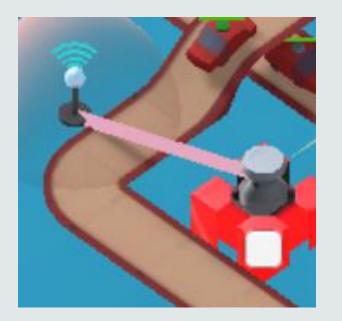
CyBok Project Showcase



SECURE CODING **GAME-BASED LAB**

2nd March, 2022

Manual Maarek

Sheung Chi Chan Heriot-Watt University

Leon McGregor

Secure Coding Game-based Lab

- Educational lab for secure coding based on a serious game of tower defence
- Complete the game-based educational platform by linking its security documentations and learning materials to CyBOK 1.1
- Help to promote serious game based learning of CyBOK



Educational Lab

Citadel Programming Lab

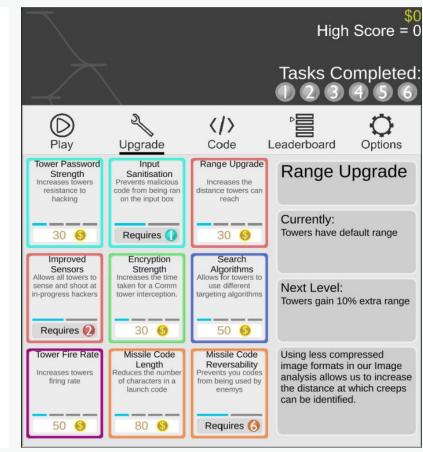
Task: SSL/TLS

Task: SSL/TLS

Transport layer security (TLS) is the successor of the now-deprecated Secure Socket Layer (SSL). They are a cryptographic based protocol to help establish and provide a secure communication channel between two stranger hosts through computer network. It can be adopted by different application in the application laver, like emails, Voice over IP (VOIP) or act as the secure channels for HTTP communication with the HTTP over SSL (HTTPS) services. TLS does not require the communication parties knowing each other in advance, the only requirement is they have the similar set of certificate validation through the x.509 certificate and public key infrastructure. With that, TLS can provide certain security features, including privacy, confidentiality, integrity and authenticity (optional) between two or more strangers who wish to communicate securely. The certificate validation and the cryptographic details and secret used in the communication are negotiate through a handshake protocol at the start of the communication. Optional two way authentication could be implemented. After a success negotiation, the TLS record protocol on each end of the communicating parties will make used of those agreed cryptographic choice and secret to wrap all remaining traffic to provide those security features. TLS is originally proposed by Internet Engineering Task Force (IETF) as SSL by Netscape in 1999.

Practical Tasks

Many of the existing SSL/TLS software and libraries has provide certain default settings to allow quick and secure negotiation of the communication channels. But sometimes when one of the parties does not have the latest standard of protocol supported, the default setting may forced to lower the security level and choose some older protocols. Also, with all those default settings, you will not have the chance to understand how the real negotiation and parameters has been considered and performed. Thus in this task, you are ask to implement a method to



keyring = KeyringContigs.torGpgExportedKeys(KeyringCont

keyring = KeyringConfigs.forGpgExportedKeys(KeyringConf

n.addSecretKey(senderPrivateKey.getBytes(StandardCharsets .addPublicKey(senderPublicKey.getBytes(StandardCharsets. .addPublicKey(receiverPublicKey.getBytes(StandardCharset ption | PGPException e) { ntStackTrace(); null;

ign the message with the stored keyring
Stream baos = new ByteArrayOutputStream();

BufferedOutputStream bos = new BufferedOutputStream(bao

- OutputStream os = BouncyGPG.encryptToStream()
 - .withConfig(keyring)
 .withStrongAlgorithms()
 .toRecipient(receiverEmail)
 .andSignWith(senderEmail)
 .armorAsciiOutput()
 .andWriteTo(bos):

Linkage to CyBOK



Input Sanitisation Input Sanitisation Input Sanitisation Encryption Network Safety Passwords Security Education Detecting Malicious Activity Activity Building Defences What is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered. How can a script be injected?	CyBOK		Х		
Input SanitisationWhat is input sanitisation?EncryptionInputs should be "sanitised", meaning they should be checked for malicious content, if any is found it should not be processed.Network SafetyHow are commands injected?PasswordsMost commonly, command injections are a result of misplaced trust in user inputs or data. Where a system blindly processes requests without checking whether they are dangerous.Security Education Detecting Malicious ActivityWhat is command injection? A command injection is when a malicious program or attacker trick a user or system into running dangerous commands locally to gain illegal/over-privileged access or informationWhat is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered.How can a script be injected?	https://www.cybok.org	Input Sanitisation			
Input SamusatorEncryptionInputs should be "sanitised", meaning they should be checked for malicious content, if any is found it should not be processed.Network SafetyPasswordsMost commonly, command injections are a result of misplaced trust in user inputs or data. Where a system blindly processes requests without checking whether they are dangerous.Security EducationDetecting Malicious ActivityBuilding DefencesWhat is command injection? A command injection is when a malicious program or attacker trick a user or system into running dangerous commands locally to gain illegal/over-privileged access or informationWhat is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered.How can a script be injected?	Input Sanitisation				
Encryptionmalicious content, if any is found it should not be processed.Network SafetyHow are commands injected?PasswordsMost commonly, command injections are a result of misplaced trust in user inputs or data. Where a system blindly processes requests without checking whether they are dangerous.Security Education Detecting Malicious ActivityWhat is command injection? A command injection is when a malicious program or attacker trick a user or system into running dangerous commands locally to gain illegal/over-privileged access or informationWhat is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered.How can a script be injected?	Input Sanitisation	What is input sanitisation?	\square		
Passwords Most commonly, command injections are a result of misplaced trust in user inputs or data. Where a system blindly processes requests without checking whether they are dangerous. Security Education What is command injection? Detecting Malicious Activity A command injection is when a malicious program or attacker trick a user or system into running dangerous commands locally to gain illegal/over-privileged access or information What is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered. How can a script be injected?	Encryption				
Passwords user inputs or data. Where a system blindly processes requests without checking whether they are dangerous. Security Education What is command injection? Activity A command injection is when a malicious program or attacker trick a user or system into running dangerous commands locally to gain illegal/over-privileged access or information What is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered. How can a script be injected?	Network Safety	How are commands injected?			
Security Education What is command injection? Activity A command injection is when a malicious program or attacker trick a user or system into running dangerous commands locally to gain illegal/over-privileged access or information What is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered. How can a script be injected?	Passwords	user inputs or data. Where a system blindly processes requests			
Activity A command injection is when a malicious program or attacker trick a user or system into running dangerous commands locally to gain illegal/over-privileged access or information What is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered. How can a script be injected?	Security Education				
Building Defences user or system into running dangerous commands locally to gain illegal/over-privileged access or information What is taint analysis? Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered. How can a script be injected?					
Taint analysis is the general term for analysing code in search of input vulnerabilities, which should be fixed when discovered. How can a script be injected?	Building Defences	user or system into running dangerous commands locally to gain			
vulnerabilities, which should be fixed when discovered. How can a script be injected?		What is taint analysis?			
A maliciously written input into an improperly sanitised input field can		How can a script be injected?			
trick the server handling the input response into running the input as code. This happens most often when special characters (such as		trick the server handling the input response into running the input as			
Citadel Programming Lab	A upity V				

CyBOK Knowledgebase Coverage

CyBOK 1.1 knowledge areas and topics	In-game exercises and corresponding game meta- phors	
Applied Cryptography		-
Authenticated Encryption(AE)schemes	String encryption	
Binding Public Keys and Identities via Certificates	Certificates	
Cryptographic Libraries	All exercises	Risk N
Diffie-Hellman Key Exchange	SSL	risk a
Digital Signatures	PGP	Secur
Hash functions	Credential storage	motiv
Managing Public Keys and Public Key Infrastructure	PGP, certificates	
Law & Regulations		Softw
electronic signatures and indentity trust services	PGP	SQL
prescriptive jurisdiction and data protection	Credential storage	codiı
Network Security		quer
Public Key Infrastructure	PGP, certificates	Web 8
TLS (Transport Layer Security)	SSL	SQL
Privacy & Online Rights		
cryptography-based access control	String encryption	input
obfuscation-based inference control	URL shortener	pass
privacy engineering	String encryption, URL	web

Risk Management & Governance risk assessment Secure Software Lifecycle motivations for secure software lifecycle Software Security SQL injection coding practices query generation Web & Mobile Security SQL-injection input sanitisation password leaks web PKI and HTTPS

All exercises

All exercises

Credential storage All exercises Credential storage

Credential storage Credential storage Credential storage PGP, certificates

Project Resources

Project public webpage

https://citadel-programming-lab.gitlab.io/

Project source and deployment guideline

https://gitlab.com/citadel-programming-lab/citadel-programming-lab