Kai R. Weiner
Worked W/ Reuben Boero

Threat Analysis (STRIDE)

Spoofing:

- Threat: An eavesdropper could monitor the unencrypted HTTP exchanges a user takes to login, thereby gaining access to their login credentials. Using these credentials, they could impersonate any user.
    - Solution: Only allow HTTPS communication.
- Threat: Using an injection attack on sql, a query could be run to gain access to an account.
    - Solution: Code protective measures against injection attacks in SQL.

Tampering:

- Threat: An eavesdropper could monitor the unencrypted HTTP exchanges a user takes to login, thereby gaining access to their login credentials. Using these credentials, they could edit the settings and blog posts on any user's account.
    - Solution: Only allow HTTPS communication.
- Threat: Using an injection attack on sql, a query could be run to delete all database information.
    - Solution: Code protective measures against injection attacks in SQL.

Repudiation:

- Threat: An eavesdropper could monitor the unencrypted HTTP exchanges a user takes to login, thereby gaining access to their login credentials. Using these credentials, they could impersonate any user and make changes on their account such that the behavior could not be traced back to them.
    - Solution: Only allow HTTPS communication.
- Threat: Using an injection attack on sql, operations could be performed that couldn't be traced back to the perpetrator.
    - Solution: Code protective measures against injection attacks in SQL.

Information Disclosure:

- Threat: An eavesdropper could monitor the unencrypted HTTP exchanges a user takes to login, thereby gaining access to their login credentials. Using these credentials, they could get the unencrypted log in information, allowing them to steal credentials and view any persona on the account.
- Threat: An eavesdropper could monitor unencrypted HTTP exchanges and see private message exchanges. From these HTTP exchanges, they could also determine the IP of your database and thereby your house address using an IP location lookup.
    - Solution: Only allow HTTPS communication.

Denial of Service:

- Threat: From the single IP address, a malicious force could perform a ddos attack on the website.
    - Solution: Use a ddos protection service.
- Threat: A malicious person could determine the ip address of your database from unencrypted HTTP exchanges, track it down, break into your unprotected home office and steal your database, preventing the site from running.
    - Solution: Only allow HTTPS communication.
- Threat: Using an injection attack on sql, a query could be run to delete all database information, making the website unable to function.
    - Solution: Code protective measures against injection attacks in SQL.

Elevation of Privilege:

- Threat: Solution: In an API exchange to get credentials, a downgrade attack could be performed, allowing a user to get information they are not supposed to have.
    - Solution: Only allow the most modern version of TLS.
- Threat: Using an injection attack on sql, a query could be run to gain sensitive information about users, even the admin and their privileges.
    - Solution: Code protective measures against injection attacks in SQL.