Threat Model:
Craft Project

Dam Security

Sunwoo Kim, Billy Endicott, Ian J Delgado, Alanna Croysdale

17 January 2023

CS 46X

Success Measures

Identification of any possible threats to our clients software available to the public. The threat modeling process will include identifying threats at each level of the web application from users to the backend to cloud services. Proper threat modeling can help identify countermeasures for each attack surface present in a web application environment. The focus of the threat modeling process on the craft team's project will be to identify the most probable threats and attacks to this web application. Below is a list illustrating expected threats at each level starting with users accessing the web application.

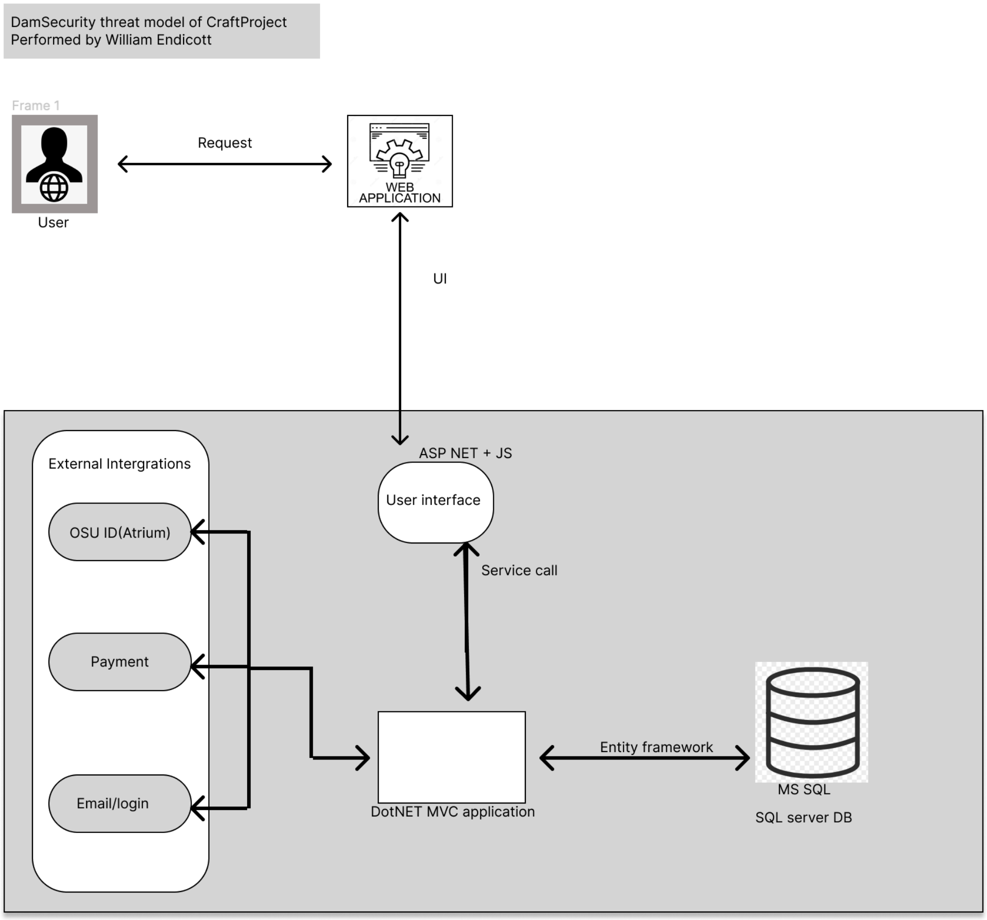

Figure 1. Basic outline of the architecture for the web application, used from the presented documentation and schematic designed by the development team of the craft team's project.

Users

Social engineering remains one of the most damaging aspects to businesses and companies. Simple social engineering can lead to malware, ransomware, leaking of credentials, and loss of digital assets. Given the importance of protecting user and employee data, it is necessary to at least minimize phishing attempts via email, phone, and even physical mail. On OWASP's top ten list of security risks, the second vulnerability listed is cryptographic failures. Cryptographic failures can lead to insecure communication. The craft team's project will be dealing with the use of users' credit cards, banking information, and shipping addresses. The use of this personal information of the users can lead to a man in the middle attack and subsequently a social engineering attack. Assets at risk in a social engineering attack on the craft team's project include customer data, employee data, availability of service, and payment information.

Web Application

The third listed vulnerability on OWASP's top ten is injections. SQL injection (SQLi) and cross-site scripting (XXS) are the most dangerous and common weaknesses in online applications. DoS (denial of service) attacks and attacks involving authentication methods are also common threats. If a website has weak authentication recommendations for its users, that can lead to a higher than normal amount of accounts being compromised.

Identification and authentication failures are listed as seventh on the OWASP's top ten. Insecure communication and platform misconfiguration will also lead to various other attacks. Security misconfiguration is the fifth vulnerability listed on the OWASP's top ten. Having all the security in the world will be useless if the application is misconfigured and vulnerable ports remain open. Assets at risk in an attack on the craft team's project involving the web application include user and employee data, user and employee authentication credentials, and sensitive material that may be stored, including payment information and associated addresses.

Files/Database

Files will have similar threats that are included in the database section. Improper encryption of data while at rest and in transit is the greatest concern for this section. A great majority of the threats from the web application section also apply here as well including SQLi and improper platform configuration. The information provided by users will be stored in the database so unencrypted sensitive data at rest needs to be accounted for since that is a commonly missed aspect of security. Files storing employee credentials, admin credentials, and customer data are the assets at risk.

Logs

Logs are an important part of running a service online. Maintaining proper security logs and event logs will help later identify if someone did something malicious on the website. It would be important to log and maintain a running file of documents that are updated and by who as well as any information that can be obtained from the interaction. If someone uploads a malicious file and an offensive file we would want the ability to find that person and hold them responsible. This is where one of the key pillars of information security comes into play. Non-repudiation will allow the administrators of the website to log the sender's information that is provided from the network traffic as well as the credentials associated with the traffic.

External Integrations

This will handle the login credentials for people accessing the product. Insecure communication is a priority to identify. Risk of attack methods on two factor authentication are seen at this level. Those include but are not limited to SMS-based man-in-the-middle attacks, pass-the-cookie attacks, and social engineering attacks from the use of 2FA. Overall, this is a service that will be handled outside of the project team's hands but it will need to be checked for the correct configuration.