Title: Threat Modelling Exercises

create a threat model based on one of the following scenarios:

1. A large international bank based in the UK.

You should use the Threat modelling Manifesto, the OWASP Threat modelling Cookbook and the ATT&CK libraries to inform your model design. Be prepared to share and discuss your designs at the seminar session this week.

You should also add your individual designs to your e-portfolio.

Application Version: 1.0

Description :

A large international bank based in the UK. With main users of the application.

Customers – who will be able to transfer money

Staff – Providing assistance to customers

Other organisations who need to make use of money being transferred from organisation to another

Government bodies – who set rules and regulations to banks.

External Dependencies

ID	Description
1	External Users logging onto the web server remotely
2	Internal Users logging onto the web page remotely (WFH)
3	Database running connecting to the web page over a private network
4	Web server is behind a Firewall using TLS /HTTPS
5	Large amount of sensitive data being handled

Entry Point

ID	Name	Description	Trust Levels
1	HTTP Ports	Web page will only be available by TLS and HTTPS	1- Users with valid login 2- User with invalid login 3- Staff
2	Main page	All users enter from the same page	1- Users with valid login 2- User with invalid login 3- Staff
3	Login Function	Function checks credentials with the database and ensure SSL secure shell logging is implemented	1- Users with valid login 2- User with invalid login 3- Staff

Exit Points

ID	Description
Cross Site Scripting	Man in the middle attacks on the web page
SQL injection	SQL attacks and modifying the Database
Denial of Service	Continues ping of service until the system is unresponsive.
Data Protection	Data Loss Protection DLP data being modified

Assets

ID	Name	Description	Trust Levels

1	User Login	Credentials for Staff and customers	1- Users with valid login 2- User with invalid login 3- Staff
2	Personal Data	Customer and Staff details	DB admin Web server's user process Database read /write
3	Web server	Access 24 by 7	Database and Web Server Admins
4	Enhancements	Execute code	Database and Web Server Admins
5	Least privilege access	Enforce least privilege access	Database, Web Server Admins and Other Staff.
6	Policy	Security and data protection Policy	All staff and customers

Trust Levels

ID	Name	Decription
1	Staff and Customers Login	Valid login details
2	Admin Login	Web Server and Database Admins
3	Least privilege access	Any super access needs justification and approved

Threat	Property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability

Elevation of Privilege	Authorization

Type of vulnerability	STRIDE Threat property	Threat	Definition	Mitigation	Recommendation	Business Impact
Network	Availability	Denial of Service DOS Attack	An attack to make the service inaccessible	Firewall Intrusion Detection System	Continues network scanning	Loss of website
Network	Availability	Phishing attack	To obtain user details by tricking the individual	Staff Training	Install anti redirectors	Loss of data
Network	Information disclosure	Misconfigured Firewalls	Company requirements not followed Outdated firewall rules	Firewall Maintenance	Reviewing periodically	Cyber attacks
Network	Integrity	Attacks on Wireless Network	Capture or modify information sent across the wireless network	Encrypting data	Least privileged access Model	Loss of data
Network	Integrity	Malware Attack	Malicious software executed designed to cause harm to the device or network.	Antivirus software	Patching the antivirus software	Exploiting vulnerability
Network	Authenticity	Spoofing (Man in the middle)	Something is pretending to be something else and modifying the data	Staff Training Using spam filters	Managing End to end connection	Loss of data

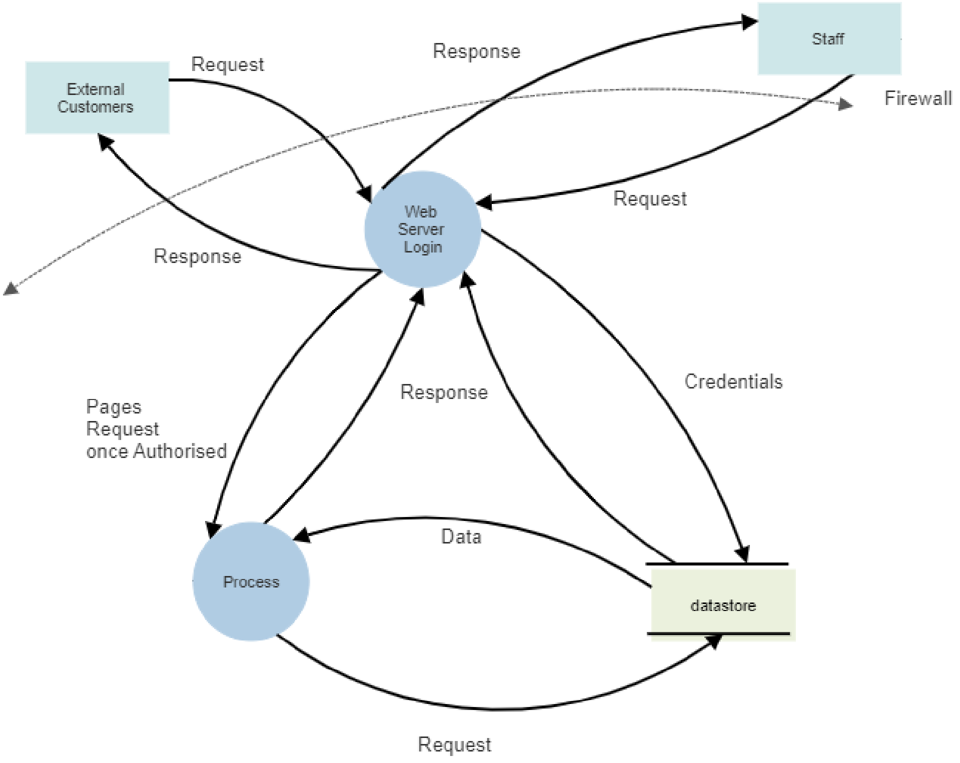
Network	Confidentiality	Data Theft	Information is stolen or taken without consent	Strong Password Encryption	Password Policy Multi-Factor Authentication	Data loss Business image impacted
Network	Integrity	Traffic Analysis attack.	Monitor the traffic flow to and from the network to obtain information	Network Scanning tools	Up to date Firewalls Intrusion Detection System Intrusion Prevention System	Loss of Data
Network	Integrity	Network Injection	Sending harmful packets within the network.	Network Scanner	Intrusion Detection System Intrusion Prevention System	Loss of data
Network	Availability	Botnets attack	Network of devices are hijacked to perform various attacks	Network scanner Configured Firewall	Intrusion Detection System Intrusion Prevention System Firewalls	Loss of website
Operating System	Authorisation	Open Ports	Ports left open can be used as a pathway for attacks	Block all unused ports	Firewall Intrusion Detection System Intrusion Prevention System	Loss of website
Operating System	Authorization	Protocol Vulnerability	Exploiting loopholes within common communication protocols like HTTP, ARP, FTP Telnet.	Vulnerability scanner	Patching to the recent versio.	Exposed to attacks.

Operating System	Authenticity	Default configurations/ Password	Not changing the system default passwords.	Disable service accounts.	Least privileged access model Regular audits Log reviews	Exposed to attacks
Operating System	Availability	Command Injection	Executing harmful OS commands to the Host Operating System	Network Scanner	Intrusion Detection System Intrusion Prevention System	Loss of data
Process	Integrity	SQL Injection	Executing SQL command to the database	Network Scanner	Intrusion Detection System Intrusion Prevention System	Loss or modification of data
Process	Availability	Brute force attack	Password trial and error attack	Strong Password	Mandatory password policy	Loss of website
Human	Confidentiality	Lack of Password policy	Organisation is not set and following the policy	Strong Password	Mandatory password policy	Loss of website
Human	Authenticity	Social Engineering attacks	Trying to obtain information to gain access to the system by exploiting the weak link of humans	Staff Training Education programs	Password Audit Random security assessment	Loss of data Loss of website
Human	Authorization Authenticity	Un-trained employees	Not providing cyber security training	Staff training Education program	Password Audit Random security assessment	Loss of data Loss of website
Human	Authorization	Lack of Social	Staff access social	Restricting the use of personal	Block social networking sites	Loss of data

	Authenticity	media policy	media during working hours or using work email addresses for personal use.	mail and websites during office hours		Loss of website.
Human	Authorization Authenticity	Misusing privileges or Access Rights.	Logging into a system with elevated access to perform non-admin tasks	Apply for least privilege access	Access control Policy	Loss of data Loss of website Loss of control
Software	Integrity	DOM injection	Manipulating the JavaScript vulnerability	Vulnerability scanner	Patching to the recent version.	Exposed to attacks
Software	Integrity	Software Library Zero-day attacks	Vulnerabilities exploited on the day of release of software	Vulnerability scanner	Patching to the recent version	Exposed to attacks.
Software	Integrity	Buffer overflow	Overwriting the buffer erasing the actual code	Secure coding	Secure coding practice	Exposed to attacks
Software	Integrity	Cross site scripting	Web application inject client side script to the web pages	Secure coding	Secure coding practice	Exposed to attacks
Software	Authenticity	Directory travels	No validation access rights in place to go to the	Secure coding Access Privileges	Secure coding practice Access rights audit via logs	Exposed to attacks

			parent directory.			
Software	Authenticity	Server-side request forgery (API forgery)	Attackers will attack the server and get and try to modify the resources.	Secure coding Access Privileges	Secure coding practice Access rights audits via logs	Exposed to attacks
Monitoring	Integrity	Review logs for suspicious activity	Periodically check logs for any abnormal activity	Review logs	Access rights audit	Identify potential threats
Data Protection	Confidentiality	Data protection standards	Follow the UK Data Protection standards	Review of the standards is maintained	Follow the standards when accessing the site	Policy breach

International bank based in the UK



Threat Tree Diagram.

DREAD

https://owasp.org/www-community/Threat_Modeling_Process

DREAD	Description	Impact	Scale	
Damage	Impact of attack	Reputation Loss of Data Loss money Data Modification Site unavailable Loss of customers	10	
Reproducibility	The attack can be reproduced	Mitigation of vulnerabilities Reviewed periodically Staff education to prepare for attacks.	2	
Exploitability	How easy to exploit the threat	Reputation Loss of Data Loss money Data Modification Site unavailable Loss of customers	7	
Affected users	Number of people effected	Impact to customer with account and payments Impact to staff due to reputation loss.	10	

		Impact to the stake holders.		
Discoverability	Discover the threat	With security teams reviewing the firewalls, Policy and network traffic the threat is easily discovered.	8	

Overall DREAD score for this threat: (10+2+7+10+8) / 5 = 13