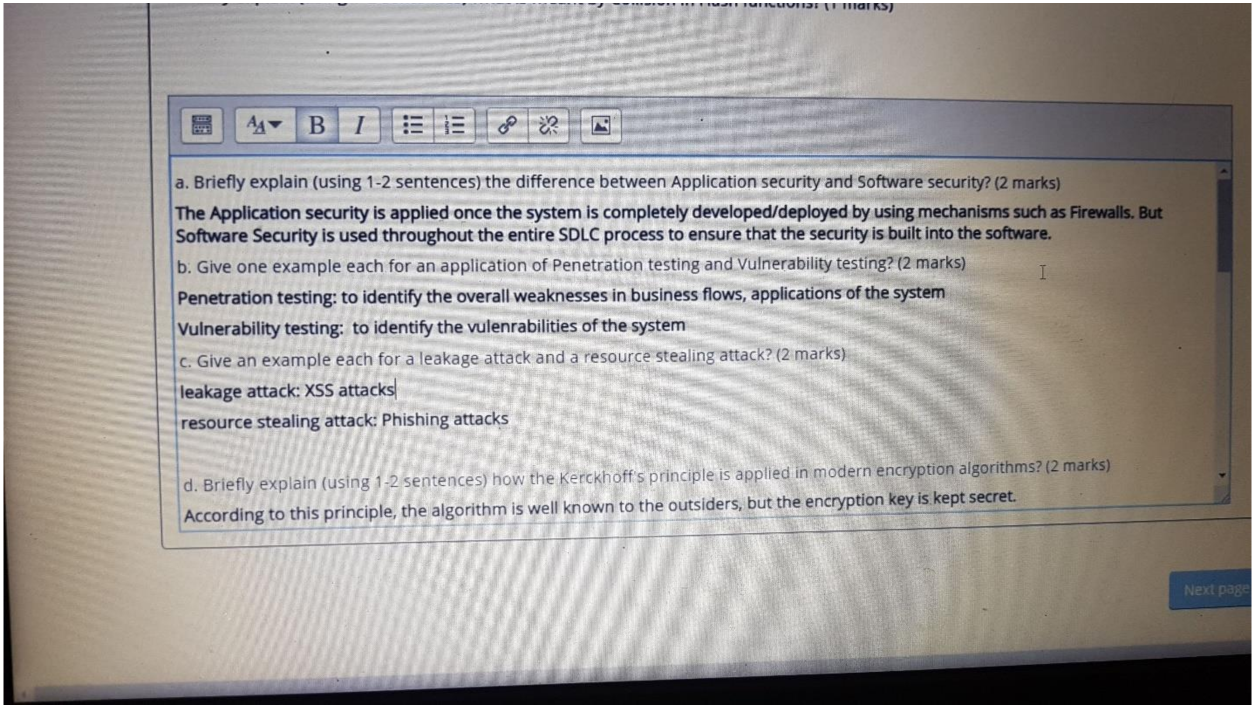
Answer Document

SSD

Question 1(a)



a. Briefly explain (using 1-2 sentences) the difference between Application security and Software security? (2 marks)

The Application security is applied once the system is completely developed/deployed by using mechanisms such as Firewalls. But Software Security is used throughout the entire SDLC process to ensure that the security is built into the software.

b. Give one example each for an application of Penetration testing and Vulnerability testing? (2 marks)

Penetration testing: to identify the overall weaknesses in business flows, applications of the system

Vulnerability testing: to identify the vulenrabilities of the system

c. Give an example each for a leakage attack and a resource stealing attack? (2 marks)

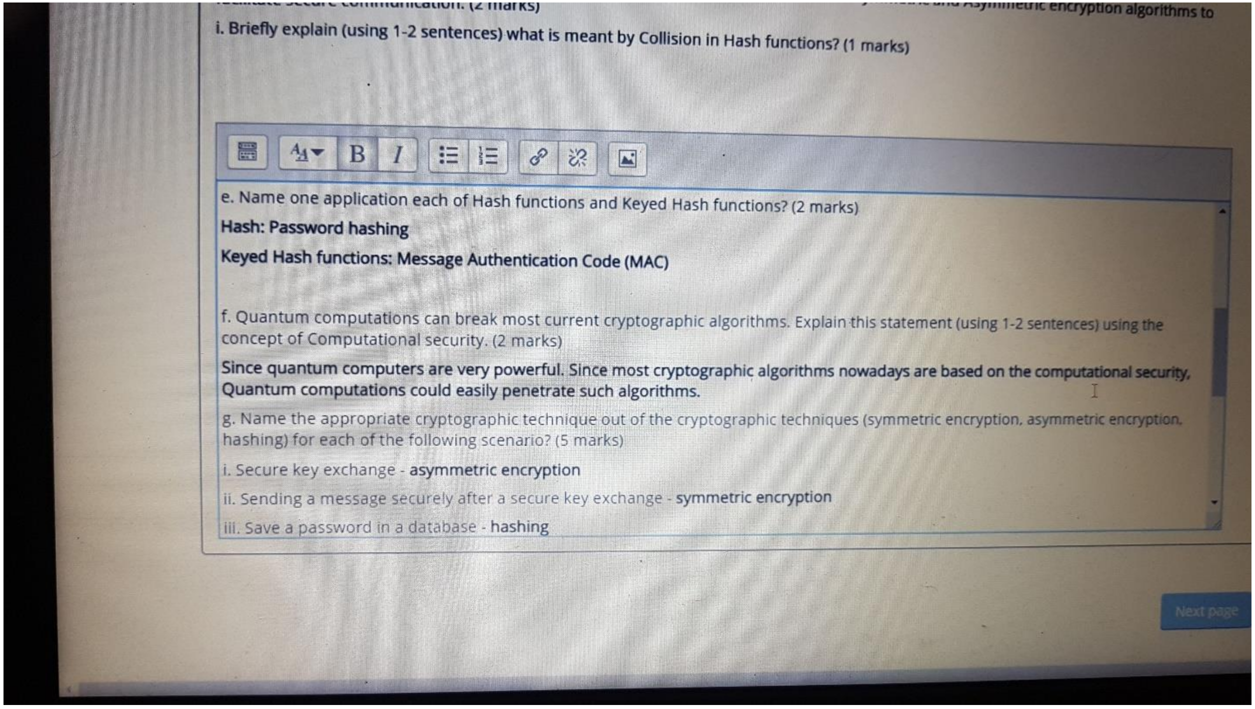
leakage attack: XSS attacks

resource stealing attack: Phishing attacks

d. Briefly explain (using 1-2 sentences) how the Kerckhoff's principle is applied in modern encryption algorithms? (2 marks)

According to this principle, the algorithm is well known to the outsiders, but the encryption key is kept secret.

Question 1(b)



i. Briefly explain (using 1-2 sentences) what is meant by Collision in Hash functions? (1 marks)

e. Name one application each of Hash functions and Keyed Hash functions? (2 marks)

Hash: Password hashing

Keyed Hash functions: Message Authentication Code (MAC)

f. Quantum computations can break most current cryptographic algorithms. Explain this statement (using 1-2 sentences) using the concept of Computational security. (2 marks)

Since quantum computers are very powerful. Since most cryptographic algorithms nowadays are based on the computational security, Quantum computations could easily penetrate such algorithms.

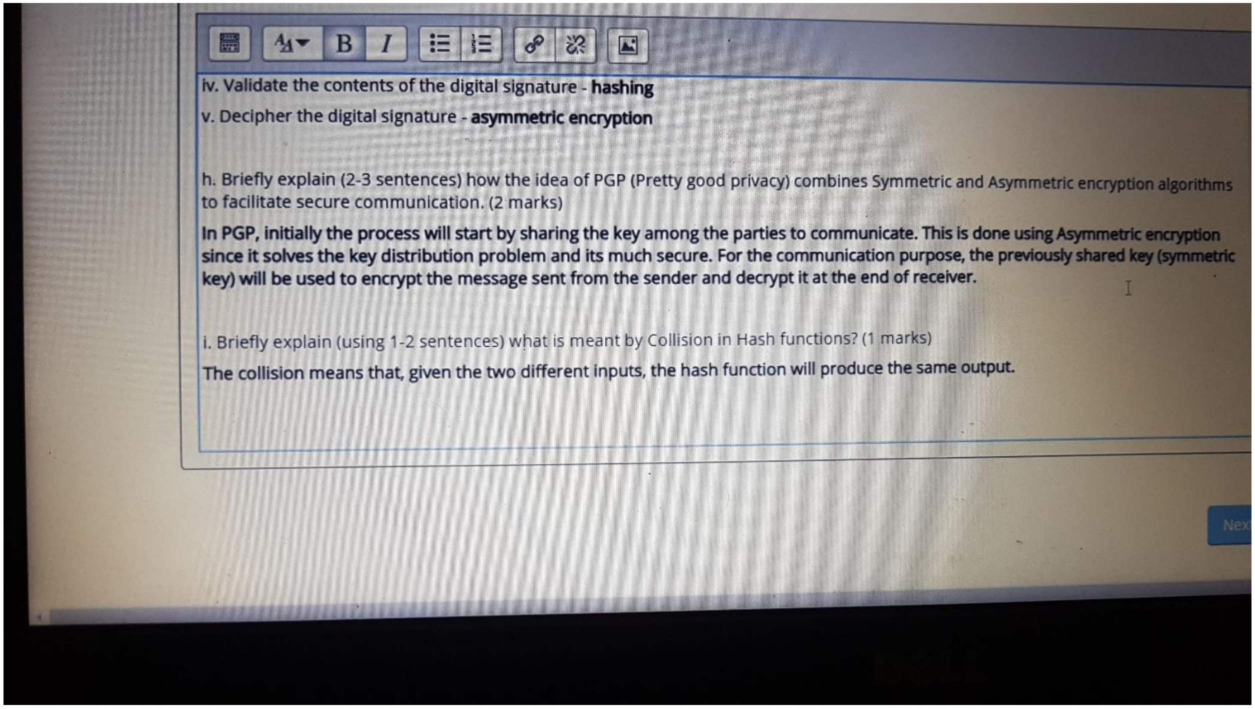
g. Name the appropriate cryptographic technique out of the cryptographic techniques (symmetric encryption, asymmetric encryption, hashing) for each of the following scenario? (5 marks)

i. Secure key exchange - asymmetric encryption

ii. Sending a message securely after a secure key exchange - symmetric encryption

iii. Save a password in a database - hashing

Question 1(c)



iv. Validate the contents of the digital signature - **hashing**

v. Decipher the digital signature - **asymmetric encryption**

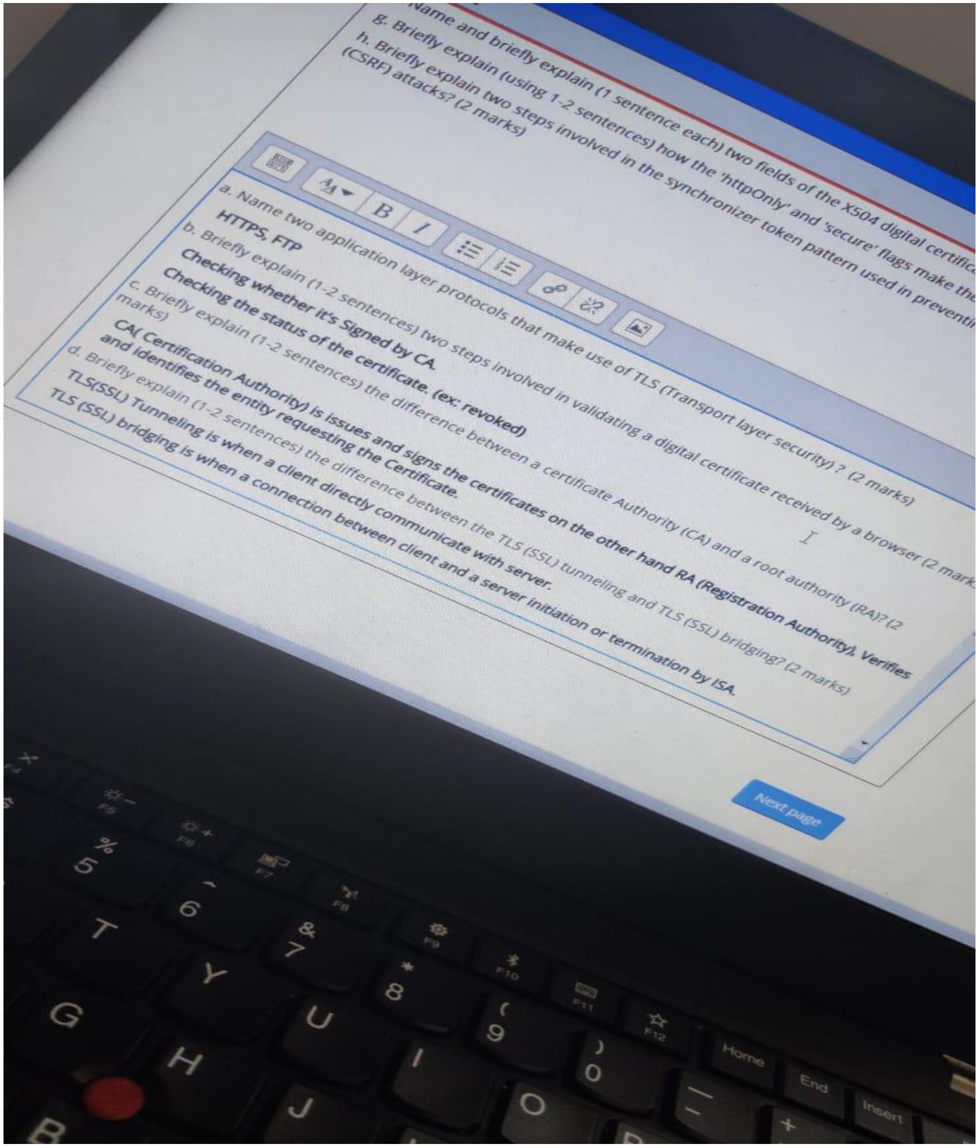
h. Briefly explain (2-3 sentences) how the idea of PGP (Pretty good privacy) combines Symmetric and Asymmetric encryption algorithms to facilitate secure communication. (2 marks)

In PGP, initially the process will start by sharing the key among the parties to communicate. This is done using Asymmetric encryption since it solves the key distribution problem and its much secure. For the communication purpose, the previously shared key (symmetric key) will be used to encrypt the message sent from the sender and decrypt it at the end of receiver.

i. Briefly explain (using 1-2 sentences) what is meant by Collision in Hash functions? (1 marks)

The collision means that, given the two different inputs, the hash function will produce the same output.

Question 2(a)



Name and briefly explain (1 sentence each) two fields of the X504 digital certific

g. Briefly explain (using 1-2 sentences) how the 'httpOnly' and 'secure' flags make the

h. Briefly explain two steps involved in the synchronizer token pattern used in preventi (CSRF) attacks? (2 marks)

a. Name two application layer protocols that make use of TLS (Transport layer security) ? (2 marks)

HTTPS, FTP

b. Briefly explain (1-2 sentences) two steps involved in validating a digital certificate received by a browser (2 mark

Checking whether it's Signed by CA.

Checking the status of the certificate. (ex: revoked)

c. Briefly explain (1-2 sentences) the difference between a certificate Authority (CA) and a root authority (RA)? (2 marks)

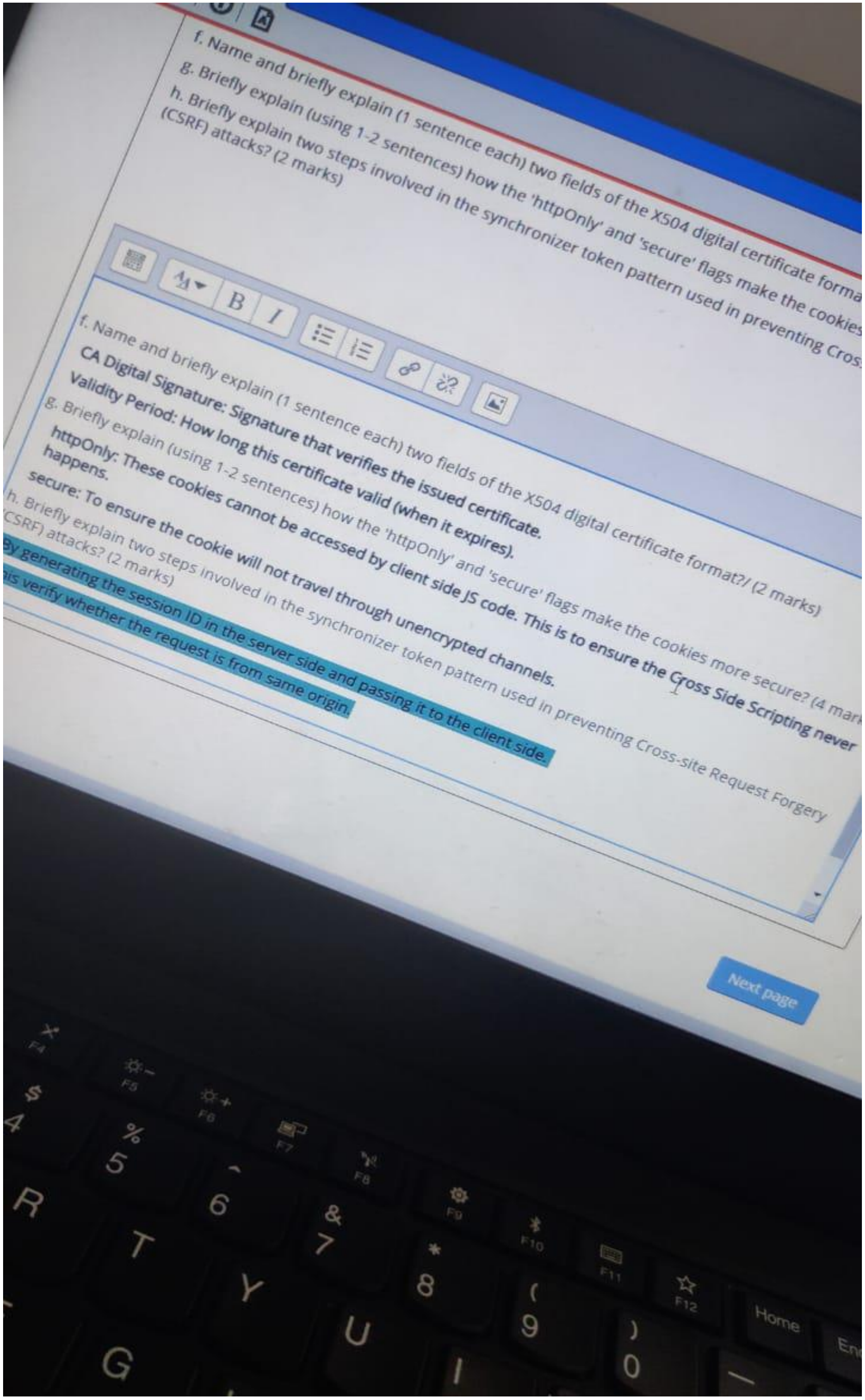
CA(Certification Authority) is issues and signs the certificates on the other hand RA (Registration Authority), Verifies and identifies the entity requesting the Certificate.

d. Briefly explain (1-2 sentences) the difference between the TLS (SSL) tunneling and TLS (SSL) bridging? (2 marks)

TLS(SSL) Tunneling is when a client directly communicate with server.

TLS (SSL) bridging is when a connection between client and a server initiation or termination by ISA.

Question 2(b)



f. Name and briefly explain (1 sentence each) two fields of the X504 digital certificate forma

g. Briefly explain (using 1-2 sentences) how the 'httpOnly' and 'secure' flags make the cookies

h. Briefly explain two steps involved in the synchronizer token pattern used in preventing Cros
(CSRF) attacks? (2 marks)

f. Name and briefly explain (1 sentence each) two fields of the X504 digital certificate format?/ (2 marks)

CA Digital Signature: Signature that verifies the issued certificate.

Validity Period: How long this certificate valid (when it expires).

g. Briefly explain (using 1-2 sentences) how the 'httpOnly' and 'secure' flags make the cookies more secure? (4 mar

httpOnly: These cookies cannot be accessed by client side JS code. This is to ensure the Cross Side Scripting never happens.

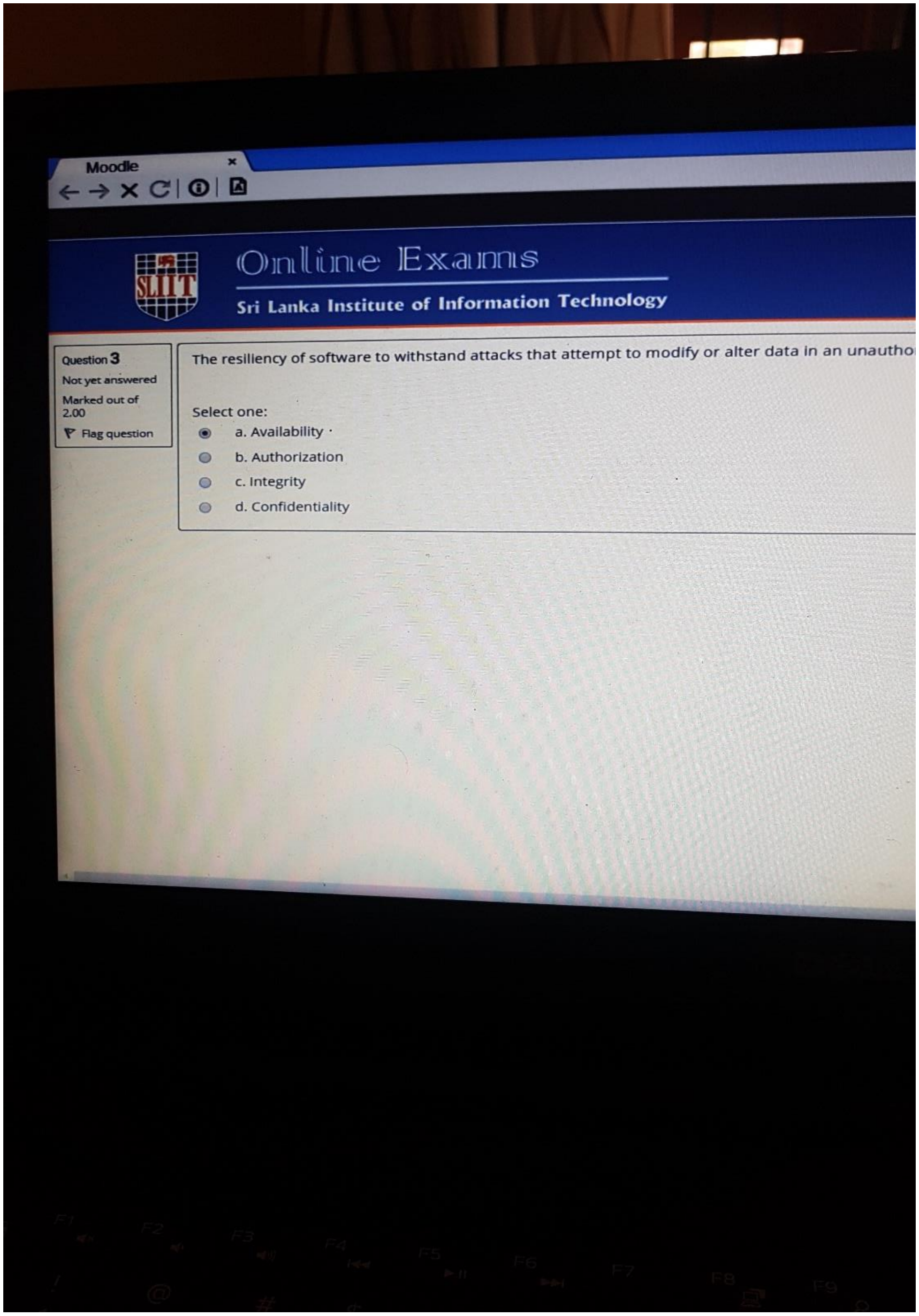
secure: To ensure the cookie will not travel through unencrypted channels.

h. Briefly explain two steps involved in the synchronizer token pattern used in preventing Cross-site Request Forgery
CSRF) attacks? (2 marks)

By generating the session ID in the server side and passing it to the client side.

is verify whether the request is from same origin.

Question 3



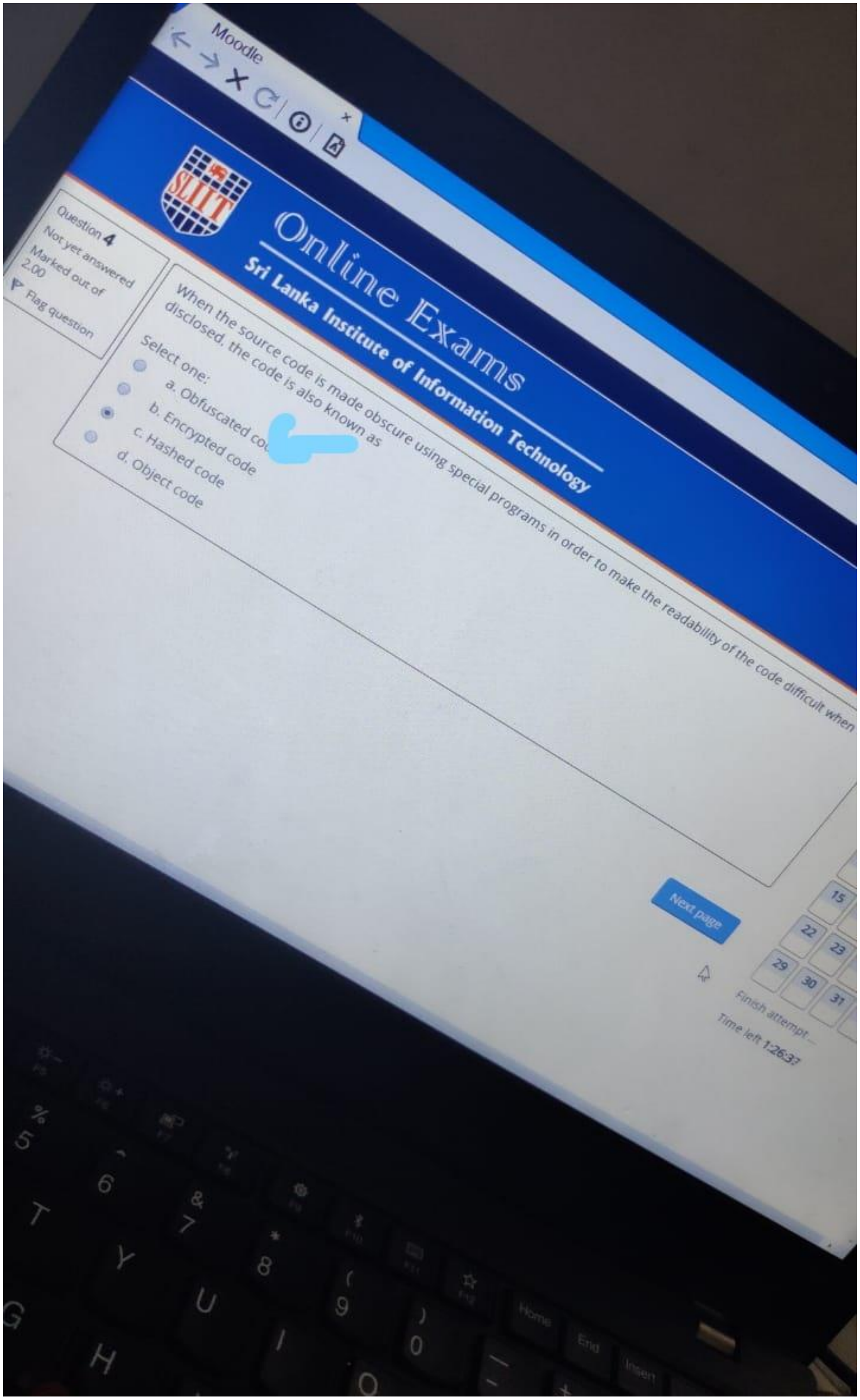
Question 3
Not yet answered
Marked out of 2.00
Flag question

The resiliency of software to withstand attacks that attempt to modify or alter data in an unautho

Select one:

- ● a. Availability
- ○ b. Authorization
- ○ c. Integrity
- ○ d. Confidentiality

Question 4



Question 4

Not yet answered

Marked out of 2.00

Flag question

When the source code is made obscure using special programs in order to make the readability of the code difficult when disclosed, the code is also known as

Select one:

○ a. Obfuscated co

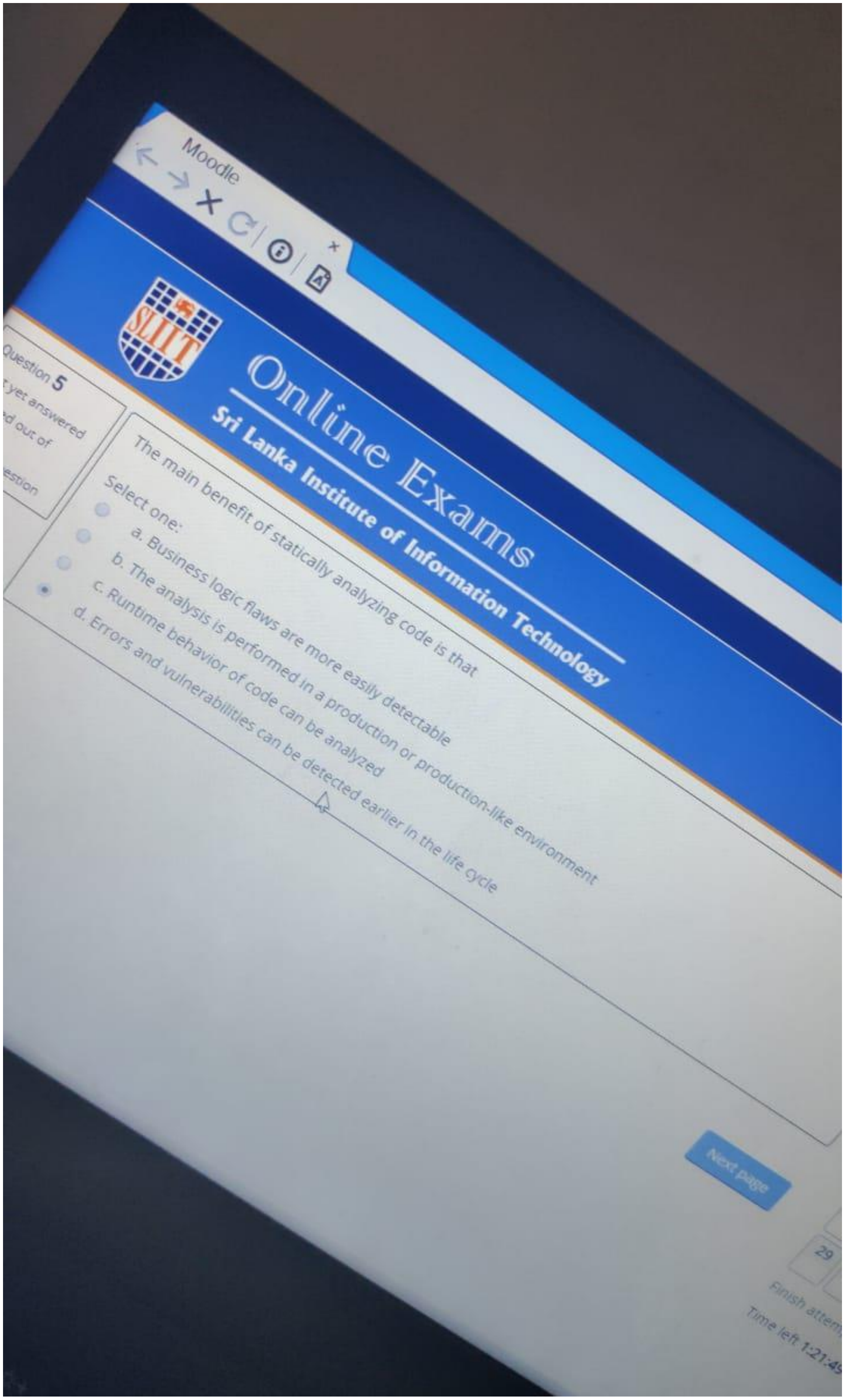
○ b. Encrypted code

● c. Hashed code

○ d. Object code

Time left 1:26:37

Question 5



The main benefit of statically analyzing code is that

Select one:

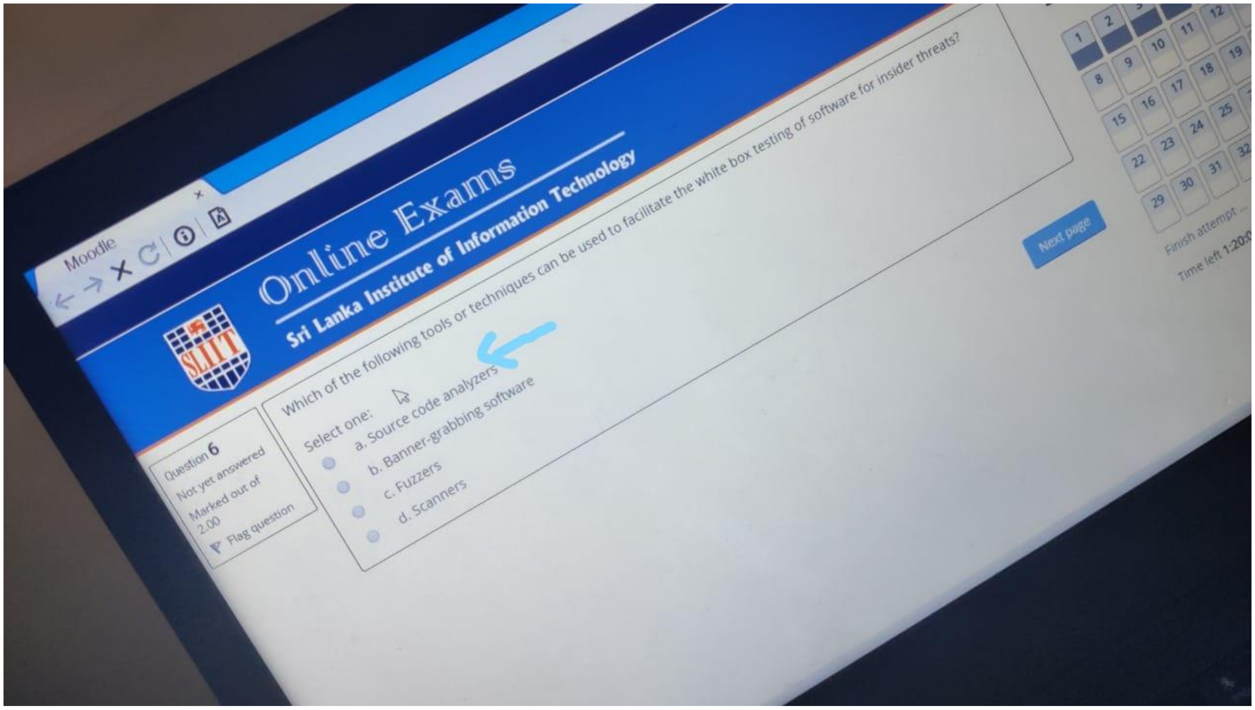
○ a. Business logic flaws are more easily detectable

○ b. The analysis is performed in a production or production-like environment

○ c. Runtime behavior of code can be analyzed

● d. Errors and vulnerabilities can be detected earlier in the life cycle

Question 6



Question 6
Not yet answered
Marked out of 2.00
Flag question

Which of the following tools or techniques can be used to facilitate the white box testing of software for insider threats?

Select one:

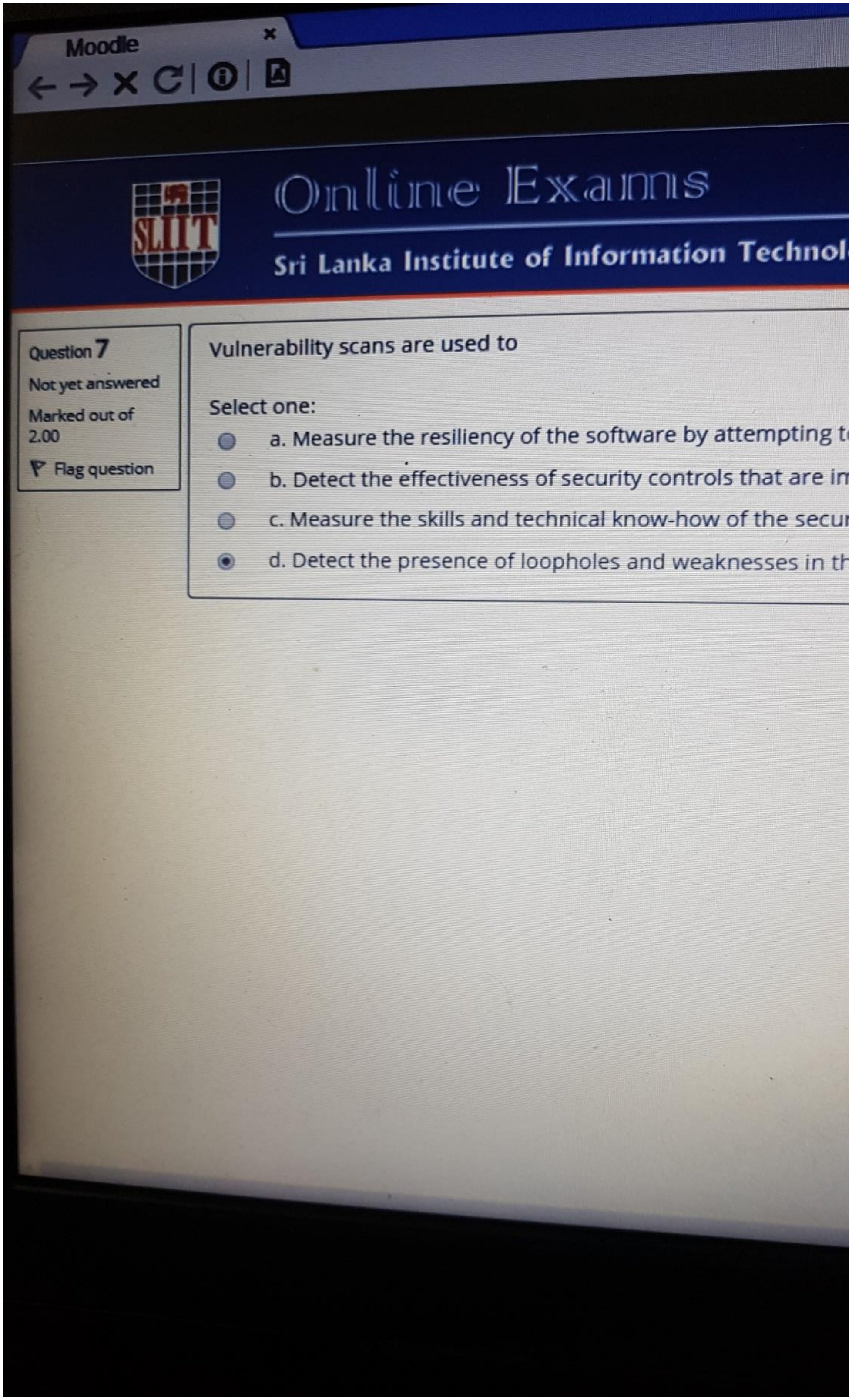
○ [✓ a. Source code analyzers]

○ b. Banner-grabbing software

○ c. Fuzzers

○ d. Scanners

Question 7



Question 7

Not yet answered

Marked out of 2.00

Flag question

Vulnerability scans are used to

Select one:

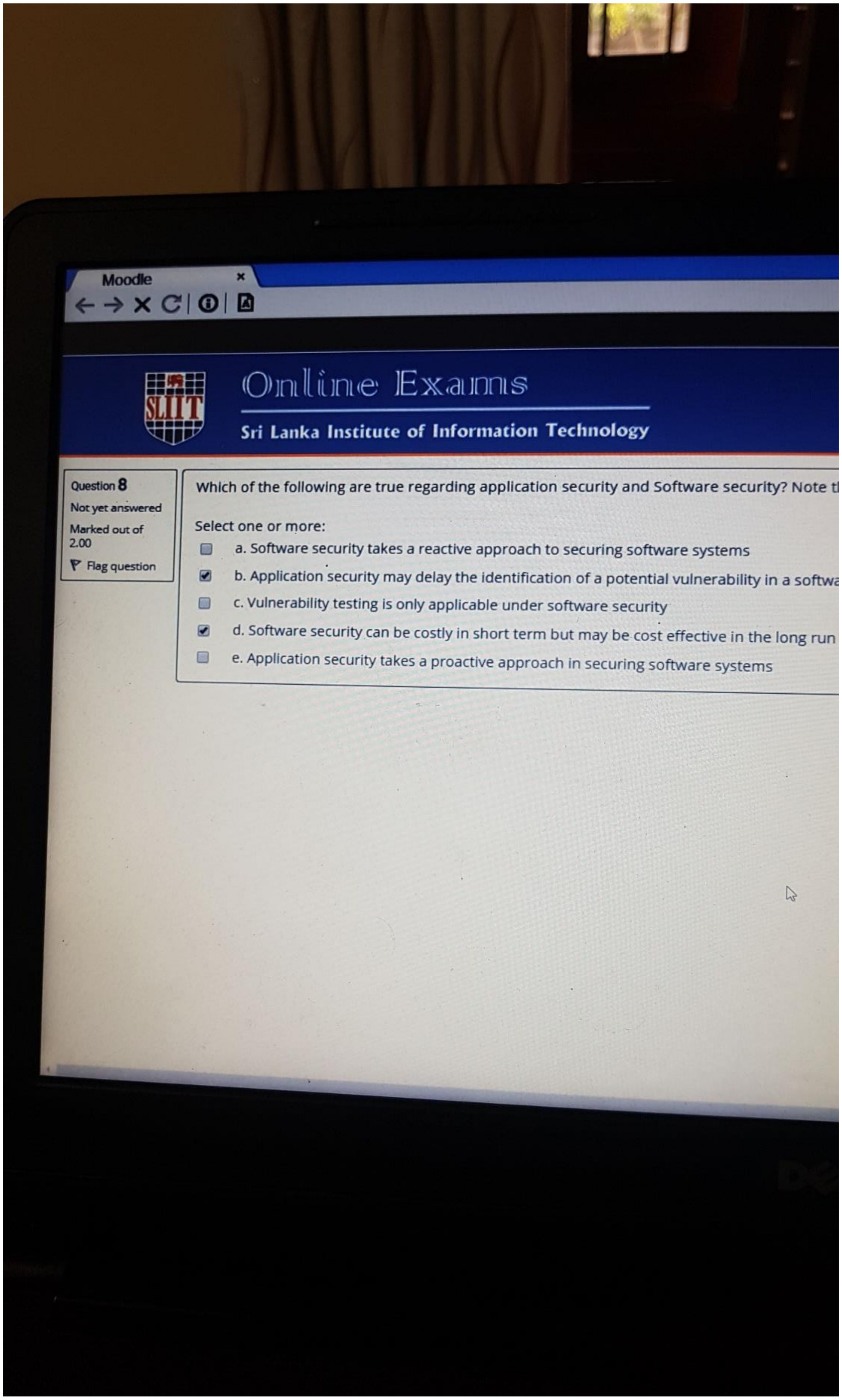
○ a. Measure the resiliency of the software by attempting t

○ b. Detect the effectiveness of security controls that are im

○ c. Measure the skills and technical know-how of the secu

● d. Detect the presence of loopholes and weaknesses in th

Question 8



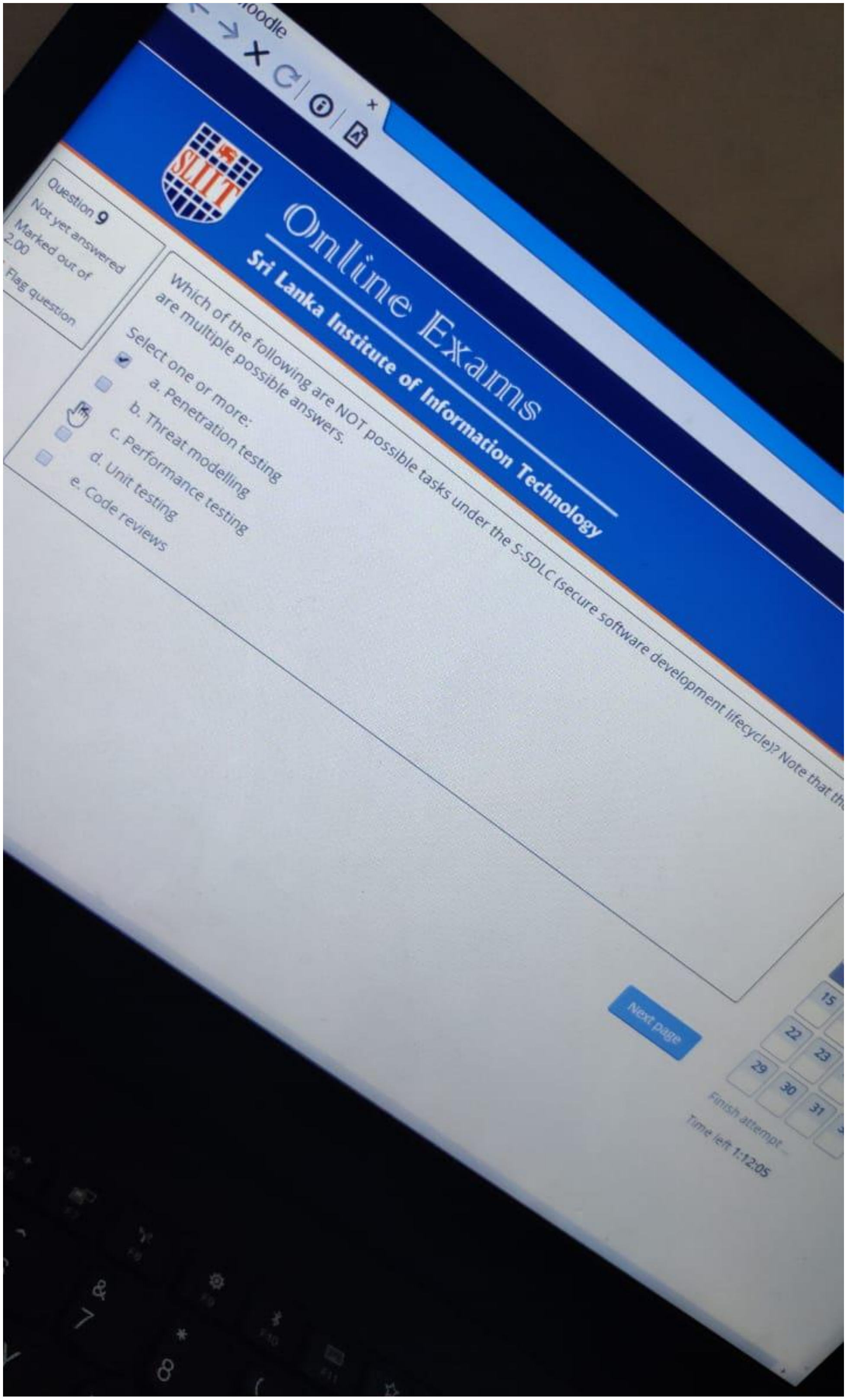
Question 8
Not yet answered
Marked out of 2.00
Flag question

Which of the following are true regarding application security and Software security? Note t

Select one or more:

- ☐ a. Software security takes a reactive approach to securing software systems
- ☑ b. Application security may delay the identification of a potential vulnerability in a softwa
- ☐ c. Vulnerability testing is only applicable under software security
- ☑ d. Software security can be costly in short term but may be cost effective in the long run
- ☐ e. Application security takes a proactive approach in securing software systems

Question 9



Question 9

Not yet answered

Marked out of 2.00

Flag question

Which of the following are NOT possible tasks under the S-SDLC (secure software development lifecycle)? Note that th are multiple possible answers.

Select one or more:

☑ a. Penetration testing

☐ b. Threat modelling

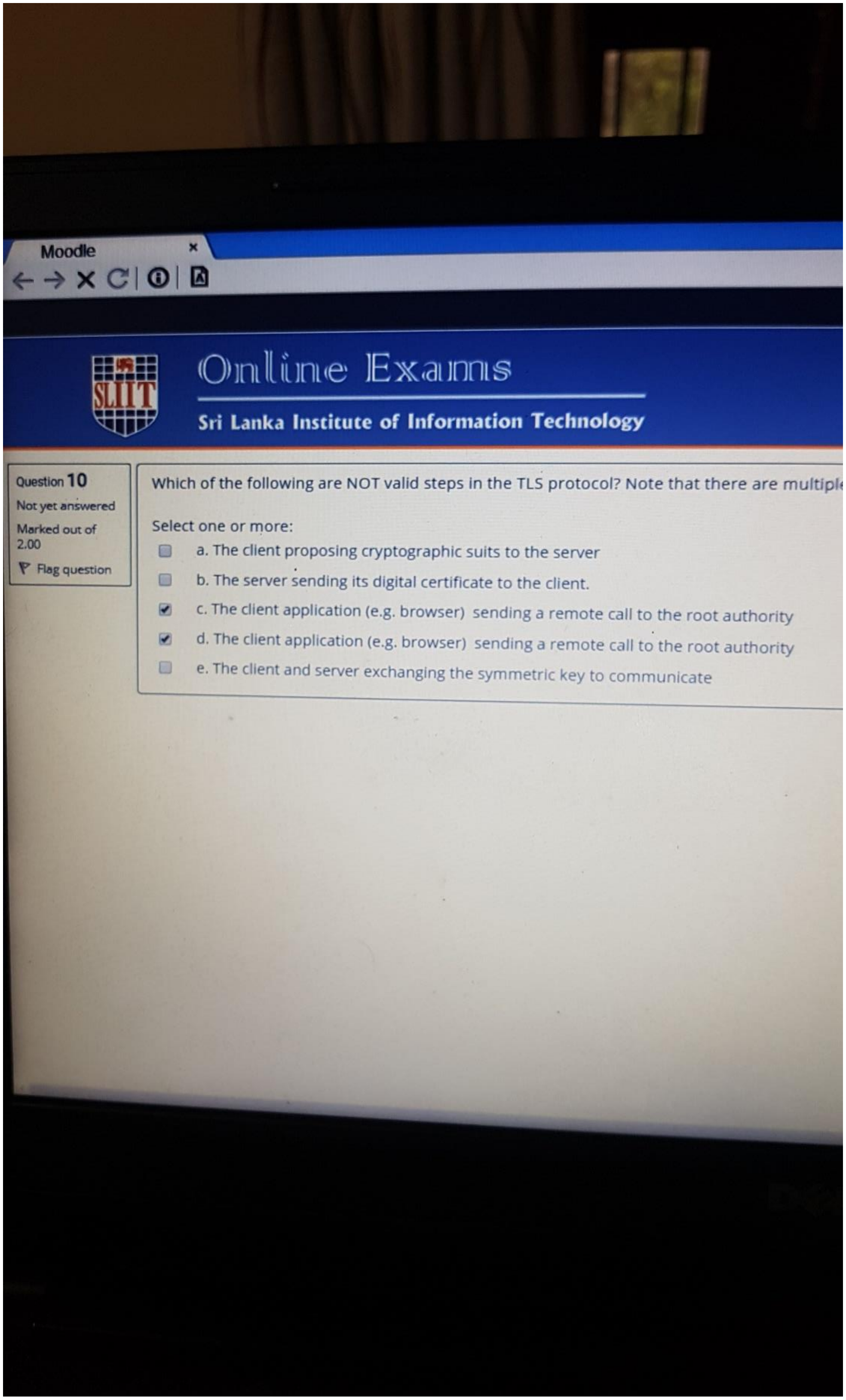
☐ c. Performance testing

☐ d. Unit testing

☐ e. Code reviews

Time left 1:12:05

Question 10

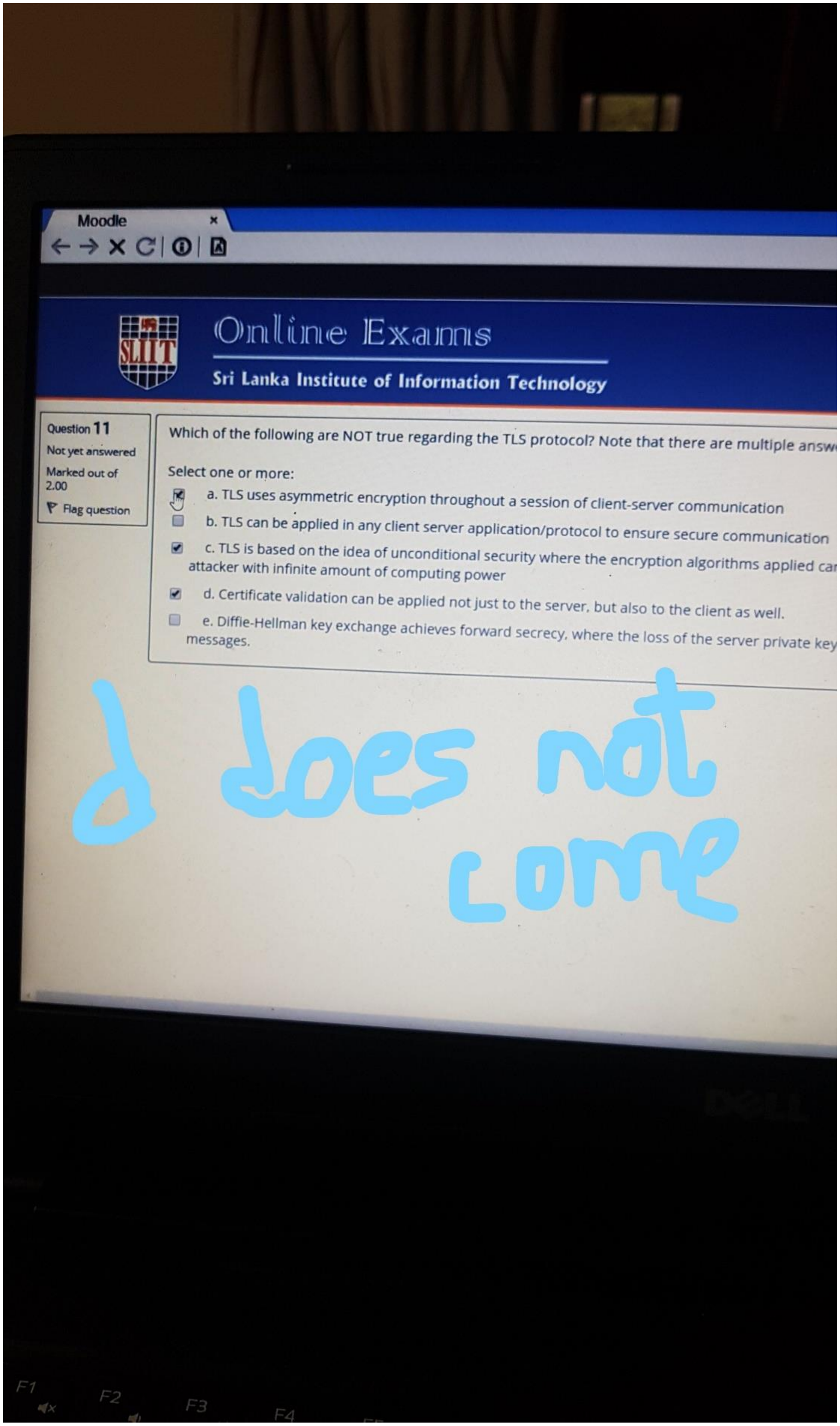


Which of the following are NOT valid steps in the TLS protocol? Note that there are multipl

Select one or more:

- □ a. The client proposing cryptographic suits to the server
- □ b. The server sending its digital certificate to the client.
- ☑ c. The client application (e.g. browser) sending a remote call to the root authority
- ☑ d. The client application (e.g. browser) sending a remote call to the root authority
- □ e. The client and server exchanging the symmetric key to communicate

Question 11



Online Exams

Sri Lanka Institute of Information Technology

Question 11

Not yet answered

Marked out of 2.00

Flag question

Which of the following are NOT true regarding the TLS protocol? Note that there are multiple answ

Select one or more:

☑ a. TLS uses asymmetric encryption throughout a session of client-server communication

□ b. TLS can be applied in any client server application/protocol to ensure secure communication

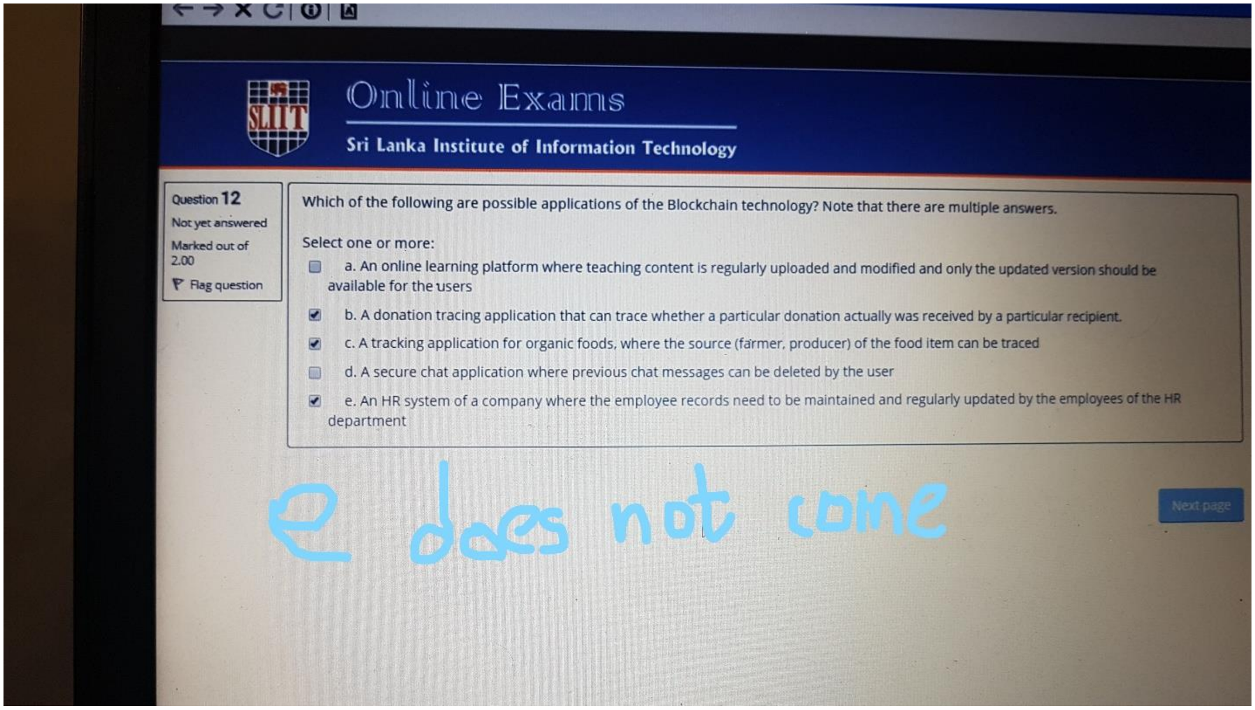
☑ c. TLS is based on the idea of unconditional security where the encryption algorithms applied ca attacker with infinite amount of computing power

☑ d. Certificate validation can be applied not just to the server, but also to the client as well.

□ e. Diffie-Hellman key exchange achieves forward secrecy, where the loss of the server private key messages.

d does not come

Question 12



Which of the following are possible applications of the Blockchain technology? Note that there are multiple answers.

Select one or more:

☐ a. An online learning platform where teaching content is regularly uploaded and modified and only the updated version should be available for the users

☑ b. A donation tracing application that can trace whether a particular donation actually was received by a particular recipient.

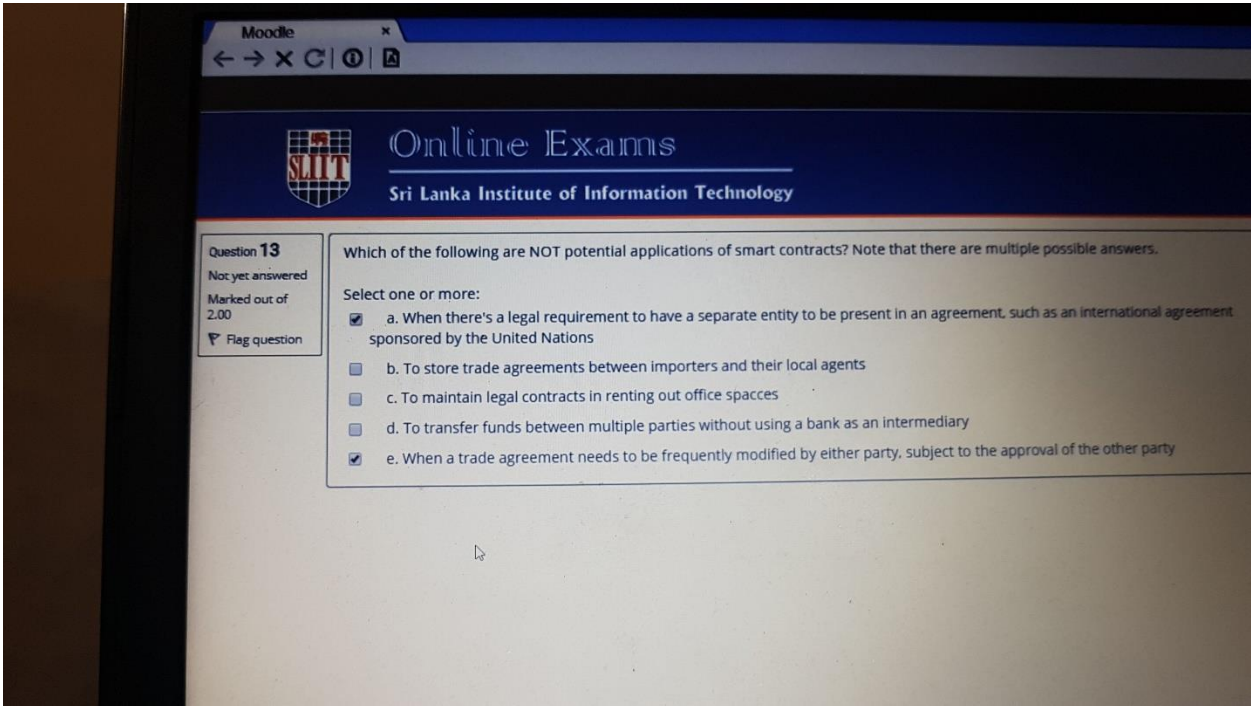
☑ c. A tracking application for organic foods, where the source (farmer, producer) of the food item can be traced

☐ d. A secure chat application where previous chat messages can be deleted by the user

☑ e. An HR system of a company where the employee records need to be maintained and regularly updated by the employees of the HR department

e does not come

Question 13



Which of the following are NOT potential applications of smart contracts? Note that there are multiple possible answers.

Select one or more:

☑ a. When there's a legal requirement to have a separate entity to be present in an agreement, such as an international agreement sponsored by the United Nations

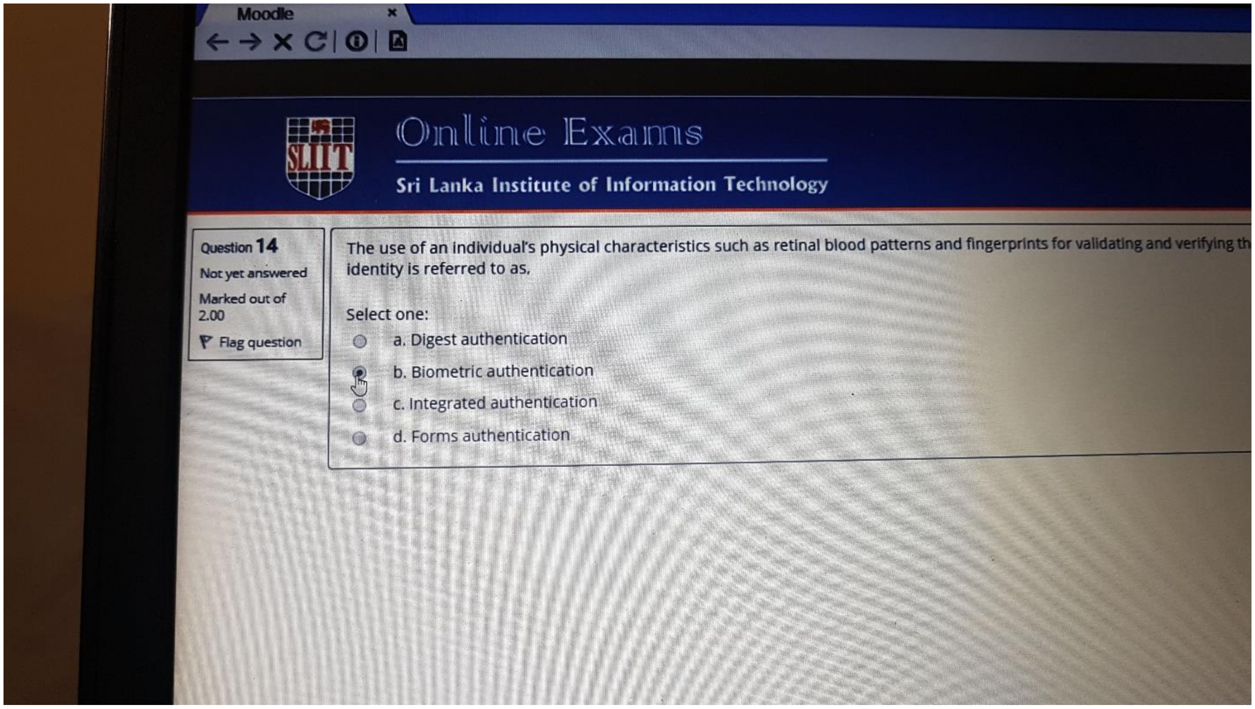
☐ b. To store trade agreements between importers and their local agents

☐ c. To maintain legal contracts in renting out office spacces

☐ d. To transfer funds between multiple parties without using a bank as an intermediary

☑ e. When a trade agreement needs to be frequently modified by either party, subject to the approval of the other party

Question 14



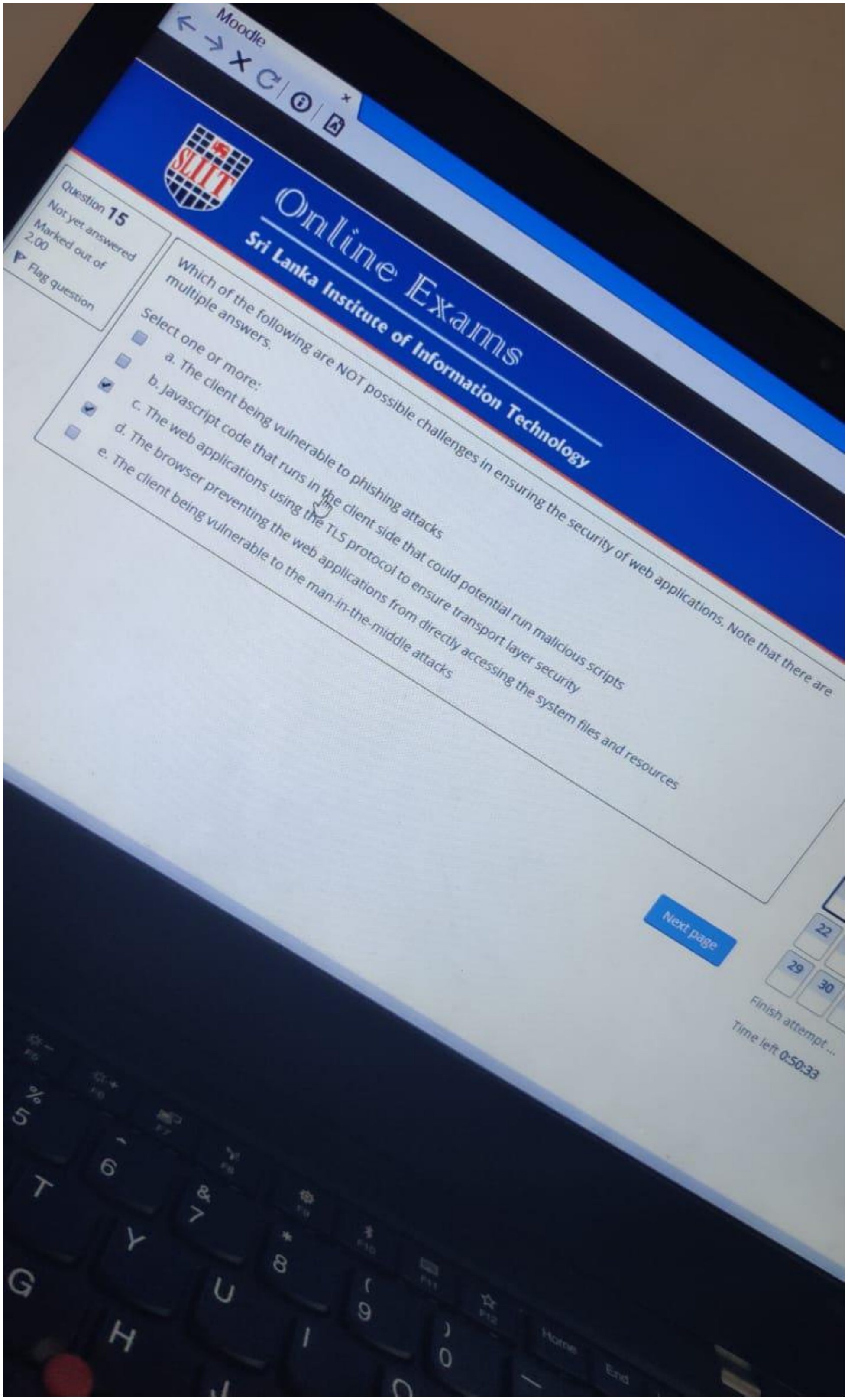
Question 14
Not yet answered
Marked out of 2.00
Flag question

The use of an individual's physical characteristics such as retinal blood patterns and fingerprints for validating and verifying th identity is referred to as,

Select one:

○ a. Digest authentication
● b. Biometric authentication
○ c. Integrated authentication
○ d. Forms authentication

Question 15



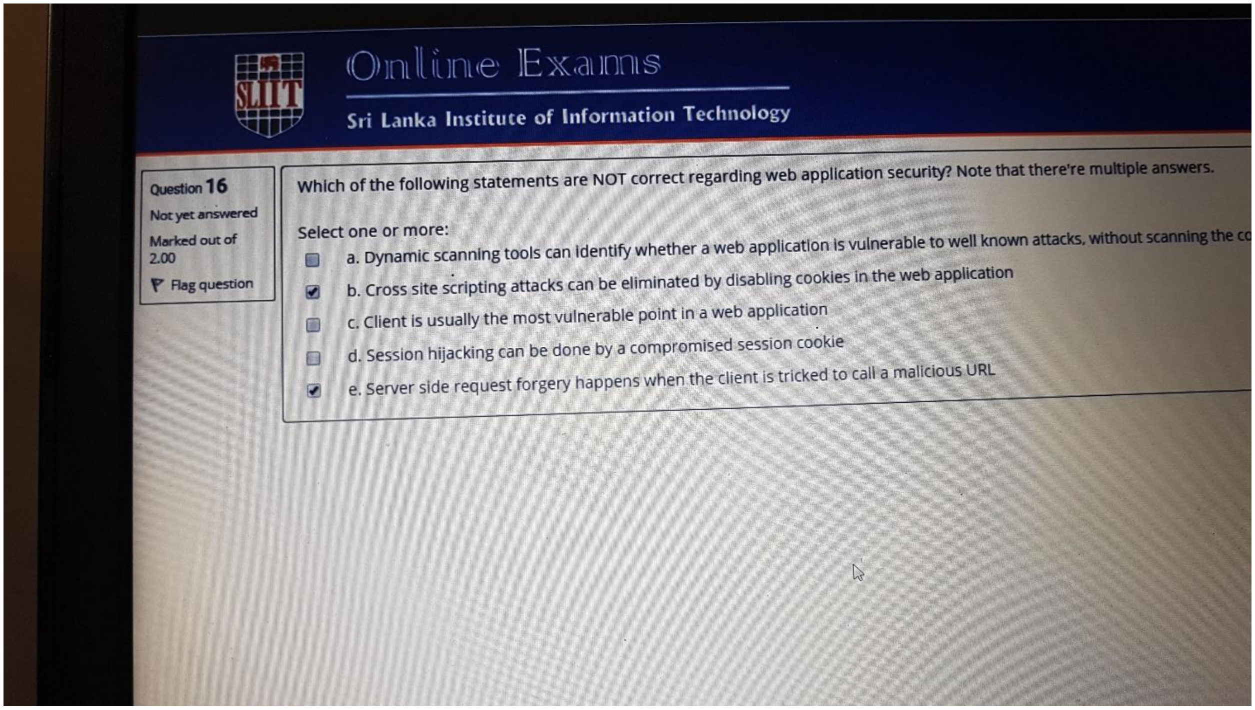
Question 15
Not yet answered
Marked out of 2.00
Flag question

Which of the following are NOT possible challenges in ensuring the security of web applications. Note that there are multiple answers.

Select one or more:

- □ a. The client being vulnerable to phishing attacks
- □ b. Javascript code that runs in the client side that could potential run malicious scripts
- ☑ c. The web applications using the TLS protocol to ensure transport layer security
- ☑ d. The browser preventing the web applications from directly accessing the system files and resources
- □ e. The client being vulnerable to the man-in-the-middle attacks

Question 16



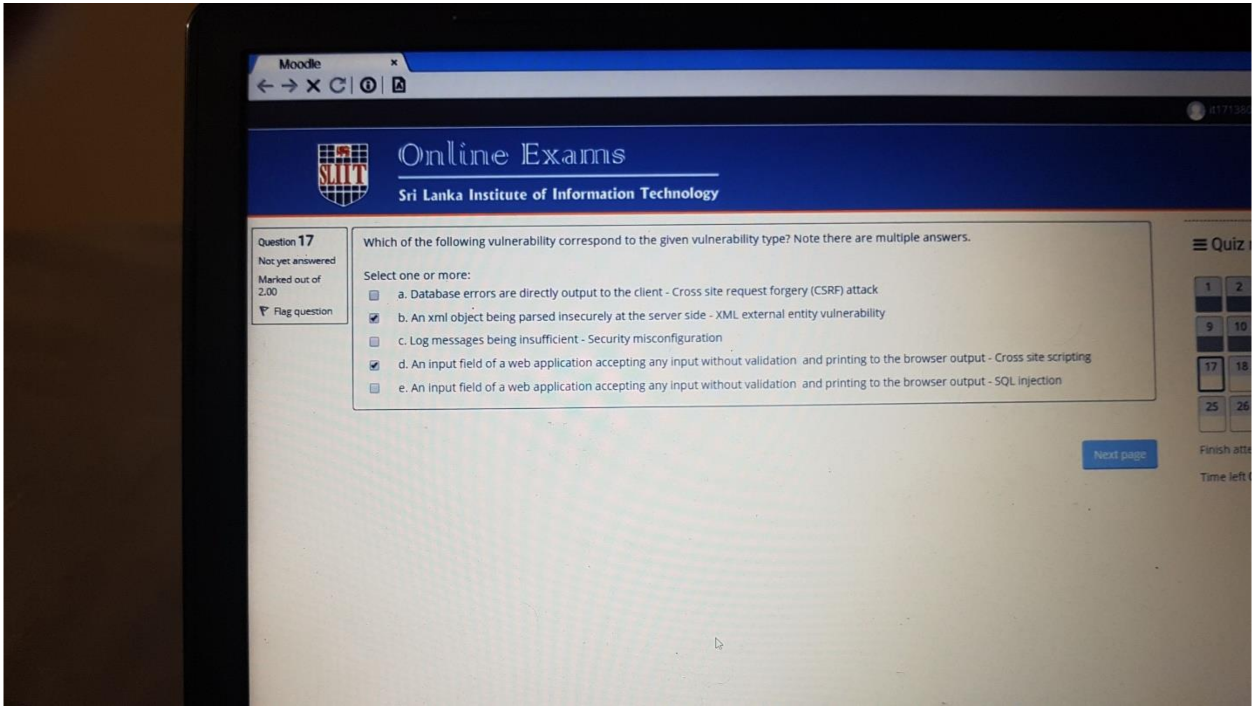
Question 16
Not yet answered
Marked out of 2.00
Flag question

Which of the following statements are NOT correct regarding web application security? Note that there're multiple answers.

Select one or more:

- □ a. Dynamic scanning tools can identify whether a web application is vulnerable to well known attacks, without scanning the co
- ☑ b. Cross site scripting attacks can be eliminated by disabling cookies in the web application
- □ c. Client is usually the most vulnerable point in a web application
- □ d. Session hijacking can be done by a compromised session cookie
- ☑ e. Server side request forgery happens when the client is tricked to call a malicious URL

Question 17



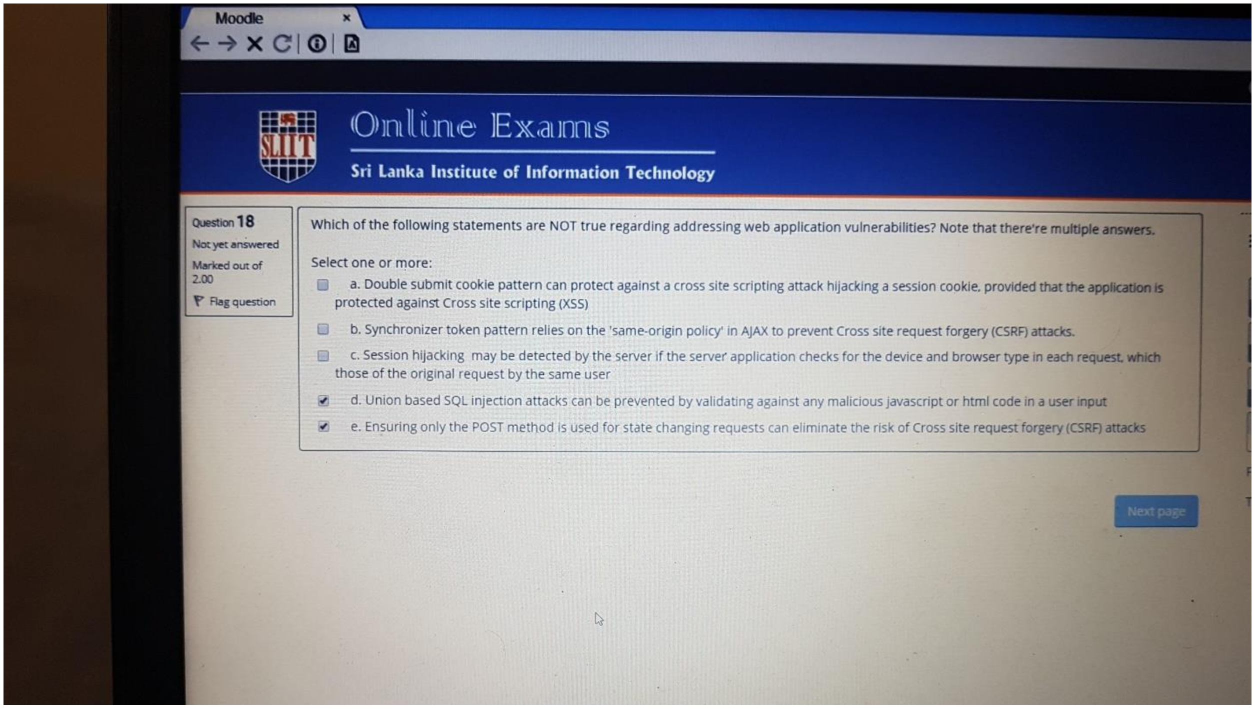
Question 17
Not yet answered
Marked out of 2.00
Flag question

Which of the following vulnerability correspond to the given vulnerability type? Note there are multiple answers.

Select one or more:

- □ a. Database errors are directly output to the client - Cross site request forgery (CSRF) attack
- ☑ b. An xml object being parsed insecurely at the server side - XML external entity vulnerability
- □ c. Log messages being insufficient - Security misconfiguration
- ☑ d. An input field of a web application accepting any input without validation and printing to the browser output - Cross site scripting
- □ e. An input field of a web application accepting any input without validation and printing to the browser output - SQL injection

Question 18



Question 18
Not yet answered
Marked out of 2.00
Flag question

Which of the following statements are NOT true regarding addressing web application vulnerabilities? Note that there're multiple answers.

Select one or more:

☐ a. Double submit cookie pattern can protect against a cross site scripting attack hijacking a session cookie, provided that the application is protected against Cross site scripting (XSS)

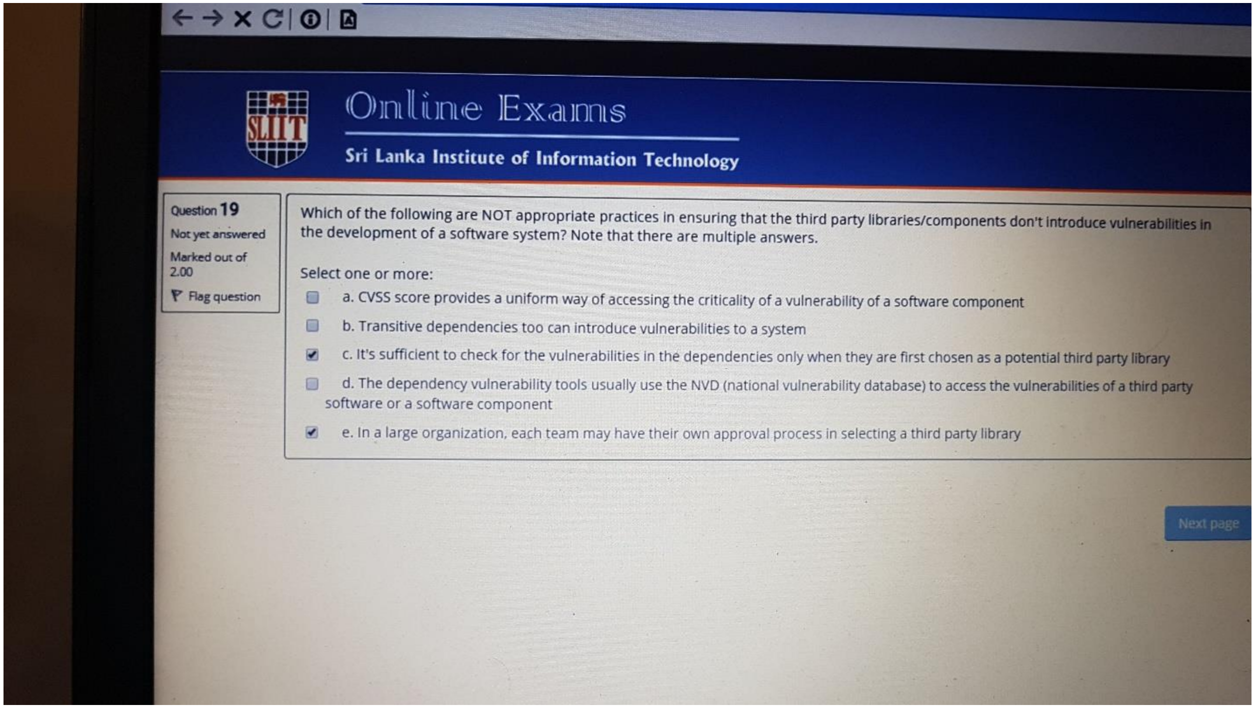
☐ b. Synchronizer token pattern relies on the 'same-origin policy' in AJAX to prevent Cross site request forgery (CSRF) attacks.

☐ c. Session hijacking may be detected by the server if the server application checks for the device and browser type in each request, which those of the original request by the same user

☑ d. Union based SQL injection attacks can be prevented by validating against any malicious javascript or html code in a user input

☑ e. Ensuring only the POST method is used for state changing requests can eliminate the risk of Cross site request forgery (CSRF) attacks

Question 19



Question 19
Not yet answered
Marked out of 2.00
Flag question

Which of the following are NOT appropriate practices in ensuring that the third party libraries/components don't introduce vulnerabilities in the development of a software system? Note that there are multiple answers.

Select one or more:

☐ a. CVSS score provides a uniform way of accessing the criticality of a vulnerability of a software component

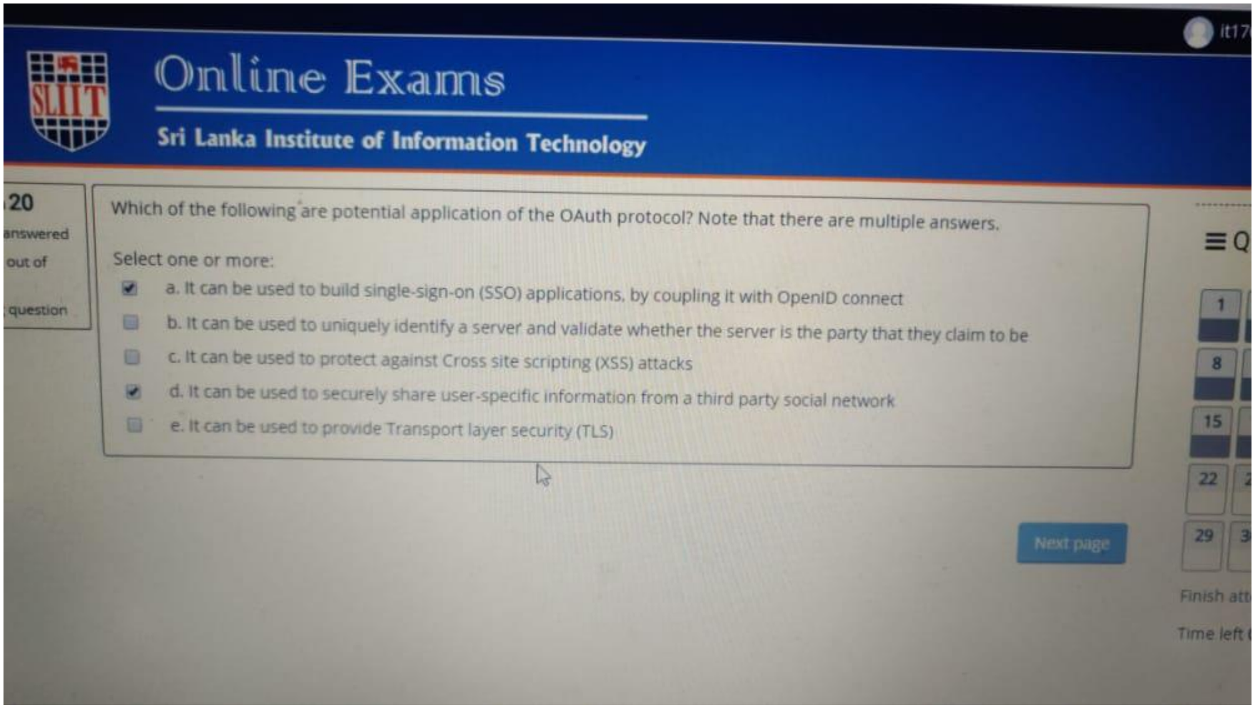
☐ b. Transitive dependencies too can introduce vulnerabilities to a system

☑ c. It's sufficient to check for the vulnerabilities in the dependencies only when they are first chosen as a potential third party library

☐ d. The dependency vulnerability tools usually use the NVD (national vulnerability database) to access the vulnerabilities of a third party software or a software component

☑ e. In a large organization, each team may have their own approval process in selecting a third party library

Question 20



Which of the following are potential application of the OAuth protocol? Note that there are multiple answers.

Select one or more:

☑ a. It can be used to build single-sign-on (SSO) applications, by coupling it with OpenID connect

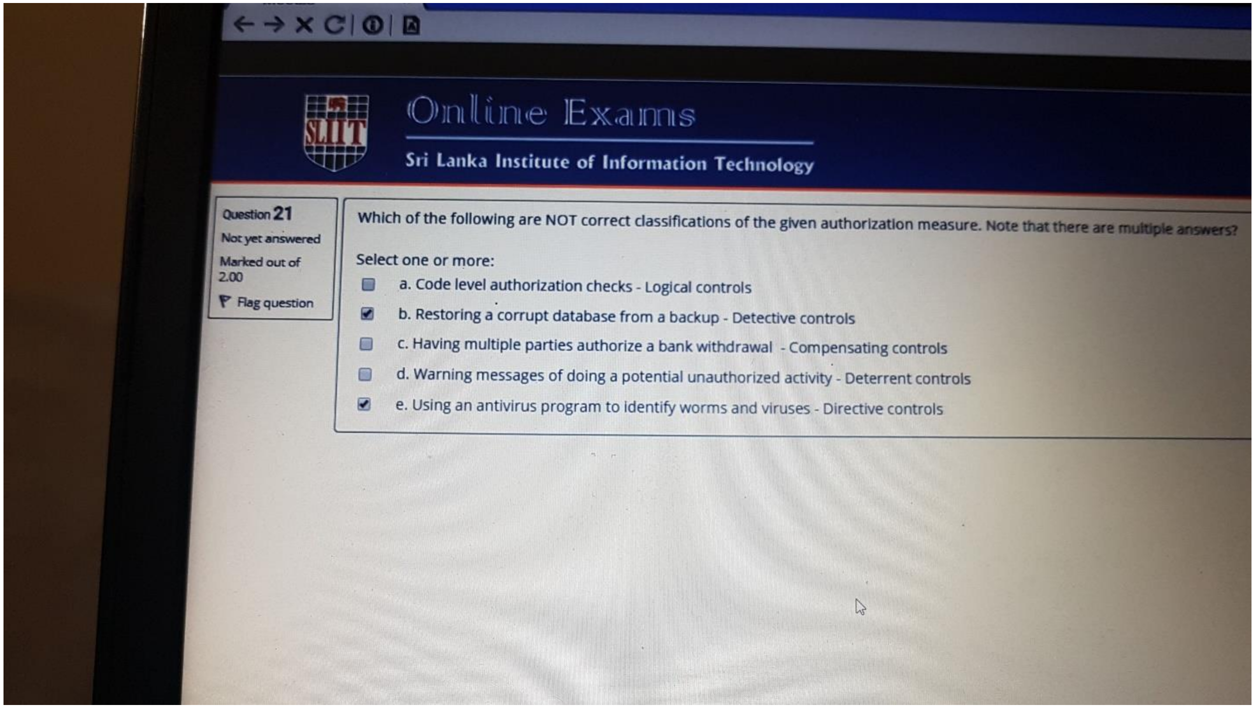
□ b. It can be used to uniquely identify a server and validate whether the server is the party that they claim to be

□ c. It can be used to protect against Cross site scripting (XSS) attacks

☑ d. It can be used to securely share user-specific information from a third party social network

□ e. It can be used to provide Transport layer security (TLS)

Question 21



Which of the following are NOT correct classifications of the given authorization measure. Note that there are multiple answers?

Select one or more:

□ a. Code level authorization checks - Logical controls

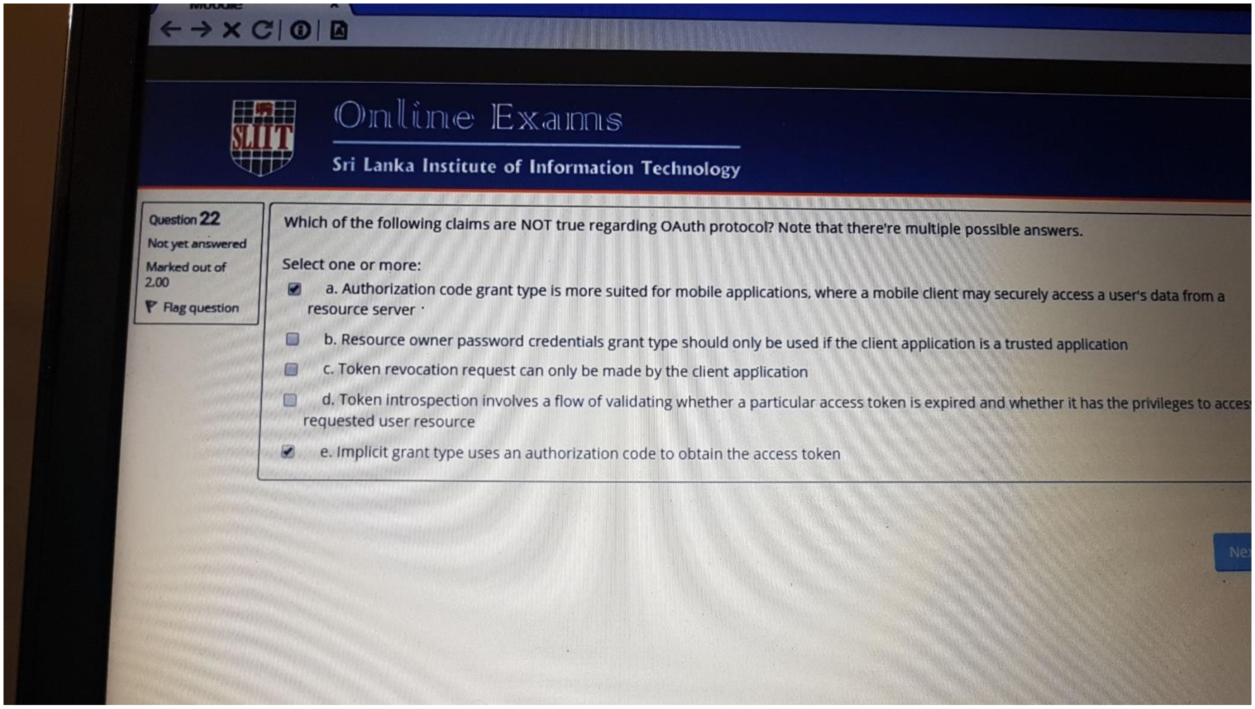
☑ b. Restoring a corrupt database from a backup - Detective controls

□ c. Having multiple parties authorize a bank withdrawal - Compensating controls

□ d. Warning messages of doing a potential unauthorized activity - Deterrent controls

☑ e. Using an antivirus program to identify worms and viruses - Directive controls

Question 22



Question 22

Not yet answered

Marked out of 2.00

Flag question

Which of the following claims are NOT true regarding OAuth protocol? Note that there're multiple possible answers.

Select one or more:

☑ a. Authorization code grant type is more suited for mobile applications, where a mobile client may securely access a user's data from a resource server

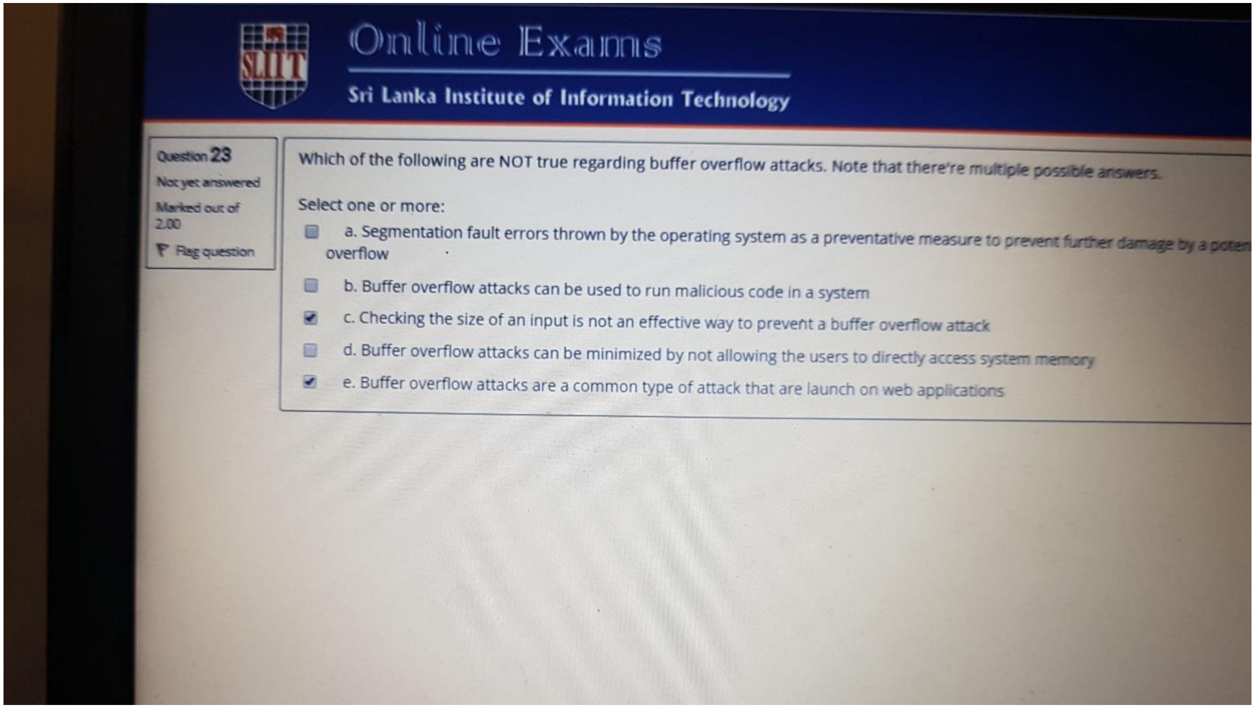
□ b. Resource owner password credentials grant type should only be used if the client application is a trusted application

□ c. Token revocation request can only be made by the client application

□ d. Token introspection involves a flow of validating whether a particular access token is expired and whether it has the privileges to acces requested user resource

☑ e. Implicit grant type uses an authorization code to obtain the access token

Question 23



Question 23

Not yet answered

Marked out of 2.00

Flag question

Which of the following are NOT true regarding buffer overflow attacks. Note that there're multiple possible answers.

Select one or more:

□ a. Segmentation fault errors thrown by the operating system as a preventative measure to prevent further damage by a poten overflow

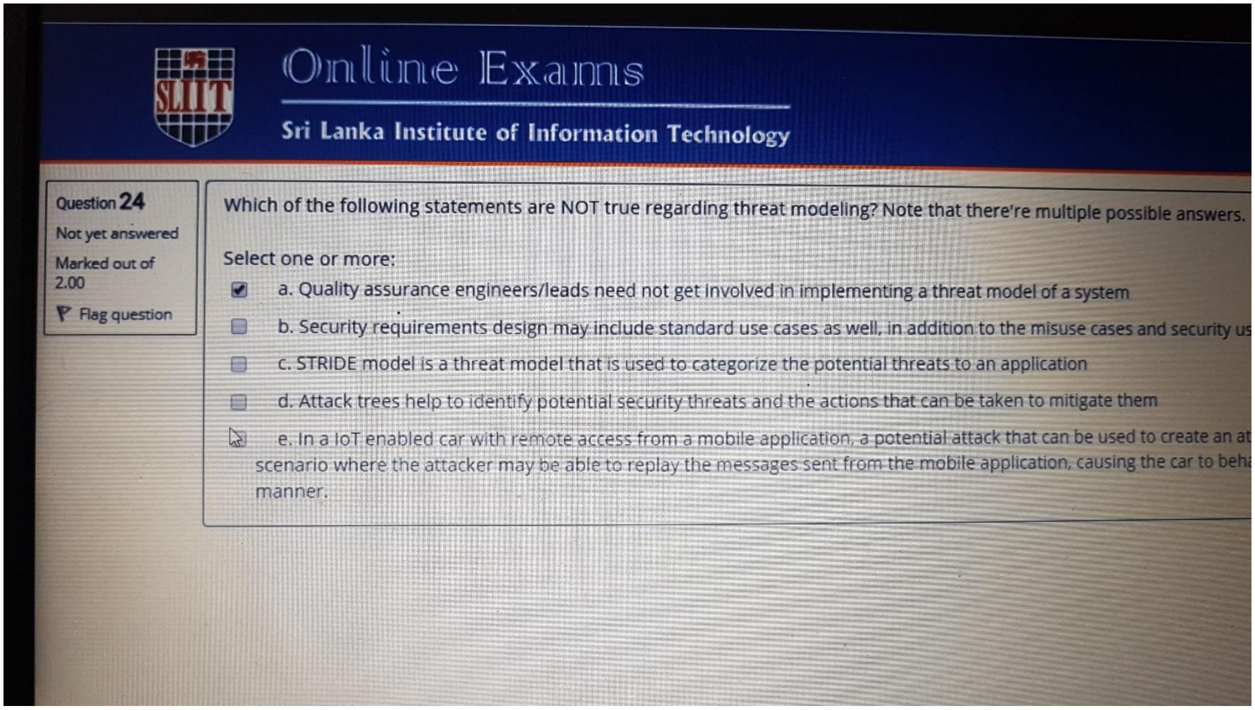
□ b. Buffer overflow attacks can be used to run malicious code in a system

☑ c. Checking the size of an input is not an effective way to prevent a buffer overflow attack

□ d. Buffer overflow attacks can be minimized by not allowing the users to directly access system memory

☑ e. Buffer overflow attacks are a common type of attack that are launch on web applications

Question 24



Question 24
Not yet answered
Marked out of 2.00
Flag question

Which of the following statements are NOT true regarding threat modeling? Note that there're multiple possible answers.

Select one or more:

☑ a. Quality assurance engineers/leads need not get involved in implementing a threat model of a system

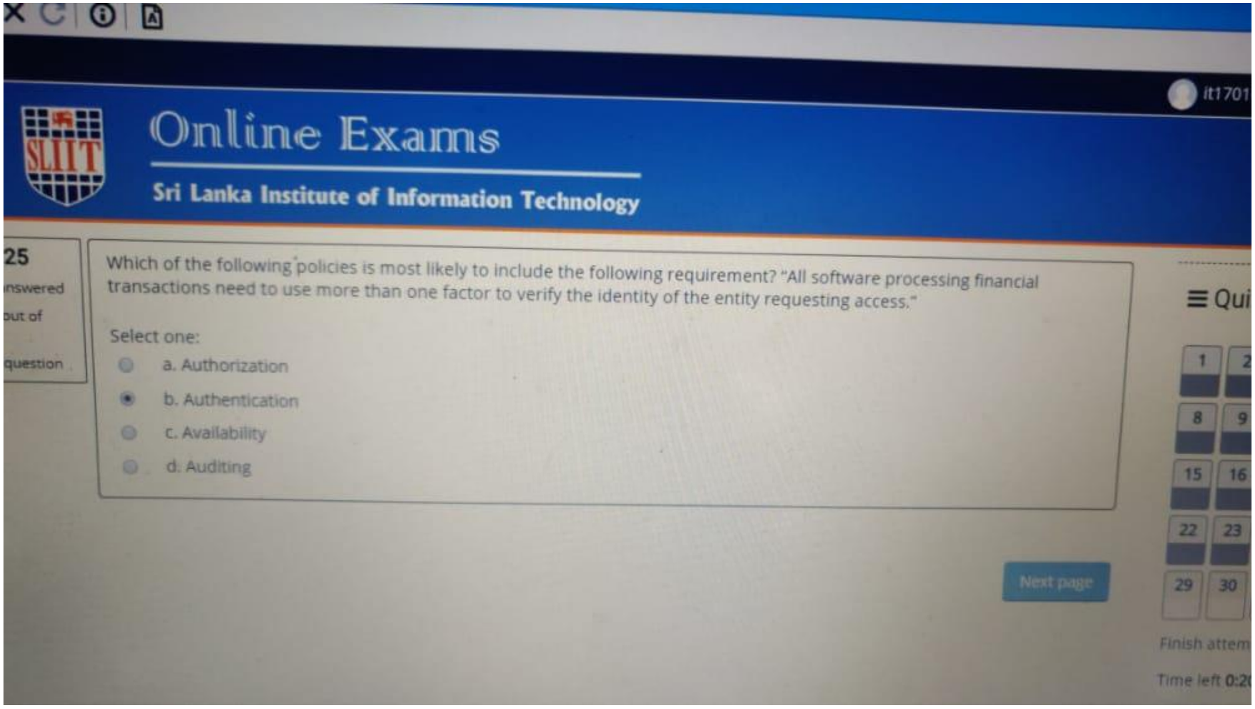
□ b. Security requirements design may include standard use cases as well, in addition to the misuse cases and security us

□ c. STRIDE model is a threat model that is used to categorize the potential threats to an application

□ d. Attack trees help to identify potential security threats and the actions that can be taken to mitigate them

□ e. In a IoT enabled car with remote access from a mobile application, a potential attack that can be used to create an at scenario where the attacker may be able to replay the messages sent from the mobile application, causing the car to beha manner.

Question 25



25
nswered
out of
question

Which of the following policies is most likely to include the following requirement? "All software processing financial transactions need to use more than one factor to verify the identity of the entity requesting access."

Select one:

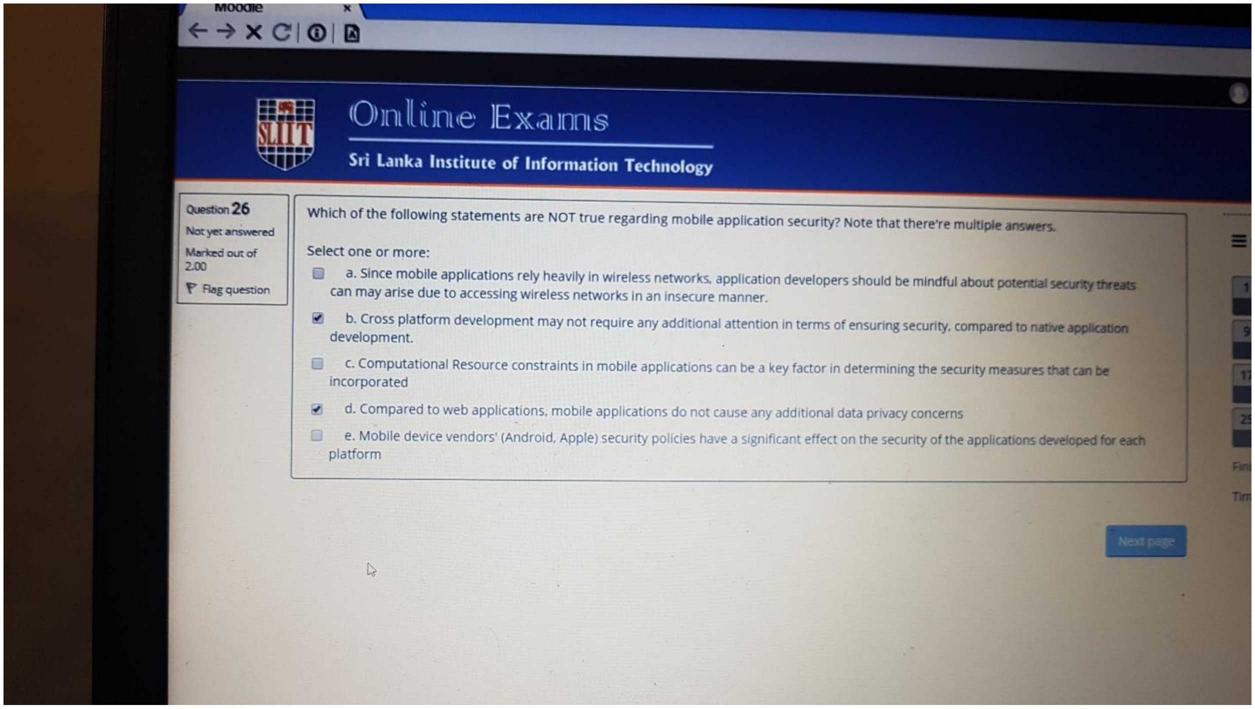
○ a. Authorization

● b. Authentication

○ c. Availability

○ d. Auditing

Question 26



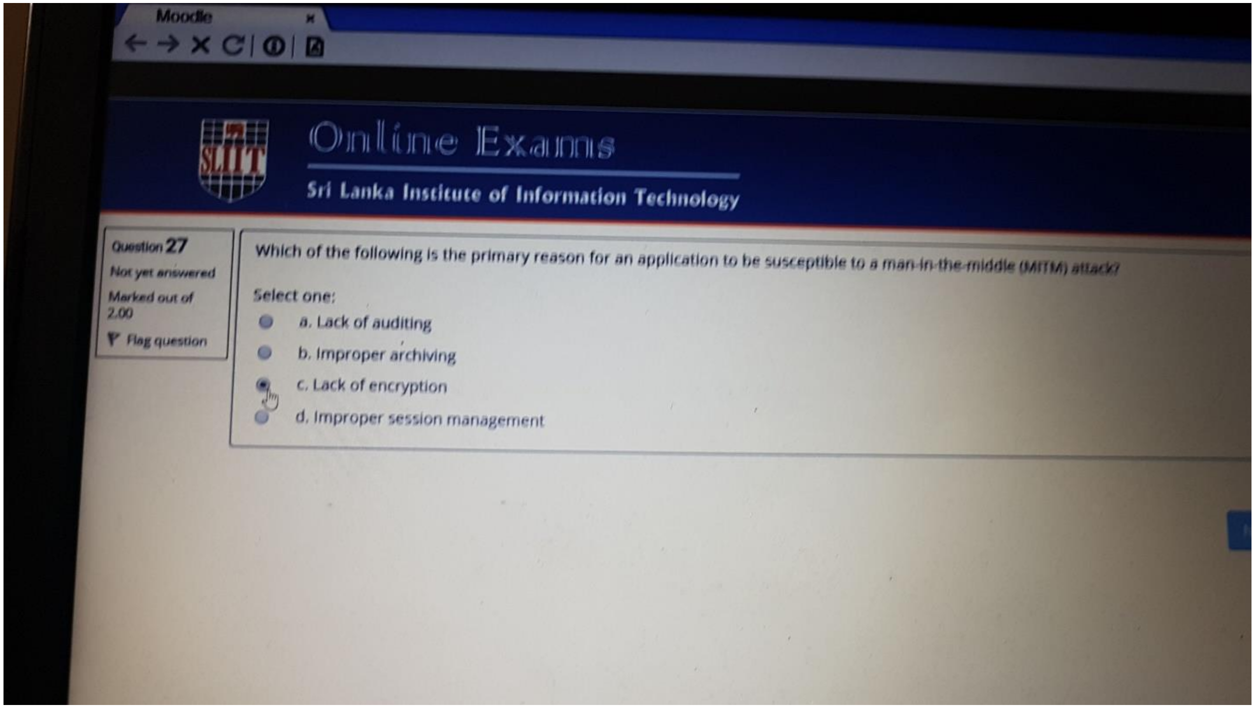
Question 26
Not yet answered
Marked out of 2.00
Flag question

Which of the following statements are NOT true regarding mobile application security? Note that there're multiple answers.

Select one or more:

- ☐ a. Since mobile applications rely heavily in wireless networks, application developers should be mindful about potential security threats can may arise due to accessing wireless networks in an insecure manner.
- ☑ b. Cross platform development may not require any additional attention in terms of ensuring security, compared to native application development.
- ☐ c. Computational Resource constraints in mobile applications can be a key factor in determining the security measures that can be incorporated
- ☑ d. Compared to web applications, mobile applications do not cause any additional data privacy concerns
- ☐ e. Mobile device vendors' (Android, Apple) security policies have a significant effect on the security of the applications developed for each platform

Question 27



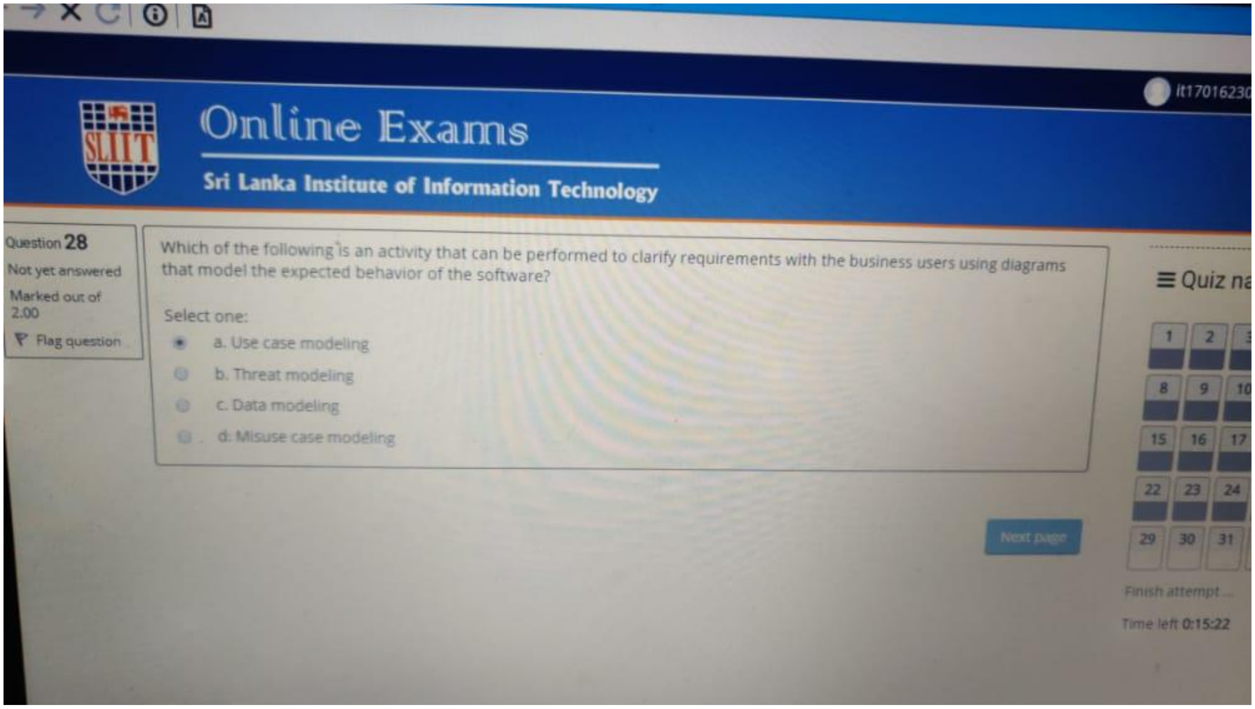
Question 27
Not yet answered
Marked out of 2.00
Flag question

Which of the following is the primary reason for an application to be susceptible to a man-in-the-middle (MITM) attack?

Select one:

- ○ a. Lack of auditing
- ○ b. Improper archiving
- ● c. Lack of encryption
- ○ d. Improper session management

Question 28



Question 28

Not yet answered

Marked out of 2.00

Which of the following is an activity that can be performed to clarify requirements with the business users using diagrams that model the expected behavior of the software?

Select one:

● a. Use case modeling

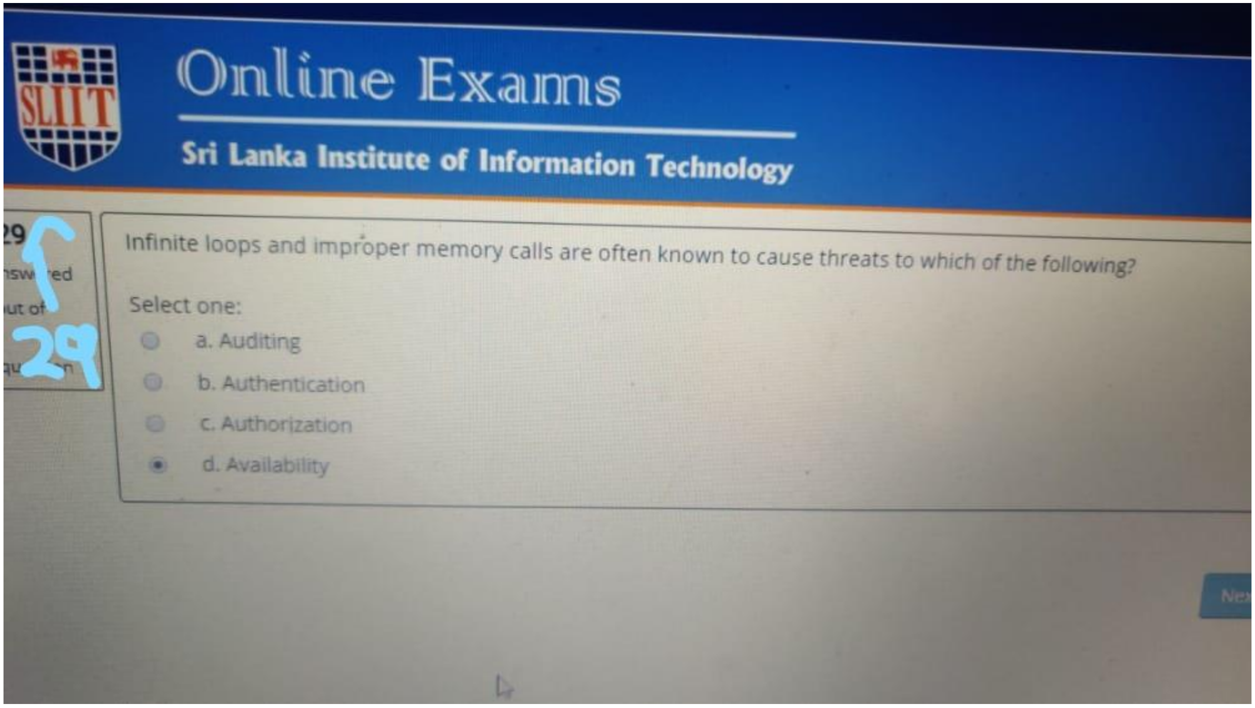
○ b. Threat modeling

○ c. Data modeling

○ d. Misuse case modeling

Time left 0:15:22

Question 29



Infinite loops and improper memory calls are often known to cause threats to which of the following?

Select one:

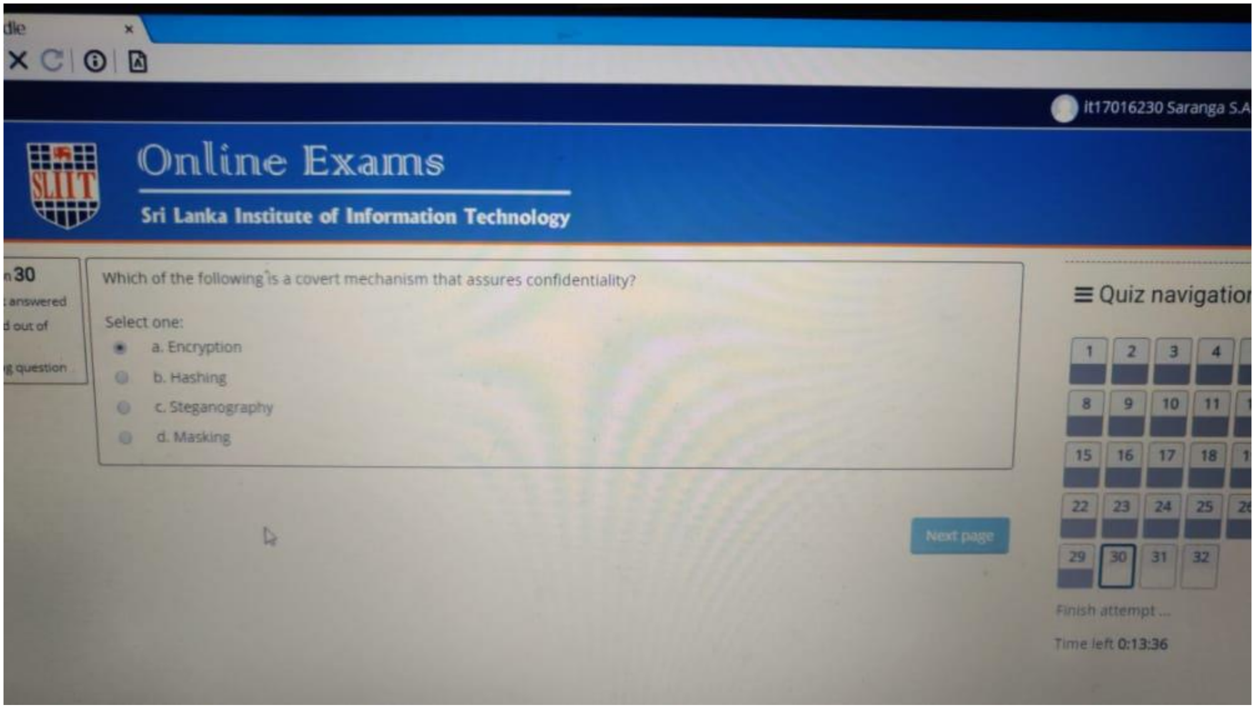
○ a. Auditing

○ b. Authentication

○ c. Authorization

● d. Availability

Question 30



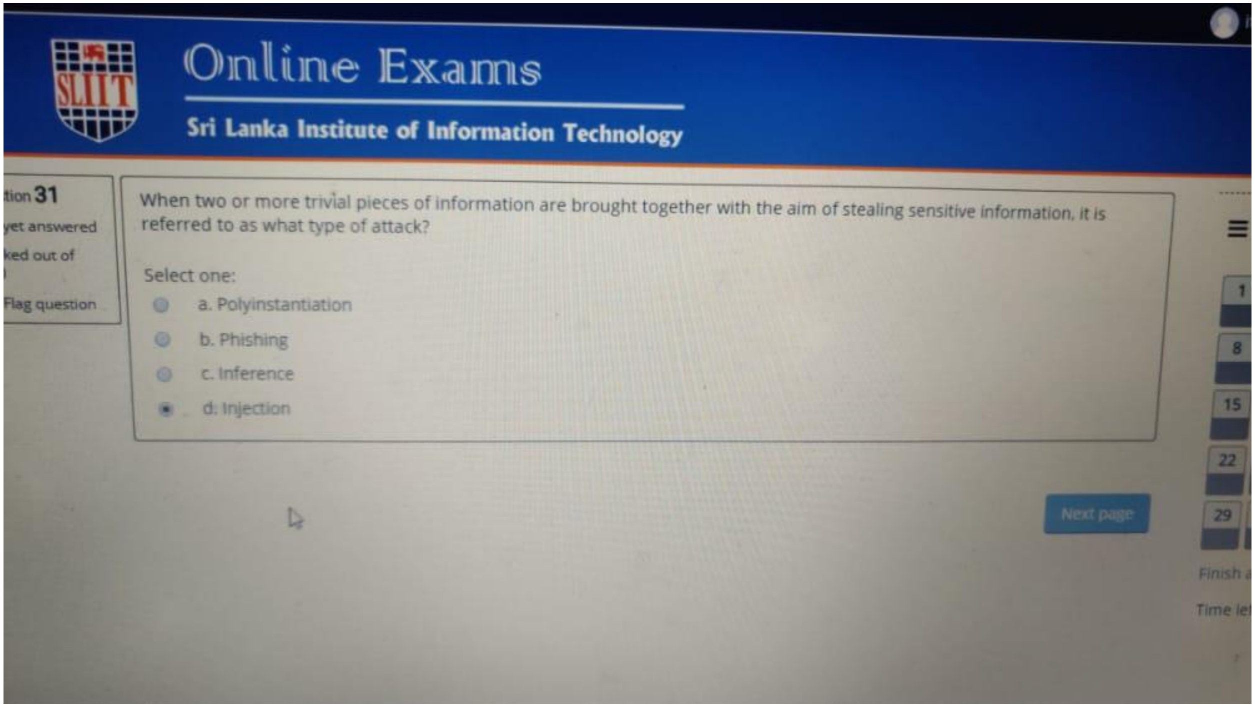
Which of the following is a covert mechanism that assures confidentiality?

Select one:

- ● a. Encryption
- ○ b. Hashing
- ○ c. Steganography
- ○ d. Masking

Time left 0:13:36

Question 31

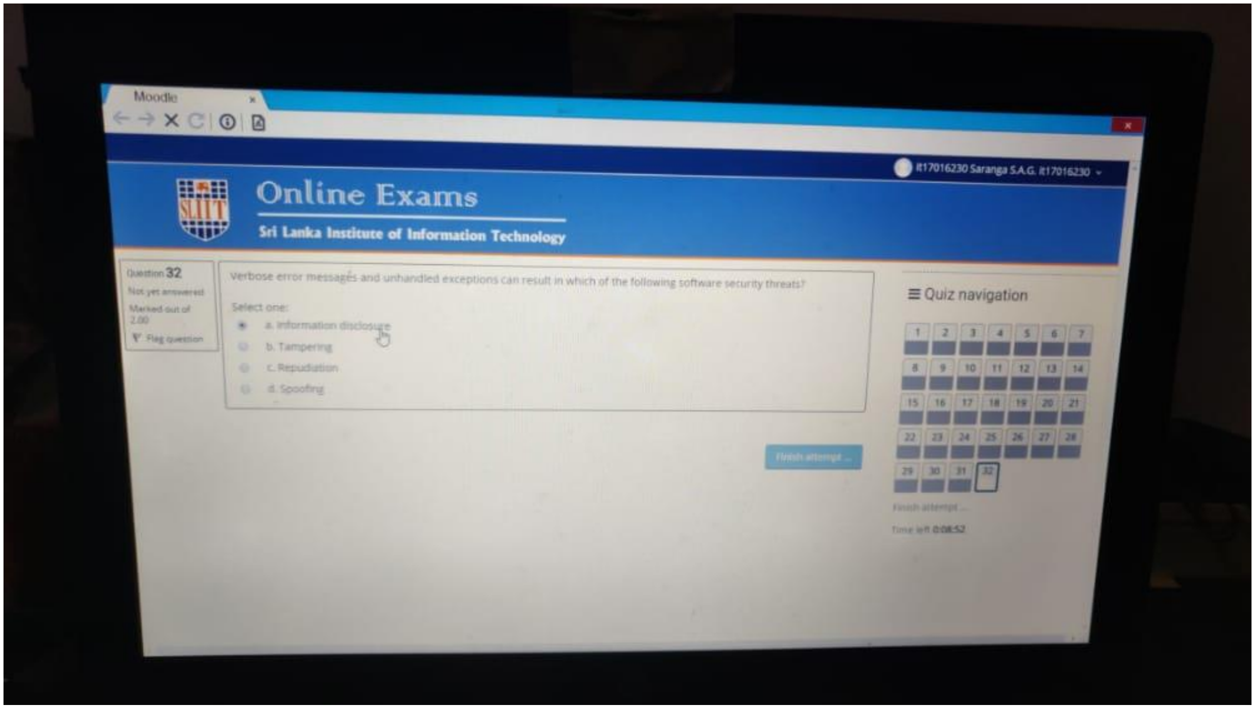


When two or more trivial pieces of information are brought together with the aim of stealing sensitive information, it is referred to as what type of attack?

Select one:

- ○ a. Polyinstantiation
- ○ b. Phishing
- ○ c. Inference
- ● d. Injection

Question 32



Question 32

Not yet answered

Marked out of 2.00

Flag question

Verbose error messages and unhandled exceptions can result in which of the following software security threats?

Select one:

● a. Information disclosure

○ b. Tampering

○ c. Repudiation

○ d. Spoofing

Time left 0:08:52