Group Members:

Alexander Eirea, Keeth Smith, Kelvin Dover, Gregory Wilkinson

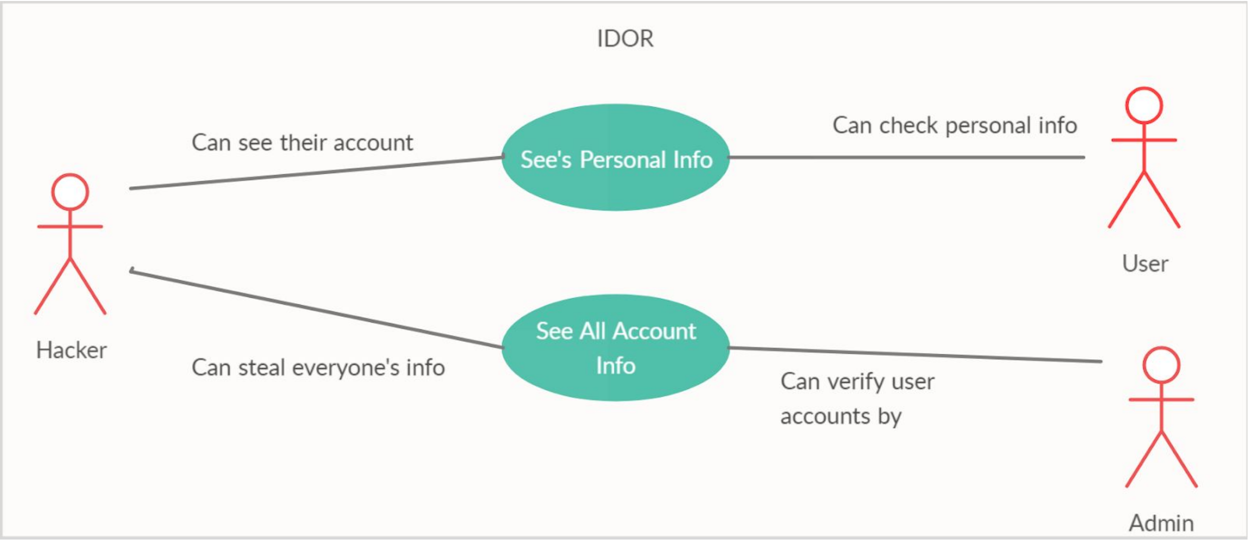
Due: 3/26/2020

Mini Project: Web Exploits (https://ss-kaks.herokuapp.com/)

IDOR

IDOR/URL manipulation attacks rely on a resource or resources being exposed to a user without access controls in place. This is typically a singular file, a database, or an admin dashboard. By gaining access to these resources an unauthorized user can gain access to and edit info they shouldn't have. IDOR attacks rely on URL path's being not verified against the user's status when accessing a page (ex. User vs Admin). The way this is mitigated is that every time a resource is accessed or data is changed, the user making the request is verified that they are able to edit the said resource. For example, on our website, the admin database can only be displayed by an admin user. If the user trying to access the admin database is not an admin, no info is displayed.

Abuse Case Diagram



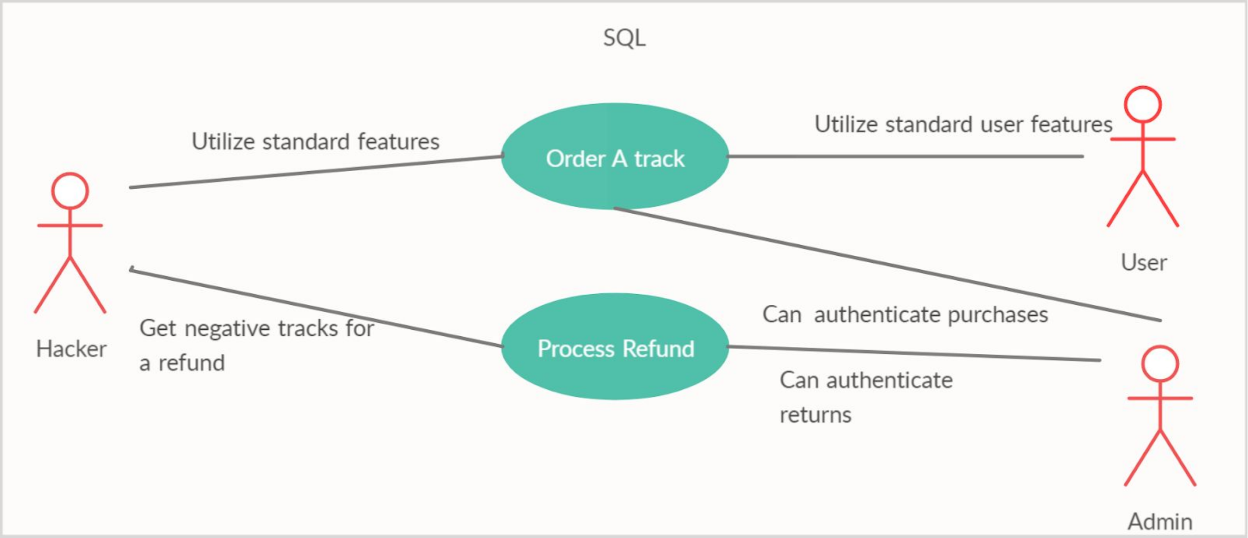
SQL

SQL injection attacks rely on input from a user being authentic input and not with malicious intent. This can be used for example in a log in where it is expected a username and password, but the user actually puts in an administrator username and a piece of code that when run against a SQL database evaluates to true, allowing access. The way this is mitigated is by what is referred to as "sanitizing" input. Input is expected to be malformed and necessary precautions are done ahead of time before it is passed to any database. Certain precautions are taken such as looking for critical escape characters such as "", '', or --. These characters can either throw an error or be deleted before running against the database.

Group Members:

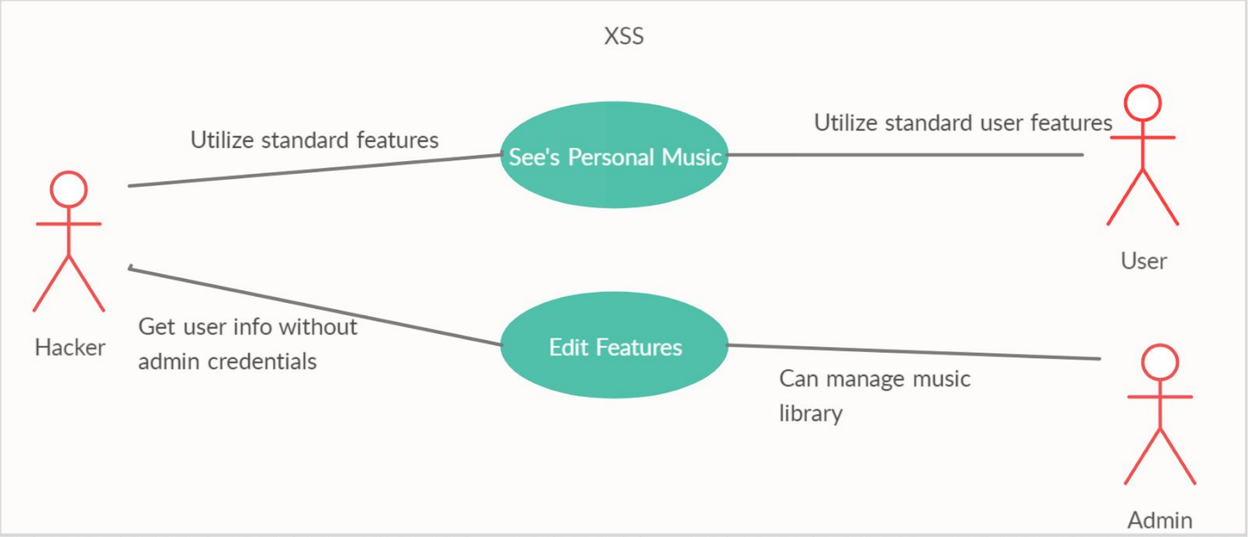
Alexander Eirea, Keeth Smith, Kelvin Dover, Gregory Wilkinson

Due: 3/26/2020


SQL
Utilize standard features
Order A track
Utilize standard user features
User
Hacker
Get negative tracks for a refund
Process Refund
Can authenticate purchases
Can authenticate returns
Admin

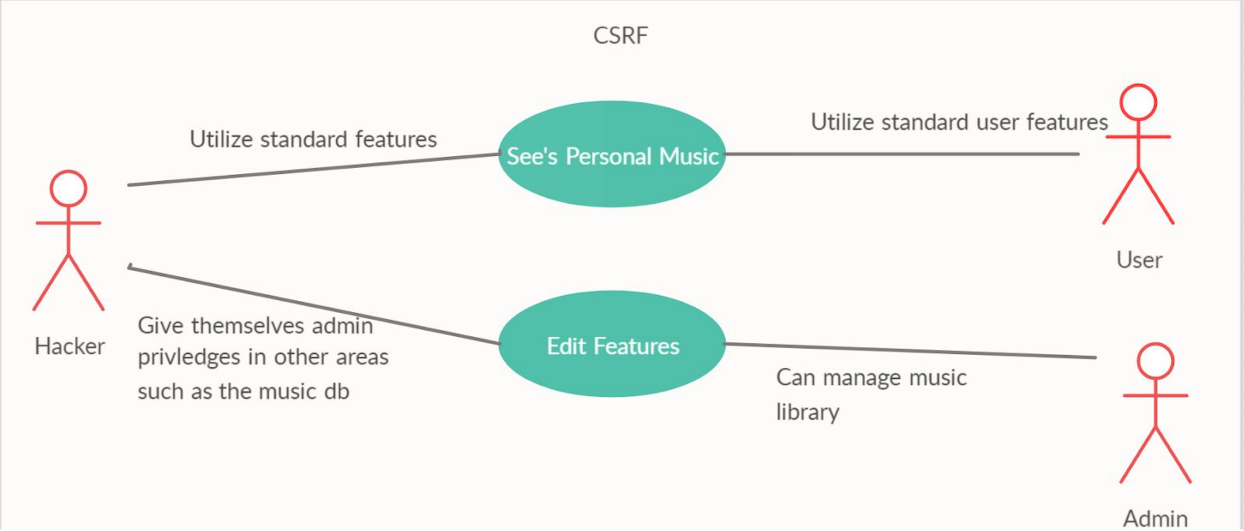
XSS

XSS attacks or "cross-site scripting" is similar to SQL injections in that it input malformed input into a parameter, such as code. However this is different in that instead of being run against a database, this is run against the web server itself, and its hope is for some critical information to be dumped by the server. The way that this is mitigated is similar to SQL in which the input is sanitized before any actions or responses are sent out. The characters are a little different in which you look for <,>, or "script". If these are found, it is either deleted or an error is thrown as the response.


XSS
Utilize standard features
See's Personal Music
Utilize standard user features
User
Hacker
Get user info without admin credentials
Edit Features
Can manage music library
Admin

CSRF

CSRF attacks force a user to execute actions unknowingly but are authenticated to do so. This attack relies on using state change requests since the end-user is what is executing the action, the user is what receives the response. By capturing a previous request, and tweaking it, that new request can now change an aspect unknowingly of the user. The way this attack is mitigated is by using specifically an "unpredictable" csrf token, tying it to a session of a user, and strictly verifying it every time an action is done.


CSRF
Utilize standard features
See's Personal Music
Utilize standard user features
User
Hacker
Give themselves admin privledges in other areas such as the music db
Edit Features
Can manage music library
Admin

Hashing & Encryption

Hashing in its essence cannot be reversed, it is a one-way operation. Once data is hashed, it cannot be unhashed. While that is not the case for encryption. Once data is encrypted, it can be unencrypted. Hashing also allows for two concepts, salt, and pepper. Both apply to data that is generated and appended to some other data before its combined result is passed through a hash. A Salt is kept in the database with the hash. A Pepper, however, is hardcoded in the website and applied to every password.