SY0-601$^{\text{Q\&As}}$

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.geekcert.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security engineer is installing a WF io protect the company\\'s website from malicious wed requests over SSL, Which of the following is needed io meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A split-tunnel VPN

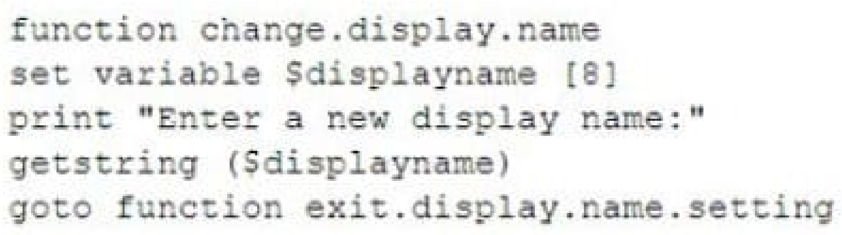
D. Load-balanced servers

Correct Answer: B

WAF can only block abnormal traffic by filtering the plaintext data.

QUESTION 2

While performing a threat-hunting exercise, a security analyst sees some unusual behavior occurring in an application when a user changes the display name. The security analyst decides to perform a static code analysis and receives the following pseudocode:



```
function change.display.name
set variable $displayname [8]
print "Enter a new display name:"
getstring ($displayname)
goto function exit.display.name.setting
```

Which of the following attack types best describes the root cause of the unusual behavior?

A. Server-side request forgery

B. Improper error handling

C. Buffer overflow

D. SQL injection

Correct Answer: D

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input12. A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system3. According to the pseudocode given in the question, the application takes a user input for display name and concatenates it with a SQL query to update the user\\'s profile. This is a vulnerable practice that allows an attacker to inject malicious SQL code into the query and execute it on the database. For example, an attacker could enter something like this as their display name: John\\'; DROP TABLE users; -This would result in the following SQL query being executed: UPDATE profile SET displayname = \\'John\\'; DROP TABLE users; --\\' WHERE userid = 1; The semicolon (;) terminates the original update statement and starts a new one that drops the users table. The double dash (? comments out the rest of the query. This would cause a catastrophic loss of data for the application.

QUESTION 3

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption

B. Data masking

C. Anonymization

D. Tokenization

Correct Answer: B

Tokenization means that all or part of data in a field is replaced with a randomly generated token. The token is stored with the original value on a token server or token vault, separate to the production database. An authorized query or app can retrieve the original value from the vault, if necessary, so tokenization is a reversible technique. Tokenization is used as a substitute for encryption, because from a regulatory perspective an encrypted field is the same value as the original data.

QUESTION 4

A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security contral standards.

Which of the following is the MOST likely source of the breach?

A. Side channel

B. Supply chain

C. Cryptographic downgrade

D. Malware

Correct Answer: B

Based on the information provided, the most likely source of the breach is the supply chain. The breach occurred when customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor. This indicates that the vendor, who is part of the supply chain, may not have the same level of security control standards as the company itself, making it a potential weak link in the overall security posture. Supply chain attacks involve targeting third-party vendors, suppliers, or business partners as a means to gain unauthorized access to the main target organization\\'s systems or data.

QUESTION 5

An enterpnse has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box

B. Red-leam

C. Bug bounty

D. Gray-box

E. Black-box

Correct Answer: C

A bug bounty program provides a monetary incentive for security researchers to discover vulnerabilities. One of the benefits is that bug bounty programs only pay researchers when they find vulnerabilities. Companies don\\'t pay researchers for their time.

Reference: https://en.wikipedia.org/wiki/Bug_bounty_program