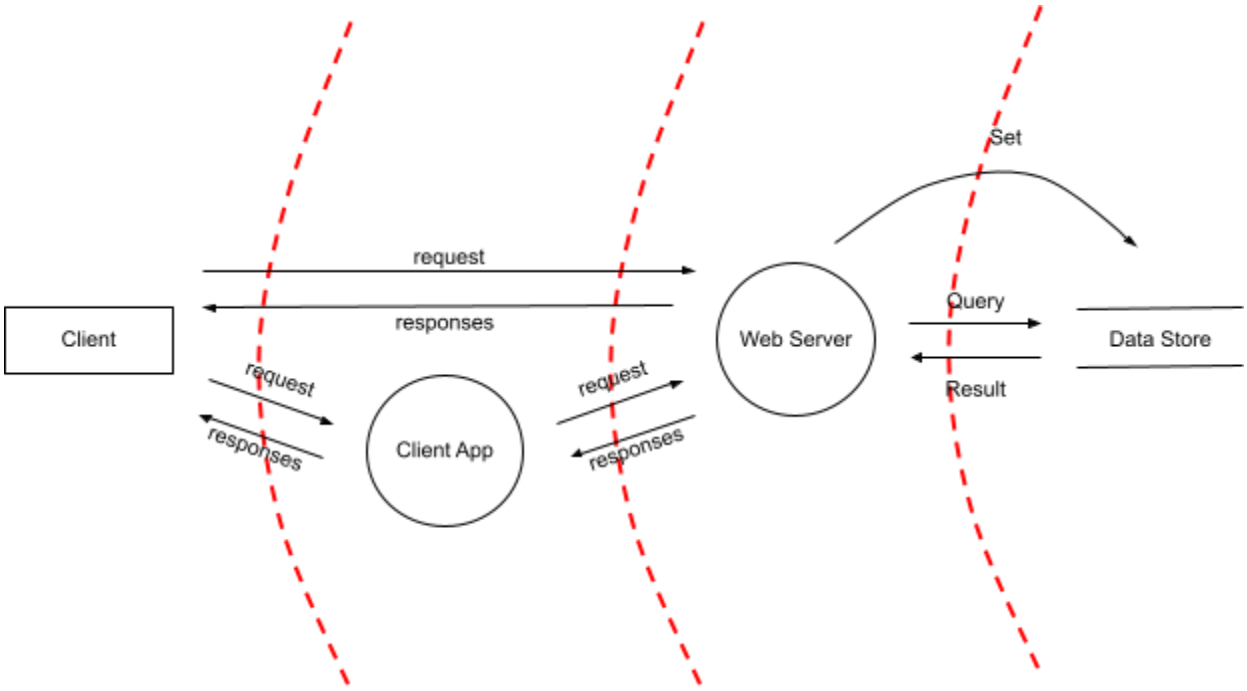
Jared Chen
May 5, 2022
CS338

THREAT ANALYSIS USING STRIDE

Data flow diagram:



STRIDE element	Threat	Mitigation
Spoofing	Mal could create a fake web client that was very similar to our real web client. Users might unknowingly try to log into Mals website, giving up either username and password.	We would want a CA to give us a certificate to prove our website is the real tapirs.com. This would give us the little lock icon in the url bar in google.
Tampering	Since we have an HTTP channel between client and web server, Mal could easily perform a PITM attack and modify packets between the two sides.	Interactions between client and web server should use HTTPS.

Repudiation Threats	If Mal somehow got access to a users account, they could build and send themselves tapirs merch using the users credit card information. The user would later claim they didn't purchase tapirs merch.	Some form of two factor authentication would prevent this as acess to the account is not enough the perform monetary transactions on the site.
Information Disclosure	HTTP is not secure, an evesdropper could access unauthorized information by reading packets.	HTTPS should be used for interactions. Encrypting packets pevents eavesdropping.
Information Disclosure	Mal could potentially send the database queries that contain SQL injection attacks. This would leak sensitive information.	Using techniques like parameterized queries, we can prevent SQL from running user input directly as code. This would prevent injection attacks from being valid inputs.
Denial of Serice	Mal could overload the server with requests, freezing/crashing the server, and preventing real users from accessing tapirs content.	Use tools such as AWS shield (not using AWS in this case) or CloudFlare to prevent DoS attacks.
Elevation of Privileges	Our site only require a username and password to sign in. If an attacker gets a username, they may be able to get the password through various means such as guessing, phishing, etc. If they access the username ans password, they have access to tapirs content they shouldn't be able to access.	Enabling some sort of two factor authentication would greatly increase the security as you would no longer be able to sign in with just a username and password.
Elevation of Privileges	Mal breaks into Jeffs house and steals the database (physical computer). They can now access all data on database.	Jeff needs better locks?
other	Passwords are saved in the database, so if a malicious	Using the salt$hash method, we can verify username and

	person gets access, they have access to all accounts on the site.	password without saving the password. Credit card information should also be encrypted in some sort of way.