Stride Assignment

By: Sydney Nguyen

Spoofing:

Threat: Mal could do several things to spoof Jeff. Mal could simply guess Jeff's username and password however this is very inefficient, as there are many combinaitons of letters and number Jeff could choose. A better technique would be to make a fake website of Tapirs Unlimited and send it to others and having them attempt to sign in to the account unders the conditions of needing to change their password because of a security breach, and give them an error. Now Mal would have full access to Tapirs Unlimited accounts.

Mitigation: Create a public key infrastructure(PKI) with certificates. To stop Mal once they have gained all access to the accounts making a two factor authentication so the user or Mal not only needs the information, but access to a trusted deceive or account.

Tampering:

Threat: Mal needs to change the data stored in the sever by either SQL injection or a HTML injection. These injections could allow Mal to alter or corrupt data in the database

Mitigation: Tapirs Unlimited can make a user data validation fields or use HTTPS which would cause Mal a PITM to see incoherent data.

Repudiation:

Threat: Mal could use another person's infromation of fake infromation pretending to be a client. Then Mal could pretend to be other clients and post harmful information with no reprercussions to Mal's account because they use someone elses.

Mitigation: A obvious way is to allow the original user that Mal is pretending to be to simply delete the post, or again force a two factor authentication to only allow the person to post items.

Information Disclosure:

Threat: Mal could person in the middle (PITM) the conversations between clients and the server. Mal could also if they get access to Jeff's account through phishing could release credentials of other accounts into the world.

Mitigation: Using HTTPS stops Mal from being able to eavesdrop on the client and server conversation and the other issue Jeff would never let anyone have access to his account and has the most secure password that could never be guessed.

Denial of Service:

Threat: Mal could DDos or make so many posts that Tapir Unlimited will not be able to function either denying Mal service because the website can no longer run. If the website does not crash then the website may be so slow that others will not be allowed to use the site.

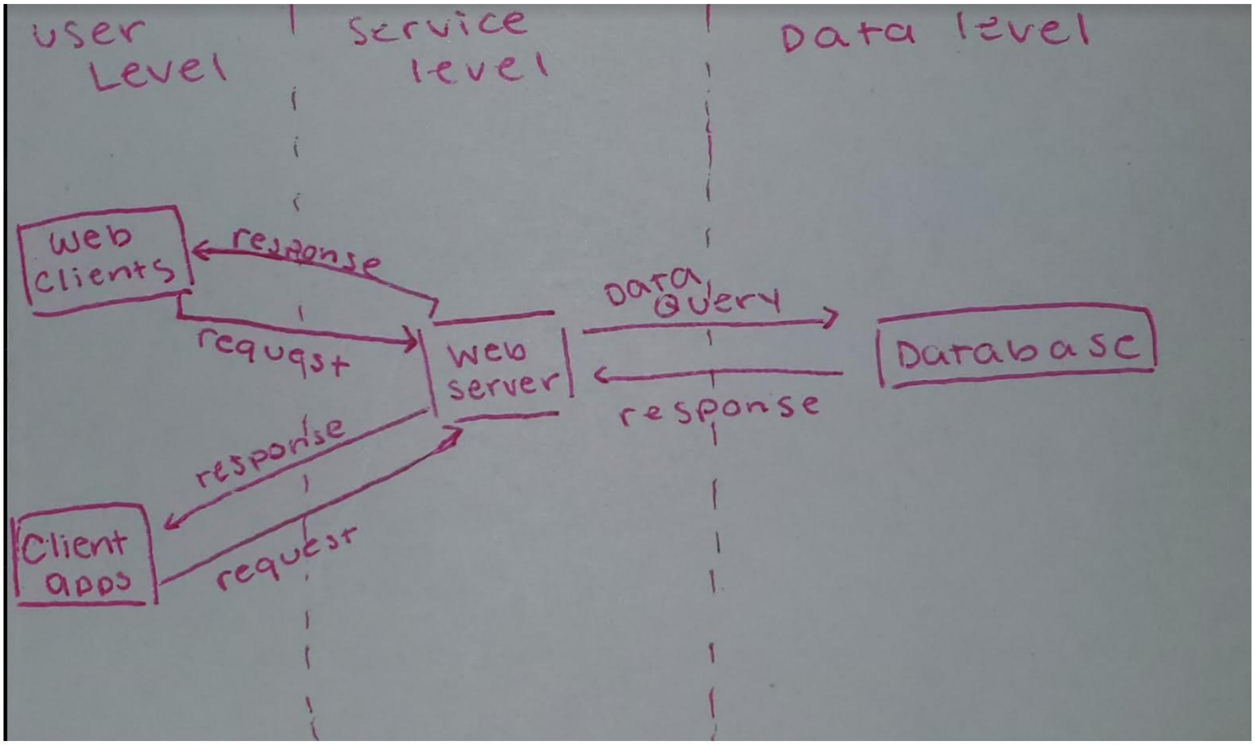
Mitigation: DDos attacks to my knowledge can not be prevented, but Tapir Unlimited can make it harder for the attacks to make the website unresponsive. For example Jeff could make a limit on the size of files that are posted or, a limit on the amount that a client can post in a given time.

Elevation of Privilege:

Threat: Mal could pretend to be a linode developer or that they are a big shot that is coming to help imporve Tapirs Unlimited and makes Jeff give them admin. If tapirs does not have something that stops Mal, Mal could simply give themself privilege and go wild deleteing posts, accounts, and spreading false anti tapir propaganda.

Mitigation: Two factor authentication or a certificate to prove Mal is actually who Mal claims to be, and Tapirs Unlimited could create a system that he only has the password to that gives other admin privileges.

Graph:


user Level
Service level
Data level
web clients
response
requqst
web server
Data Query
Database
response
response
Client apps
request