

Question **4**

Answer saved

Marked out of
1

🚩 Flag
question

In one of fundamental security design principles, access decisions should be based on permissions; i.e., the default is lack of access. This called?

- ☐ a. least common mechanism
- ☐ b. Economy of mechanism
- ☒ c. Fail-safe defaults
- ☐ d. least privilege

[Clear my choice](#)

Question **5**

Answer saved

Marked out of
1

🚩 Flag
question

If the mobile app stores any passwords or shared secrets locally on the device, it most likely suffers from

- ☒ a. Insecure authentication
- ☐ b. Insecure Data
- ☐ c. Insufficient cryptography
- ☐ d. bad cod quality

[Clear my choice](#)

Question 6

Answer saved

Marked out of
3

Flag
question

What is sending premium-rate SMS fraud attack?



It's a type of fraud where the victim is sent fake SMS messages tricking him into calling a certain number, or responding with a message, with very high fees of course.

Once the user responds or gets tricked, he loses money either from his balance, or he will see a huge phone bill at the end of the month.

Question **7**

Answer saved

Marked out of
1

🚩 Flag
question

Using of TLS protocol can solve the problem of:

- ☐ a. Reverse Engineering
- ☐ b. Extraneous Functionality
- ☐ c. Insecure Authentication
- ☒ d. insecure communication

[Clear my choice](#)

Question 8

Answer saved

Marked out of
2

Flag
question

Look to the following mobile message, do you think is it a phishing message? Justify your answer.



Yes.

1. It's saying that I've won a huge amount of money which is very unbelievable.
2. It's spoofing a popular company's name.
3. It's asking me to go to a suspicious looking website to claim my prize, why not just contact me through phone?
4. The helpline e-mail clearly has nothing to do with the company itself.
5. The way "Alert!!:Your..." is written is very weird and abnormal.

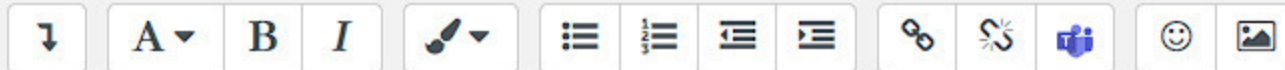
Question 9

Answer saved

Marked out of
3

Flag
question

Is a Google business strategy(Android) play role in the appearance of security issues comparing with Apple's business strategy (IOs)? Discuss your answer



No, Google's Android is a very secure system when you're downloading apps only from Play Store, so the problem is not with the system, the problem is when a user starts side-loading apps from untrusted sources, putting his mobile phone at risk. It's a good thing to have freedom to do whatever you want with an operating system, but you will be doing it at your own risk.

Question **10**

Answer saved

Marked out of
1

🚩 Flag
question

implement platform-specific best security practices for the mobile interface and server-side operations is the best solution for:

- ☐ a. Insecure Data
- ☐ b. Code Tampering
- ☐ c. Extraneous Functionality
- ☒ d. Improper Platform Usage

[Clear my choice](#)

Question **11**

Answer saved

Marked out of
1

🚩 Flag
question

Possession-based authentication is:

- ☒ a. Something you have
- ☐ b. Something you know
- ☐ c. Something you are
- ☐ d. Something you prefer

[Clear my choice](#)

Question **12**

Answer saved

Marked out of
1

🚩 Flag
question

the "Economy of Mechanism" principle means that The design of security measures should be as complex as possible in order to reduce the system vulnerabilities.

Select one:

- ☐ True
- ☒ False

Question **13**

Answer saved

Marked out of
1

🚩 Flag
question

If a developer accidentally includes a password as a comment in a hybrid app. This risk could be classified under :

- ☐ a. Brute force attack
- ☐ b. obfuscation tools
- ☒ c. Extraneous Functionality
- ☐ d. Code Tampering

[Clear my choice](#)

Question **14**

Answer saved

Marked out of
1

🚩 Flag
question

The weakest authentication method in smartphones in case you are a famous YouTuber

- ☒ a. Face unlock
- ☐ b. PIN
- ☐ c. Password
- ☐ d. Pattern lock

[Clear my choice](#)

Question **15**

Answer saved

Marked out of
1

🚩 Flag
question

If the app uses a weak cryptography algorithm, this could cause:

- ☐ a. Insecure Data
- ☐ b. Insecure Authentication
- ☐ c. Insecure Communication
- ☒ d. Insufficient cryptography

[Clear my choice](#)

[Previous page](#)

[Next page](#)

Question **16**

Answer saved

Marked out of
1

🚩 Flag
question

Our privacy is the most important thing that we could lose in case if our smartphone attacked

Select one:

☒ True

☐ False

Question **17**

Answer saved

Marked out of
1

🚩 Flag
question

Using IMEI, a hacker can control your phone or any apps installed

Select one:

☐ True

☒ False

Question **18**

Answer saved

Marked out of
1

🚩 Flag
question

The hiding of the internal system structure to increase security, this principle called :

- ☒ a. Encapsulation
- ☐ b. Modularity
- ☐ c. Isolation
- ☐ d. Economy of mechanism

[Clear my choice](#)

Question **19**

Answer saved

Marked out of
1

🚩 Flag
question

Insecure Authentication may give an attacker useful information on an application's logic and security measures

Select one:

☐ True

☒ False

Question **20**

Answer saved

Marked out of
1

🚩 Flag
question

Vulnerabilities like buffer overflow and format string could be existed due to:

- ☐ a. Code Tampering
- ☐ b. insecure authentication
- ☒ c. Code quality
- ☐ d. Extraneous Functionality

[Clear my choice](#)

Question **21**

Answer saved

Marked out of
1

🚩 Flag
question

MASVS serves as a baseline for manual security testing and as a template for automated security tests during or after development

Select one:

☒ True

☐ False

Question **22**

Answer saved

Marked out of
1

🚩 Flag
question

In one of fundamental security design principles, use of multiple, overlapping protection approaches.

- ☒ a. Layering
- ☐ b. Modularity
- ☐ c. Encapsulation
- ☐ d. Isolation

[Clear my choice](#)

Question 23

Answer saved

Marked out of
3Flag
question

Many websites provide fishing attack for hackers (fishing insight, Z-shadow, etc.), is it safe to use these websites? Justify your answer.



Of course not, because you can not guarantee the safety and privacy of the information you got through phishing, also, your login credentials that you used to login to that website can possibly be used against you.

Any usernames and passwords you get through phishing will be stored in the database of that website and they will most likely use them for benefit.

Question 1

Answer saved

Marked out of
1

Flag
question

In one of **Fundamental security design principles**, security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access. This called?

- ☐ a. least common mechanism
- ☐ b. Economy of mechanism
- ☒ c. psychological accountability
- ☐ d. Fail-safe defaults

[Clear my choice](#)

Question **2**

Answer saved

Marked out of
1

🚩 Flag
question

Using the data stored in memory to access the system rather than get back to a database stored in H.D could increase the performance of any system, but that could break a system's security. to resolve this problem we should apply the following principle:


- ☒ a. complete mediation
- ☐ b. least common mechanism
- ☐ c. Economy of mechanism
- ☐ d. Open design

[Clear my choice](#)

Question **3**

Answer saved

Marked out of
1

 Remove
flag

If the modification or update of security mechanisms used in my systems regardless of any system that uses these mechanisms specifically

- ☐ a. Isolation
- ☐ b. Economy of mechanism
- ☒ c. Modularity
- ☐ d. Encapsulation

[Clear my choice](#)