the organization to monitor and control the devices of the employees, which may raise legal and ethical issues, such as data ownership, consent, and compliance. Furthermore, implementing a mobile device management solution that restricts the installation of non-approved applications would not completely prevent phishing incidents, as the employees could still receive phishing emails, messages, or links through the approved applications, unless the organization implements strict security controls and policies on the applications, which may affect the user experience and functionality4.

* C. Require all employee devices to use a company-provided VPN for internet access: This option is not sufficient because it does not address the root cause of phishing incidents, which is the human factor.

Requiring all employee devices to use a company-provided VPN for internet access would provide the organization with some benefits, such as encrypting the network traffic, hiding the IP address, and bypassing geo-restrictions. However, requiring all employee devices to use a company-provided VPN for internet access would not prevent phishing incidents, as the employees could still fall victim to phishing emails, messages, or links that lure them to malicious websites or applications, unless the organization implements strict security controls and policies on the VPN, which may affect the network performance and reliability.

References:

* 1: What is Cybersecurity Awareness Training? | Definition, Benefits & Best Practices | Kaspersky

* 2: How to Prevent Phishing Attacks with Security Awareness Training | Infosec

* 3: BYOD vs. Corporate-Owned Devices: Pros and Cons | Bitglass

* 4: Mobile Device Management (MDM) | OWASP Foundation

* : What is a VPN and why do you need one? Everything you need to know | ZDNet

NO.101 Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim&#8217;s machine.

Joel waits for the victim to access the infected web application so as to compromise the victim&#8217;s machine.

Which of the following techniques is used by Joel in the above scenario?
* DNS rebinding attack
* Clickjacking attack
* MarioNet attack
* Watering hole attack
Web Application Threats &#8211; Watering Hole Attack In a watering hole attack, the attacker identifies the kinds of websites a target company/individual frequently surfs and tests those particular websites to identify any possible vulnerabilities. Attacker injects malicious script/code into the web application that can redirect the webpage and download malware onto the victim machine. (P.1797/1781)

NO.102 Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing &#8220;server publishing&#8221;?
* Overloading Port Address Translation
* Dynamic Port Address Translation
* Dynamic Network Address Translation
* Static Network Address Translation

NO.103 A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network.

What are some things he can do to prevent it? Select the best answers.
* Use port security on his switches.
* Use a tool like ARPwatch to monitor for strange ARP activity.
* Use a firewall between all LAN segments.
* If you have a small network, use static ARP entries.
* Use only static IP addresses on all PC&#8217;s.

NO.104 The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, &#8220;Implement strong access control measures&#8221;?
* Regularly test security systems and processes.
* Encrypt transmission of cardholder data across open, public networks.
* Assign a unique ID to each person with computer access.

* Use and regularly update anti-virus software on all systems commonly affected by malware.

NO.105 Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?
* Use the built-in Windows Update tool
* Use a scan tool like Nessus
* Check MITRE.org for the latest list of CVE findings
* Create a disk image of a clean Windows installation

NO.106 You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!

What seems to be wrong?
* The nmap syntax is wrong.
* This is a common behavior for a corrupted nmap application.
* The outgoing TCP/IP fingerprinting is blocked by the host firewall.
* OS Scan requires root privileges.

NO.107 Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?
* False-negative
* False-positive
* Brute force attack
* Backdoor
https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives- and-false-negatives/
False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn&#8217;t. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats &#8211; overlooked by security tooling because they&#8217;re dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

NO.108 You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?
* tcp.srcport= = 514 && ip.src= = 192.168.0.99
* tcp.srcport= = 514 && ip.src= = 192.168.150
* tcp.dstport= = 514 && ip.dst= = 192.168.0.99
* tcp.dstport= = 514 && ip.dst= = 192.168.0.150

NO.109 A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context

but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?
* The Python version installed on the CEH&#8217;s machine is incompatible with the Idap3 library
* The secure LDAP connection was not properly initialized due to a lack of &#8216;use_ssl = True&#8217; in the server object creation
* The enumeration process was blocked by the target system&#8217;s intrusion detection system
* The system failed to establish a connection due to an incorrect port number
The most plausible reason for the situation is that the secure LDAP connection was not properly initialized due to a lack of &#8216;use_ssl = True&#8217; in the server object creation. To use secure LDAP (LDAPS), the CEH needs to specify the use_ssl parameter as True when creating the server object with the ldap3 library in Python. This parameter tells the library to use SSL/TLS encryption for the LDAP communication. If the parameter is omitted or set to False, the library will use plain LDAP, which may not be accepted by the target system that only allows secure LDAP connections12. For example, the CEH can use the following code to create a secure LDAP server object:

from ldap3 import Server, Connection, ALL

server = Server(&#8216;ldaps://<target_ip>&#8217;, use_ssl=True, get_info=ALL)

connection = Connection(server, user='<username>&#8217;, password='<password>&#8217;) connection.bind() The other options are not as plausible as option B for the following reasons:

* A. The Python version installed on the CEH&#8217;s machine is incompatible with the ldap3 library: This option is unlikely because the ldap3 library supports Python versions from 2.6 to 3.9, which covers most of the commonly used Python versions3. Moreover, if the Python version was incompatible, the CEH would not be able to install the library or import it in the code, and would encounter errors before establishing the connection.

* C. The enumeration process was blocked by the target system&#8217;s intrusion detection system: This option is possible but not very plausible because the CEH was able to establish a connection with the target, which means the intrusion detection system did not block the initial handshake. Moreover, the enumeration process would not affect the response of the target system, but rather the visibility of the results. If the intrusion detection system detected and blocked the enumeration, the CEH would receive an error message or a blank response, not an unexpected response.

* D. The system failed to establish a connection due to an incorrect port number: This option is incorrect because the CEH was able to establish a connection with the target, which means the port number was correct. If the port number was incorrect, the CEH would not be able to connect to the target system at all, and would receive a connection refused error.

References:

* 1: ldap3 &#8211; LDAP library for Python

* 2: How to use LDAPS with Python &#8211; Stack Overflow

* 3: ldap3 2.9 documentation

NO.110 Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?
* DROWN attack

* Padding oracle attack
* Side-channel attack
* DUHK attack

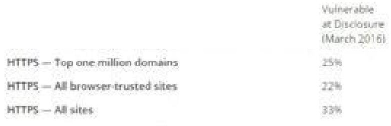
DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March

2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.

What will the attackers gain?Any communication between users and the server. This typically includes, however isn&#8217;t limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

Who is vulnerable?Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:



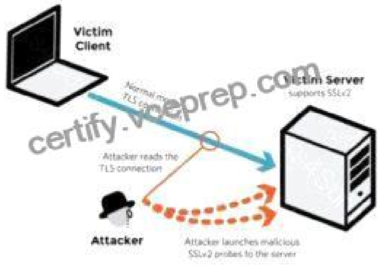
	Vulnerable at Disclosure (March 2016)
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

SSLv2

Operators of vulnerable servers got to take action. there&#8217;s nothing practical that browsers or end-users will do on their own to protect against this attack.

Is my site vulnerable?Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn&#8217;t thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.


Victim Client
Normal modern TLS connection
Victim Server
supports SSLv2
Attacker reads the TLS connection
Attacker
Attacker launches malicious SSLv2 probes to the server

SSLv2

* It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.

* Its private key is used on any other serverthat allows SSLv2 connections, even for another protocol.

Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.

A server is vulnerable to DROWN if:SSLv2

How do I protect my server?To protect against DROWN, server operators need to ensure that their private keys software used anyplace with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.

Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:

OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s. Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for &#8216;Server&#8217;, as outlined in KB245030. albeit users haven&#8217;t taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don&#8217;t seem to be supported by default.

Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more moderen version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere Other affected software and in operation systems:

Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat

Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar ready to take action to guard against the attack.

NO.111 Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (GHDB) with an emphasis on VPN footprinting.

Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?
* intitle: This operator restricts results to only the pages containing the specified term in the title
* location: This operator finds information for a specific location
* inur: This operator restricts the results to only the pages containing the specified word in the URL
* link: This operator searches websites or pages that contain links to the specified website or page

The location: operator is the least useful in providing the attacker with sensitive VPN-related information, because it does not directly relate to VPN configuration, credentials, or vulnerabilities. The location: operator finds information for a specific location, such as a city, country, or region. For example, location:paris would return results related to Paris, France. However, this operator does not help the attacker to identify or access VPN servers or clients, unless they are specifically named or indexed by their location, which is unlikely.

The other operators are more useful in providing the attacker with sensitive VPN-related information, because they can help the attacker to find pages or files that contain VPN configuration, credentials, or vulnerabilities.

The intitle: operator restricts results to only the pages containing the specified term in the title. For example, intitle:vpn would return pages with VPN in their title, which may include VPN guides, manuals, or tutorials.

The inurl: operator restricts the results to only the pages containing the specified word in the URL. For example, inurl:vpn would return pages with VPN in their URL, which may include VPN login portals, configuration files, or directories. The link: operator searches websites or pages that contain links to the specified website or page. For example, link:vpn.com would return pages that link to vpn.com, which may include VPN reviews, comparisons, or recommendations. References:

* Google Search Operators: The Complete List (44 Advanced Operators)

* Footprinting through search engines

* Module 02: Footprinting and Reconnaissance

NO.112 Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?
* LNMIB2.MIB
* WINS.MIB
* DHCP.MIS
* MIB_II.MIB
DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts

# HOSTMIB.MIB: Monitors and manages host resources

# LNMIB2.MIB: Contains object types for workstation and server services

# MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system

# WINS.MIB: For the Windows Internet Name Service (WINS)

NO.113 When a security analyst prepares for the formal security assessment &#8211; what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?
* Data items and vulnerability scanning
* Interviewing employees and network engineers
* Reviewing the firewalls configuration
* Source code review

NO.114 A company&#8217;s Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?
* Cross-site scripting vulnerability
* SQL injection vulnerability
* Web site defacement vulnerability
* Gross-site Request Forgery vulnerability
There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws: non-persistent and persistent. In this issue, we consider the non-persistent cross-site scripting vulnerability.

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross- site scripting flaw will ensue.

NO.115 John, a security analyst working for an organization, found a critical vulnerability on the organization&#8217;s LAN that allows him to view financial and personal information about the rest of the employees. Before reporting the vulnerability, he examines the information shown by the vulnerability for two days without disclosing any information to third parties or other internal employees. He does so out of curiosity about the other employees and may take advantage of this information later. What would John be considered as?
* Cybercriminal
* Black hat
* White hat
* Gray hat

312-50v13 PDF Dumps Are Helpful To produce Your Dreams Correct QA's:
https://www.vceprep.com/312-50v13-latest-vce-prep.html]