Lily Haas
Brainstormed with Ashok Khare and Emma Roskopf
Threat Analysis Using STRIDE

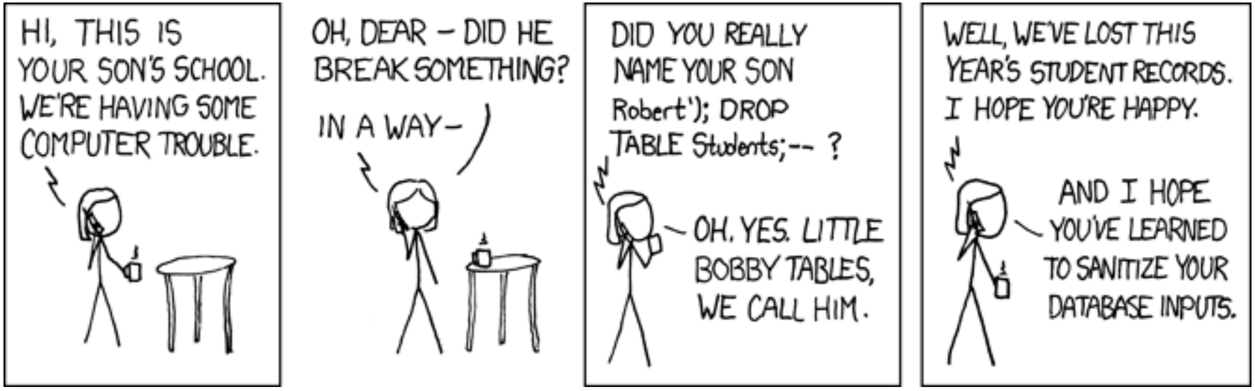
Possible Threats to Tapirs Unlimited by STRIDE Category

Spoofing

1. A rival company makes a fake Tapirs Unlimited with false information on it. They start stealing traffic from the real Tapirs Unlimited.
    a. Mitigations: Make sure you have a valid certificate and send the fake website a cease and desist.
2. Someone private messages users and poses as a mod to trick them into sending their passwords.
    a. Mitigations: Give moderator accounts a special symbol that verifies they are a mod and put a warning in private messages to never send your password to anyone, even moderators.
3. A moderator signs in to their account while on a fake wifi network (ie someone's phone hotspot renamed to the name of a local business) and their password is intercepted.
    a. Mitigations: Require moderators to use two factor authentication and have moderator sign in take place with HTTPS.
    b. This can also be considered Information Disclosure but since the scenario involves a fake network I am placing it under Spoofing.

Tampering

1. Someone uses SQL injection in their username to delete data from the database.


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

    a. Mitigations: Sanitize your inputs.
2. A guest in Jeff's house uses his computer to modify usernames on the database.
    a. Mitigations: Jeff puts a password on his computer.

Repudiation

1. Someone whose account has been banned creates a new account to circumvent the ban.
    a. Mitigations: Ban Ips in addition to accounts.
2. Someone gets usernames from public forum posts and continually tries common passwords on them until one works.

    a. Mitigations: Prevent users from using common passwords, require two factor authentication when logging in from a new location.

Information Disclosure

1. Someone uses SQL injection to acquire credit card numbers from the database.
    a. Mitigations: Sanitize your database inputs.
2. An administrator leaks database information.
    a. Mitigations: Require anyone with database access sign an NDA.

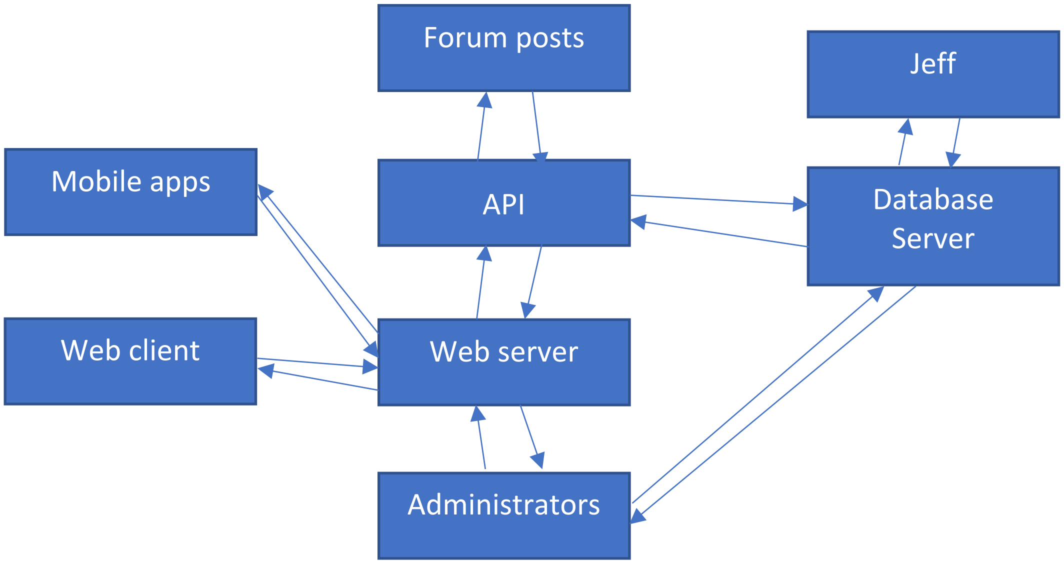
Denial of Service

1. Jeff's computer has a wifi adapter in it and when he updates the operating system the wifi adapter cause the computer t constantly blue screen (yes this happened to me, yes I'm still annoyed.) Since the database cannot be accessed many aspects of the site do not work.
    a. Jeff makes sure his computer does not have hardware issues that would prevent it from working.
2. An update to mobile operating systems requires the application be updated to satisfy new requirements before the app can be used.
    a. Communicate with the App Store and Play Store about new requirements for upcoming software updates so you can have updates ready as soon as possible.

Elevation of Privilege

1. A Linode employee uses their access to the web server to promote themself to moderator and begins spreading misinformation on tapirs.
    a. Have a specific contract with Linode so if this happens you can sue for breach of contract.
2. A moderator forgets to log out of their account on a public library computer and someone finds the site logged in a few hours later.
    a. Add an auto log off feature that requires users to re-input their password after a period of inactivity.

Data Flow Diagram


Forum posts
Jeff
Mobile apps
API
Database Server
Web client
Web server
Administrators