

RC0-501^{Q&As}

CompTIA Security+ Recertification Exam

Pass CompTIA RC0-501 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/rc0-501.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

- A. Header manipulation
- B. Cookie hijacking
- C. Cross-site scripting
- D. Xml injection

Correct Answer: A

QUESTION 2

For each of the given items, select the appropriate authentication category from the drop down choices.

Item	Response
Fingerprint scan	<input type="text"/>
Hardware token	<input type="text"/>
Smart card	<input type="text"/>
Password	<input type="text"/>
PIN number	<input type="text"/>
Retina Scan	<input type="text"/>

Select the appropriate authentication type for the following items:

Hot Area:

Item	Response
Fingerprint scan	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
PIN number	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Retina Scan	<input type="text"/> Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication

Correct Answer:

Item	Response
Fingerprint scan	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Hardware token	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Smart card	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Password	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
PIN number	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication
Retina Scan	<ul style="list-style-type: none">Biometric authenticationOne Time PasswordMulti-factorPAP authenticationPAP authenticationBiometric authentication

Biometrics refers to a collection of physical attributes of the human body that can be used as identification or an authentication factor. Fingerprints and retinas are physical attributes of the human body.

Two types of tokens exist, Time-based one-time password (TOTP) tokens and HMACbased one-time password (HOTP). TOTP tokens generate passwords at fixed time intervals, whereas HOTP tokens generate passwords not based on fixed

time intervals but instead based on a non-repeating one-way function, such as a hash or HMAC operation.

Smart cards can have Multi-factor and proximity authentication embedded into it.

PAP allows for two entities to share a password in advance and use the password as the basis of authentication. The same goes for PIN numbers.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 282, 285

http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle

http://en.wikipedia.org/wiki/Smart_card#Security

QUESTION 3

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?

- A. Service level agreement
- B. Interconnection security agreement
- C. Non-disclosure agreement
- D. Business process analysis

Correct Answer: A

QUESTION 4

An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

- A. Certificate pinning
- B. Certificate stapling
- C. Certificate chaining
- D. Certificate with extended validation

Correct Answer: A

QUESTION 5

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

- A. An ephemeral key was used for one of the messages
- B. A stream cipher was used for the initial email; a block cipher was used for the reply
- C. Out-of-band key exchange has taken place
- D. Asymmetric encryption is being used

Correct Answer: D

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are

referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

[Latest RC0-501 Dumps](#)

[RC0-501 Practice Test](#)

[RC0-501 Study Guide](#)