

Iniziato	domenica, 17 dicembre 2023, 11:15
Stato	Completato
Terminato	domenica, 17 dicembre 2023, 11:15
Tempo impiegato	28 secondi
Valutazione	5,00 su un massimo di 6,00 (83,33%)

Domanda 1

Risposta corretta

Select which attack does not involve social engineering among the following ones:

- ☒ a. Data Masking: a technique used to protect sensitive information by replacing it with fictional or obfuscated data ✓
- ☐ b. Phishing: sending fraudulent emails or messages that appear to be from a trustworthy source to deceive individuals into revealing sensitive information or performing certain actions
- ☐ c. Impersonation: Pretending to be someone else, such as a coworker or a representative from a reputable organization, to gain trust and manipulate individuals into providing confidential information

Risposta corretta.

La risposta corretta è:

Data Masking: a technique used to protect sensitive information by replacing it with fictional or obfuscated data

Domanda 2

Risposta corretta

How can you attack an app by exploiting dynamic code loading technique?

- ☐ a. By inspecting the code to be dynamically loaded in the private directory of the app
- ☒ b. By replacing the original downloaded binary file with a malicious one ✓
- ☐ c. By sniffing the network traffic during the download of the binary file from a remote server

Risposta corretta.

La risposta corretta è:

By replacing the original downloaded binary file with a malicious one

Domanda 3[Webmail](#) | [Uniweb](#)

Risposta errata

Which is NOT a possible reason that leads towards cryptographic vulnerabilities?

- ☒ a. Misuse of cryptographic libraries ✖
- ☐ b. Network traffic in cleartext
- ☐ c. Poor implementation of cryptographic libraries

Risposta errata.

La risposta corretta è:

Network traffic in cleartext

Domanda 4

Risposta corretta

What is the Android Confused Deputy attack, and how does it work? Select the correct answer

- ☒ a. The Confused Deputy attack is a security vulnerability that occurs when an Android app grants excessive permissions to other apps without appropriate authorization checks. It allows a malicious app to misuse the granted permissions and access sensitive user data or perform unauthorized actions. ✔
- ☐ b. The Confused Deputy attack is a method of exploiting vulnerabilities in the Android operating system to gain unauthorized root access to a device. It works by bypassing the security mechanisms and gaining escalated privileges.
- ☐ c. The Confused Deputy attack is a social engineering technique where an attacker tricks an Android user into downloading and installing a malicious app that steals sensitive information. The attack typically involves phishing emails or fake app stores.

Risposta corretta.

La risposta corretta è:

The Confused Deputy attack is a security vulnerability that occurs when an Android app grants excessive permissions to other apps without appropriate authorization checks. It allows a malicious app to misuse the granted permissions and access sensitive user data or perform unauthorized actions.

What is Android overpermissioning, and what are its implications?

- ☐ a. Android overpermissioning refers to the practice of granting unnecessary permissions to Android apps, leading to reduced performance and increased battery consumption.
- ☐ b. Android overpermissioning is a technique used by malicious apps to gain unauthorized access to user data by exploiting vulnerabilities in the Android operating system.
- ☒ c. Android overpermissioning is the phenomenon where Android apps request more permissions than necessary for their intended functionality. This can potentially expose user data to privacy risks and increase the attack surface for potential security breaches. ✓

Risposta corretta.

La risposta corretta è:

Android overpermissioning is the phenomenon where Android apps request more permissions than necessary for their intended functionality. This can potentially expose user data to privacy risks and increase the attack surface for potential security breaches.

What is zip path traversal, and how does it pose a security risk?

- ☐ a. Zip path traversal is a feature in ZIP compression that allows users to navigate through the directory structure of a compressed archive. While it may confuse users, it does not pose any security risk.
- ☒ b. Zip path traversal is a security vulnerability that allows an attacker to extract files to arbitrary locations on a system, potentially overwriting sensitive files or executing malicious code. ✓
- ☐ c. Zip path traversal is a technique used to compress and extract files and folders in a compressed ZIP archive. It does not pose any security risk but is solely a method for managing files.

Risposta corretta.

La risposta corretta è:

Zip path traversal is a security vulnerability that allows an attacker to extract files to arbitrary locations on a system, potentially overwriting sensitive files or executing malicious code.