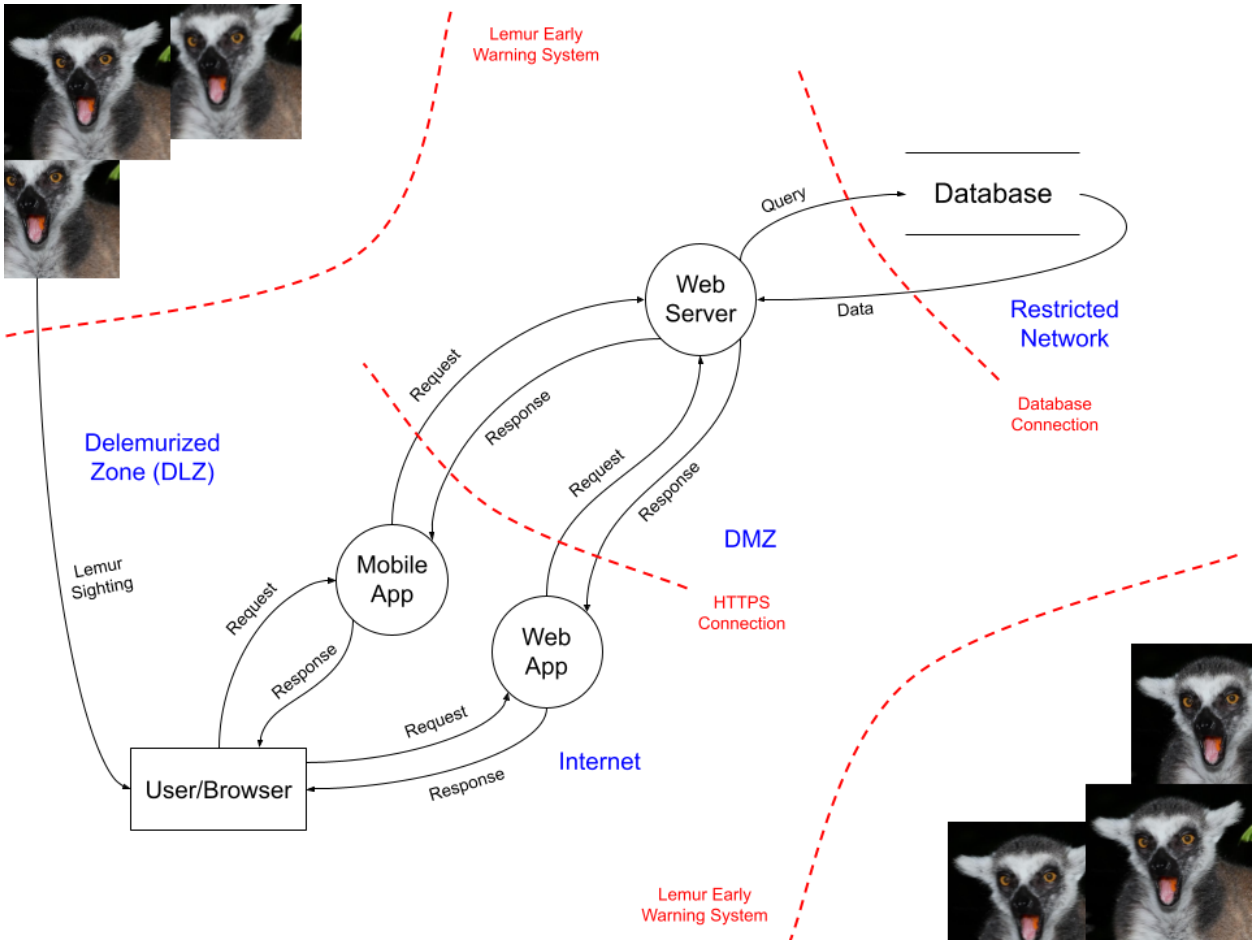
Soren DeHaan and Carl Tankersley

- Spoofing
  - Cookie Replay :: encrypt network traffic to prevent cookies from being intercepted by a MITM and use shorter-term cookies so that an attacker can't have access indefinitely if they get a hold of a user's cookies
  - Session Hijacking
  - CSRF :: logic-structure dependent, check edge cases?
  - MITM :: require all traffic to use HTTPS
  - ARP spoofing :: require all traffic to use HTTPS
  - IP spoofing :: use IPv6, check outgoing packet source addresses
  - DNS spoofing
- Tampering
  - XSS :: logic-structure dependent, check edge cases?
  - SQL Injection :: treat user input as data rather than code using prepared statements
- Repudiation
  - Audit Log Deletion :: backup logs off network
  - Insecure Backup :: keep backups on a separate machine so that compromising the original logs does not grant access to the backups
  - Claims to not have received :: logging, third party verification
- Information Disclosure
  - Eavesdropping :: encrypt network traffic
  - Get data from logs/temp files :: encrypt log data
  - Verbose exception :: give the user as little information as possible about exceptions to prevent them from learning about the structure of the code
- Denial of Service
  - SYN Flood :: "blackhole" incoming data, get excess bandwidth, temporarily route to dedicated anti-DDoS service
  - Rampaging Lemur Attack (RLA) :: Lemur sirens, early watch system, anti-lemur personal defense trainings
- Elevation of Privilege
  - Logic Flow Attacks :: logic-structure dependent, check edge cases
  - Sends inputs the code doesn't handle properly :: logic-structure dependent, check edge cases


Lemur Early
Warning System
Database
Query
Web
Server
Data
Restricted
Network
Database
Connection
Request
Response
Request
Response
Delemurized
Zone (DLZ)
DMZ
Lemur
Sighting
Mobile
App
Request
Response
Web
App
HTTPS
Connection
Request
Response
User/Browser
Internet
Lemur Early
Warning System