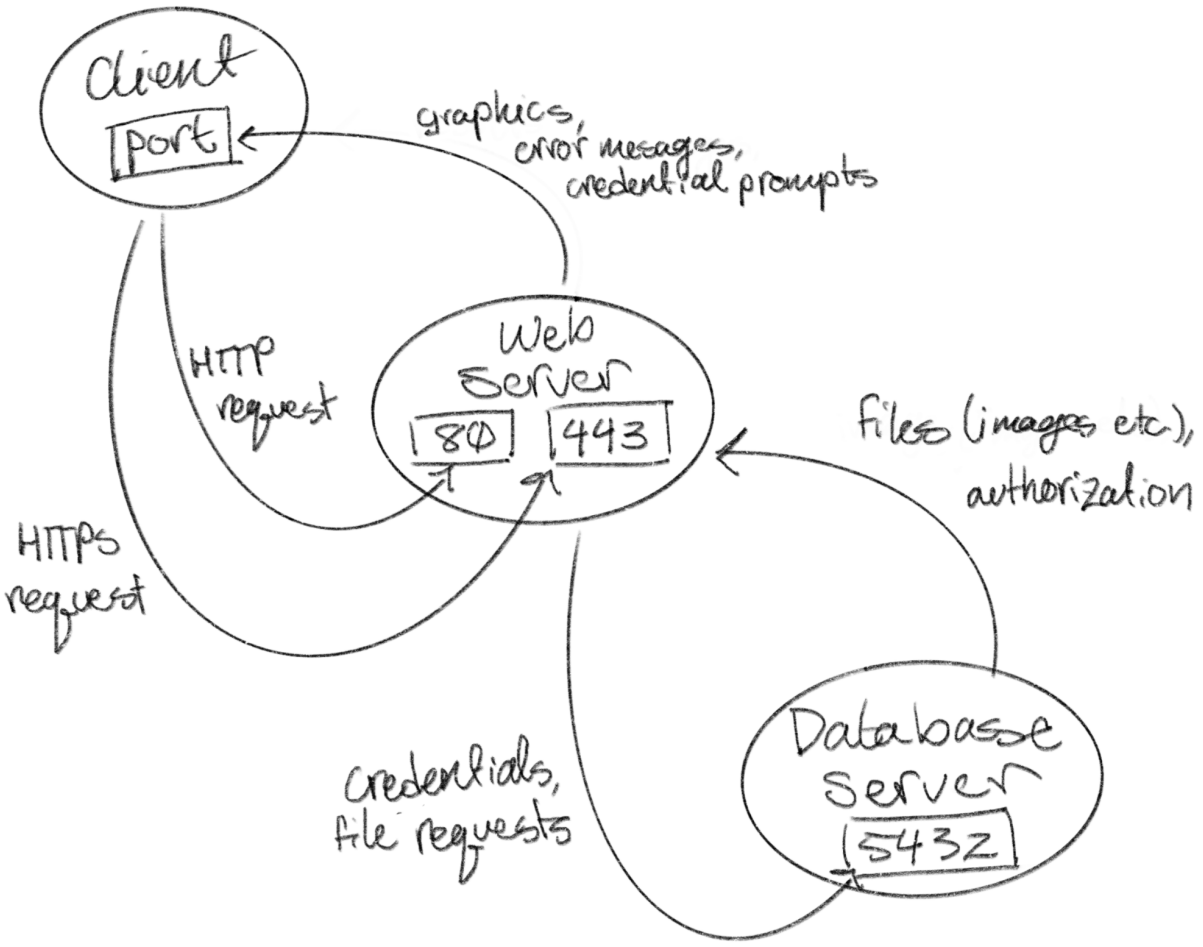
Phi Rapacz



Spoofing

Threat: Mal's client claims to be the web server asking for files for someone already logged in.
Precaution a: Web server has a public/private key, signature, and certificate of its own that the database server may check for.
Precaution b: Web server must submit a user's credentials for all restricted information (perhaps making use of a cache, which Mal would not have access to due to not actually being the web server).

Tampering

Threat 1: AITM changes the contents of a credential packet in order to prevent a user from accessing their account.
Precaution 1: I actually have no idea how to solve this one, because the AITM just wants to make the information invalid.

Threat 2: If Mal gains access to Jeff's office, they can mess with the physical server inside.

Precaution 2: Keep a backup of important files, updating periodically. Also, always lock your office Jeff and don't go giving Petra the key.

Repudiation

Threat: Once a user has gained access as an editor to the Tapir Wiki on the site, they can change the information of a page.
Precaution: Keep a record of changes to the Tapir Wiki (going back maybe not forever, but somewhat) and the account that made those changes.

Information Disclosure

Threat: Mal's client (or a dumb user's client) claims it cannot use HTTPS, asks to open a connection over HTTP.
Precaution: Do not allow servers to open connections over HTTPS. Just don't.

Denial of Service

Threat: (see T1)
Precaution: (see T1)

Elevation of Privilege

Threat: (see T2)
Precaution (see T2)