Armira Nance
CS 338: Computer Security
Prof. Jeff Ondich

Security Vulnerabilities in the Tapirs Unlimited Framework (STRIDE)

I. Spoofing (affects Authenticity)

Spoofing is a vulnerability that exists in the Tapirs Unlimited Framework (TUF), most notably in the relationship between the web server and the database server. Because the web server listens for HTTP connections, the added layer of security that we would have with HTTPS is gone. That means that it's easier to create a fake version of the website where users might be tricked into entering their login credentials.

This could be remedied by solely using HTTP connections on the web server.

II. Tampering (violates Integrity)

The database server is also compromised by the use of HTTP, because it is easy for attackers to modify database queries and alter information transmitted between the database and web servers.

This would also be resolved by using HTTPS.

III. Repudiation (violates Non-Repudiability)

The communication between the web client and web server is vulnerable to an Adversary-in-the-Middle attack, as it's easy for an intruder to gain access to and alter information without either party knowing that the communication has been compromised.

There are many solutions to this problem, one of which is to publish the certificate users should expect to see if they've reached the correct destination.

IV. Information Disclosure (violates Confidentiality)

The line of communication between the client apps and the database server is vulnerable to a SQL Injection attack, because intruders are able to send SQL queries to the database server and gain access to sensitive information.

The solution to this is to validate any input coming from the client apps to the database server.

V. Denial-of-Service (affects Availability)

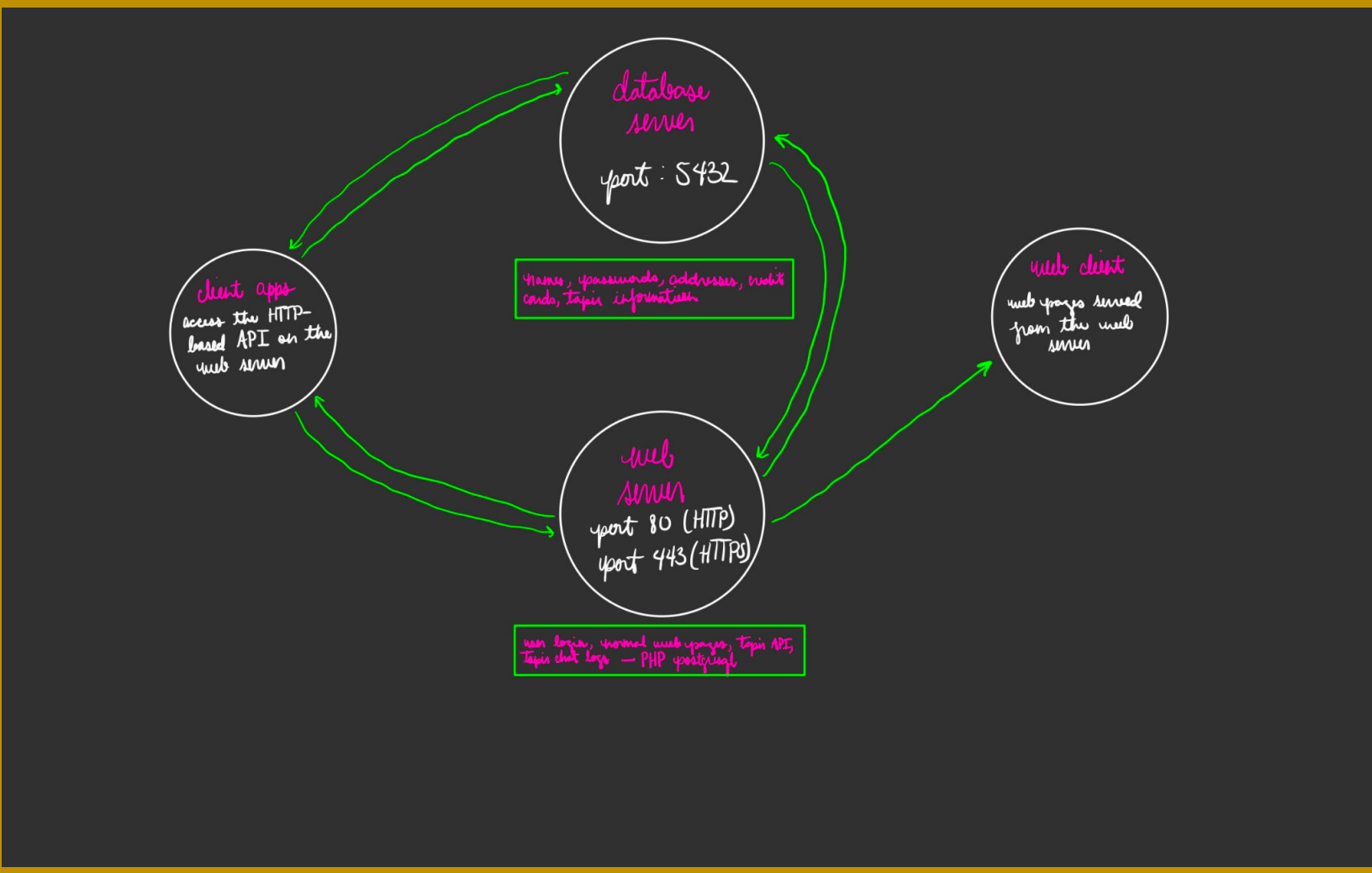
Denial-of-Service attacks put the web client at risk, because it makes the webpage unavailable and inaccessible for a period of time.

A way to mitigate that risk is to implement traffic management strategies to ensure that the web server can detect sudden changes in traffic, strange patterns, and malicious data requests.

VI. Elevation of Privilege (violates Authorization)

Attackers can use buffer overflow vulnerabilities in client apps to gain higher levels of access than they should have.

The solution to this is to set character limits for input and use programming languages that don't allow direct access to memory (i.e. do not use C – like, ever).


database server
port : 5432
names, passwords, addresses, credit cards, tapir information
client apps
access the HTTP-based API on the web server
web client
web pages served from the web server
web server
port 80 (HTTP)
port 443 (HTTPS)
user login, normal web pages, tapir API, tapir chat logs — PHP postgres