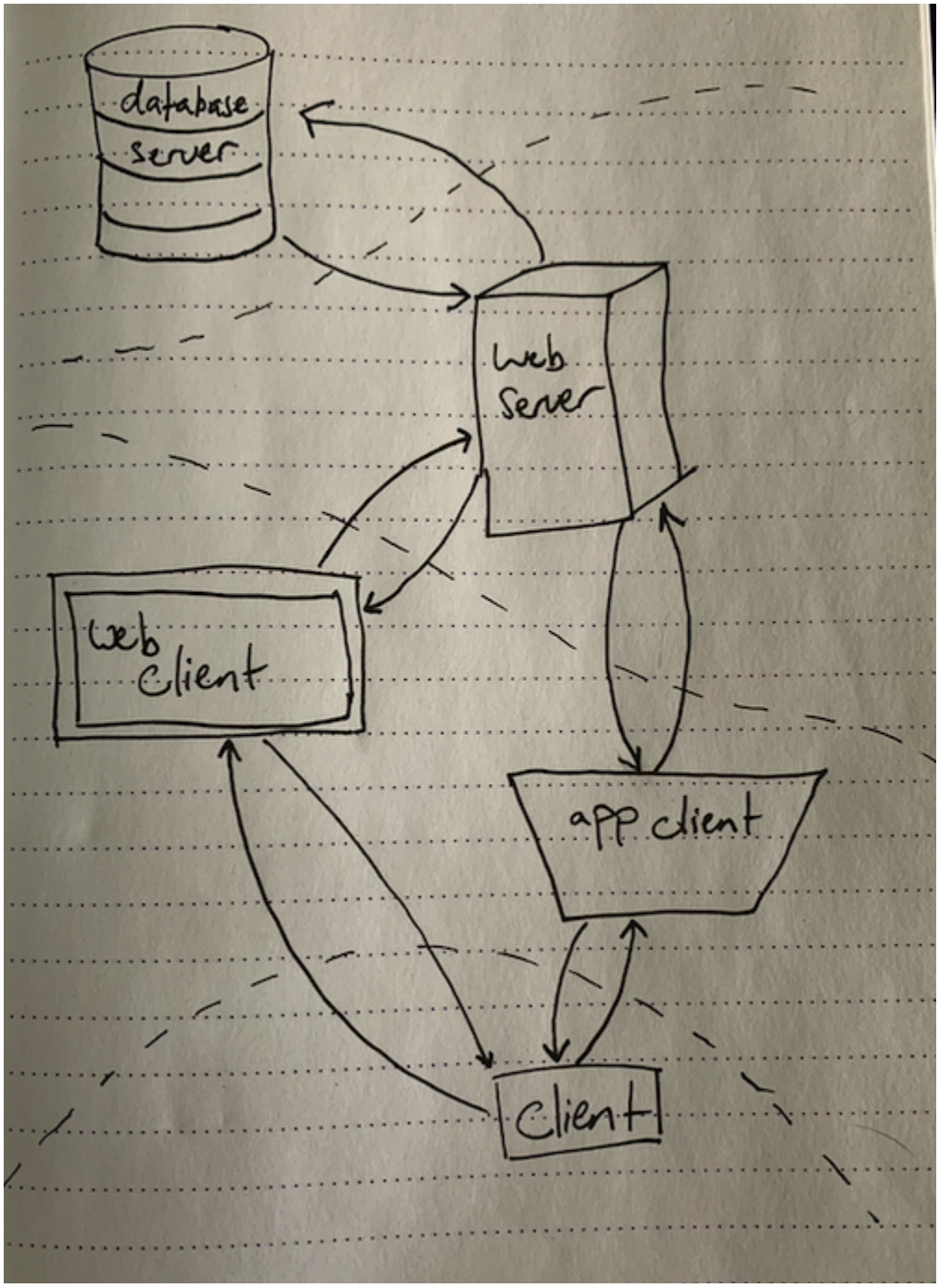
Yasmeen Awad



Threats + Mitigations:

Threat: attacker on client's network performs a MITM attack via ARP spoofing and modifies
Mitigation: use ARP spoofing detectors
STRIDE element: spoofing

Threat: client injects SQL when searching for lemurs which deletes all data
Mitigation: check all user-input textboxes for SQL injection, only accept text that does not contain SQL code
STRIDE element: tampering

Threat: eavesdropper listens in on client's interaction with the app client
Mitigation: all interactions occur through HTTPS
STRIDE element: information disclosure

Threat: client posts a photo of a lemur that contains some explicit content (which is against the rules), but the client claims that they did not post that photo and therefore should not be blocked from the site - they claim that someone else posted it from their account
Mitigation: with every photo post, store the location, IP, and MAC address from which the post originated. Have each user sign the transmission that sends the post info with a digital signature encrypted with their personal secret key
STRIDE element: repudiation

Threat: an attacker repeatedly sends SYN packets to the web server, overwhelming the server and causing it to crash
Mitigation: physically connect the web server only to the web client, app client, and database (through physical wires) and only accept packets from the physically connected web client, app client, and database
STRIDE element: denial of service

Threat: an attacker finds a bug which allows them to login to the app as an admin without the admin password. The attacker uses this privilege to delete all lemur data.
Mitigation: required unit testing of permissions that affirm that users can only access the privileges that they are supposed to be able to access
STRIDE element: elevation of privilege