ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Cisco

Code: 350-701

Exam: Implementing and Operating Cisco Security Core Technologies (SCOR)

https://www.examsnest.com/exam/350-701/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 32.3

Question: 1

[Security Concepts]
In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

A. Smurf
B. distributed denial of service
C. cross-site scripting
D. rootkit exploit

Answer: C

Explanation:

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.
Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on.
For example the code below is written in hex: <a
href=javascript:alert&#
x28'XSS')>Click Here
is equivalent to:
Click Here
Note: In the format "&#xhhhh", hhhh is the code point in hexadecimal form.

Question: 2

[Security Concepts]
Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

A. user input validation in a web page or web application
B. Linux and Windows operating systems
C. database
D. web page images

Answer: A

Explanation:

SQL injection usually occurs when you ask a user for input, like their username/userid, but the user gives ("injects") you an SQL statement that you will unknowingly run on your database. For example:
Look at the following example, which creates a SELECT statement by adding a variable (txtUserId) to a select
string. The variable is fetched from user input (getRequestString):
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
If user enter something like this: "100 OR 1=1" then the SzQL statement will look like this:
SELECT * FROM Users WHERE UserId = 100 OR 1=1;
The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE. A hacker might get access to all the user names and passwords in this database.

Question: 3

[Security Concepts]
Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two)

A. Check integer, float, or Boolean string parameters to ensure accurate values.
B. Use prepared statements and parameterized queries.
C. Secure the connection between the web and the app tier.
D. Write SQL code instead of using object-relational mapping libraries.
E. Block SQL code execution in the web application database login.

Answer: B,E

Explanation:

SQL injection attacks are a type of code injection technique that exploit the use of dynamic SQL queries in web applications. Attackers can inject malicious SQL statements into user input fields, such as login forms, search boxes, or URLs, and execute them on the underlying database. This can result in unauthorized access, data theft, data corruption, or denial of service.
To prevent SQL injection attacks, web developers should use the following techniques:
Use prepared statements and parameterized queries: Prepared statements are SQL queries that are precompiled and executed with user-supplied parameters. Parameterized queries are SQL queries that use placeholders for user input and bind them to actual values at runtime. Both techniques separate the SQL code from the user input, making it impossible for attackers to inject SQL commands into the query. For example, in Java, PreparedStatement is a class that implements parameterized queries. In PHP, PDO and mysqli are extensions that support prepared statements.
Block SQL code execution in the web application database login: Web applications should use a dedicated database user account with limited privileges to connect to the database. This account should only have the permissions necessary to perform the required operations, such as select, insert, update, or delete. It should not have the permissions to execute arbitrary SQL commands, such as create, drop, alter, grant, or revoke. This way, even if an attacker manages to inject SQL code into the query, the database will reject it due to insufficient privileges.
Reference:

[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 5: Securing the Cloud, Lesson 5.2: Cloud Application Security, Topic 5.2.2: SQL Injection
SQL Injection Prevention - OWASP Cheat Sheet Series
How to Prevent SQL Injection: 5 Key Prevention Methods - eSecurityPlanet
How to Protect Against SQL Injection Attacks

Question: 4

[Content Security]
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two)

A. Patch for cross-site scripting.
B. Perform backups to the private cloud.
C. Protect against input validation and character escapes in the endpoint.

D. Install a spam and virus email filter.
E. Protect systems with an up-to-date antimalware program

Answer: D,E

Explanation:

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable
source. It is usually done through email. The goal is to steal sensitive data like credit card and login information,
or to install malware on the victim's machine.

Question: 5

[Content Security]
Which two mechanisms are used to control phishing attacks? (Choose two)

A. Enable browser alerts for fraudulent websites.
B. Define security group memberships.
C. Revoke expired CRL of the websites.
D. Use antispyware software.
E. Implement email filtering techniques.

Answer: A,E

Explanation:

Phishing attacks are a type of social engineering that aim to trick users into revealing their personal or financial information, or installing malware on their devices. To control phishing attacks, users and organizations need to implement various preventive and reactive measures, such as:
Enable browser alerts for fraudulent websites. Most modern browsers have built-in features that can warn users when they visit a website that is suspected of being malicious or impersonating a legitimate entity. These alerts can help users avoid falling for phishing scams that use fake web pages to capture their credentials or other sensitive data. For example, Google Chrome has a Safe Browsing feature that

displays a red warning page when users try to access a deceptive site. Users should always pay attention to these alerts and avoid proceeding to untrusted sites.
Implement email filtering techniques. Email is one of the most common channels for phishing attacks, as attackers can send spoofed messages that appear to come from trusted sources, such as banks, government agencies, or colleagues. Email filtering techniques can help block or flag suspicious emails based on various criteria, such as the sender's address, the subject line, the content, or the attachments. For example, Microsoft Outlook has a Junk Email Filter that can move potential phishing emails to a separate folder or delete them automatically. Users should also be careful not to open or reply to any unsolicited or unexpected emails, especially those that ask for personal or financial information, or contain links or attachments.
Other mechanisms that can help control phishing attacks include:
Use strong passwords and enable two-factor authentication. Even if users fall victim to phishing attacks and reveal their passwords, they can still protect their accounts by using strong and unique passwords for each service, and enabling two-factor authentication (2FA) whenever possible. 2FA adds an extra layer of security by requiring users to enter a code or a token that is sent to their phone or email, or generated by an app, in addition to their password. This way, even if attackers obtain the password, they cannot access the account without the second factor.
Don't ignore update messages. Users should always keep their operating systems, browsers, and applications updated with the latest security patches and fixes. These updates can help prevent phishing attacks that exploit known vulnerabilities or bugs in the software. Users should also use antivirus and antispyware software that can detect and remove malware that may be installed by phishing attacks.
Exercise caution when opening emails or clicking on links. Users should always be skeptical and vigilant when they receive emails or messages that ask them to take urgent or unusual actions, such as verifying their account, updating their payment information, or downloading a file. Users should also check the sender's address, the spelling and grammar, and the URL of any links before clicking on them. Users can hover over the link to see the actual destination, or use a link scanner tool, such as VirusTotal, to check if the link is malicious or not.
Reference :=
1: https://safebrowsing.google.com/ 2: https://support.microsoft.com/en-us/office/overview-of-the-junk-email-filter-5ae3ea8e-cf41-4fa0-b02a-3b96e21de089 3: https://www.virustotal.com/gui/home/url

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Cisco

Code: 350-701

Exam: Implementing and Operating Cisco Security Core Technologies (SCOR)

https://www.examsnest.com/exam/350-701/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation