NAVIGATING WEB SESSIONS

A Beginner's Guide

Presented by: Anukasha Singh

ABOUT ME

Hi, I’m Anukasha!

Working as a Senior Software Engineer in miniOrange.
Been in the world of Cyber Security for 4 years now.

Dealt with a lot of session issues :)

I HAVE AN E-COMMERCE SITE

AND WANT TO ALLOW USERS TO LOGIN BEFORE PURCHASING.

I have implemented the following:

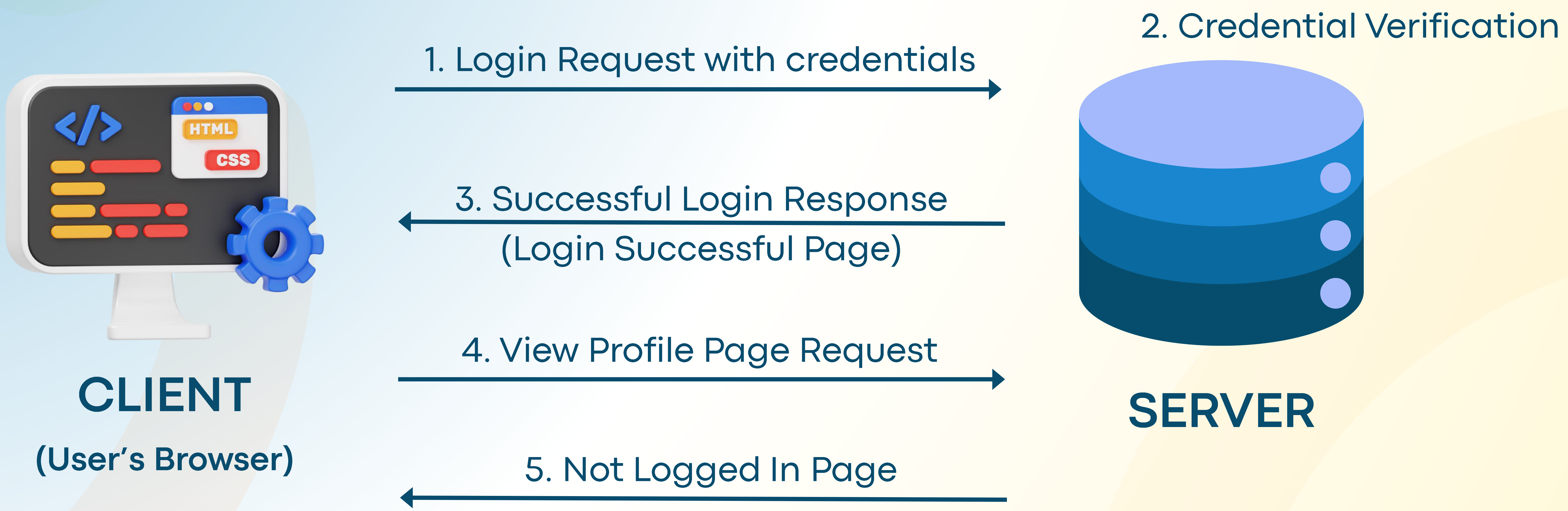
- A login page that asks the user for his credentials.
- Verification of these credentials from the database.

THE CHALLENGE

✕ ✓

STORING THE USER'S STATE
How to check with every subsequent request that the user is logged-in?

THE PROBLEM



1. Login Request with credentials

2. Credential Verification

3. Successful Login Response (Login Successful Page)

4. View Profile Page Request

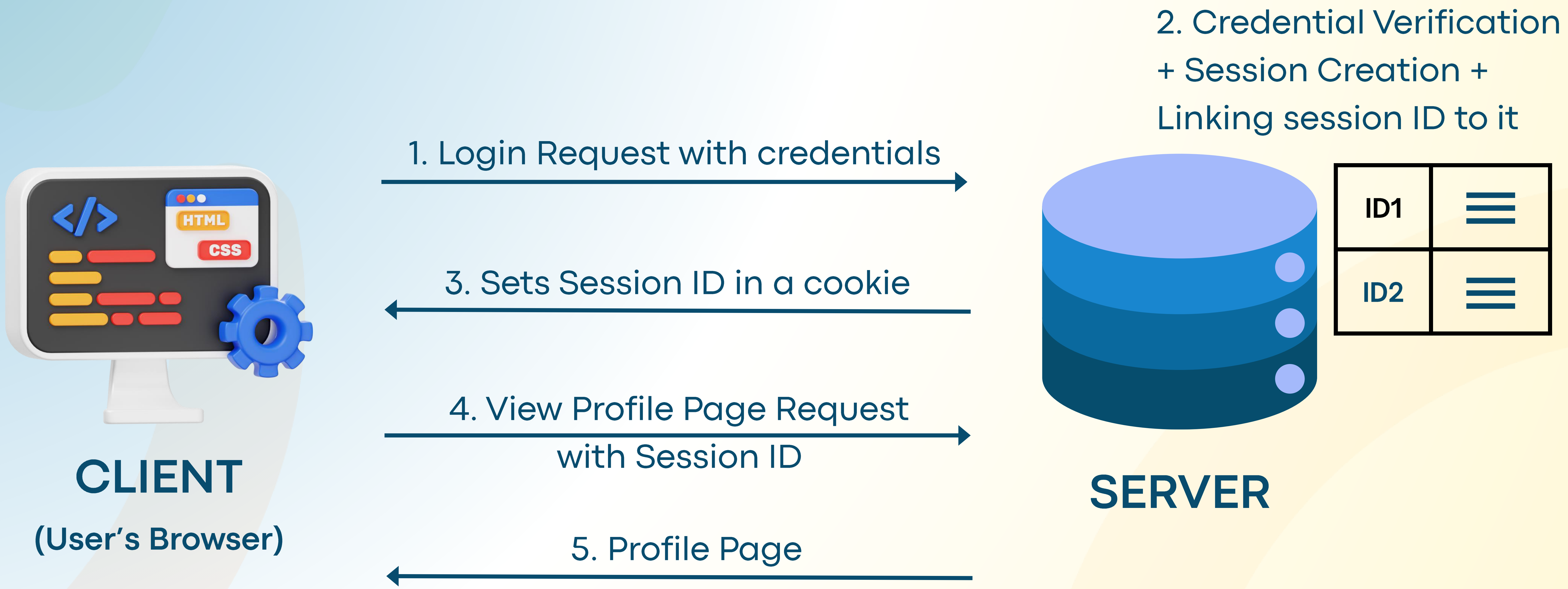
5. Not Logged In Page

CLIENT

(User's Browser)

SERVER

WEB SESSIONS TO THE RESCUE!



CLIENT

(User's Browser)

SERVER

1. Login Request with credentials

2. Credential Verification + Session Creation + Linking session ID to it

3. Sets Session ID in a cookie

4. View Profile Page Request with Session ID

5. Profile Page

WEB SESSIONS

Why sessions?

- *Secure*
- *Control via session management*

What are Web Sessions?

- *Server-side Temporary Information*
- *A **session ID** is associated with this information for identification*
- *This session ID is stored on the client side for subsequent requests*

HOW DO WEB APPLICATIONS UTILIZE WEB SESSIONS?

Pre-authentication

- User Language Preference
- Shopping Cart Information

many more

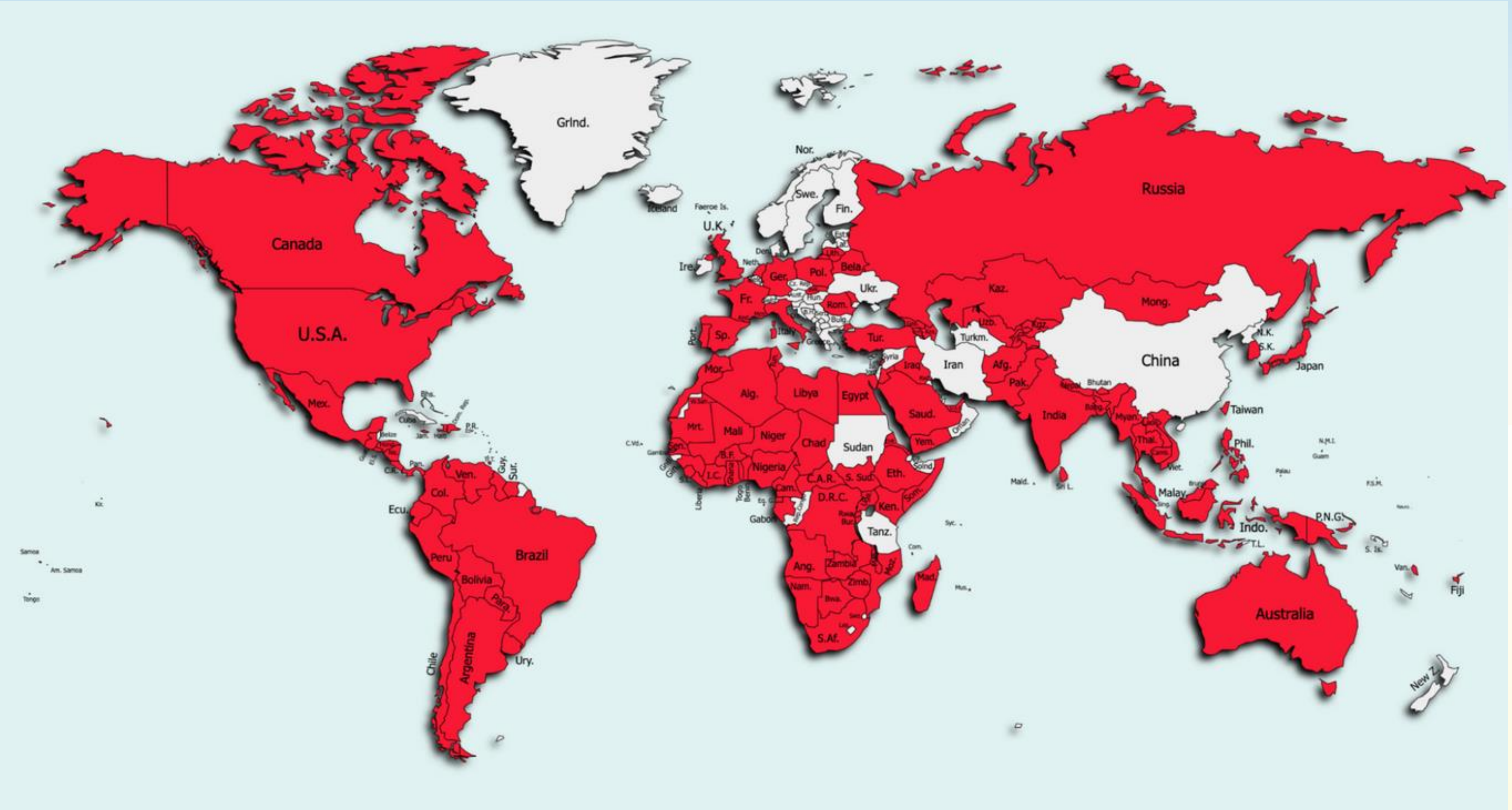
Post-authentication

Storing the user's state and other relevant information for a user who is logged-in to the site.

FACEBOOK SESSION HIJACKING

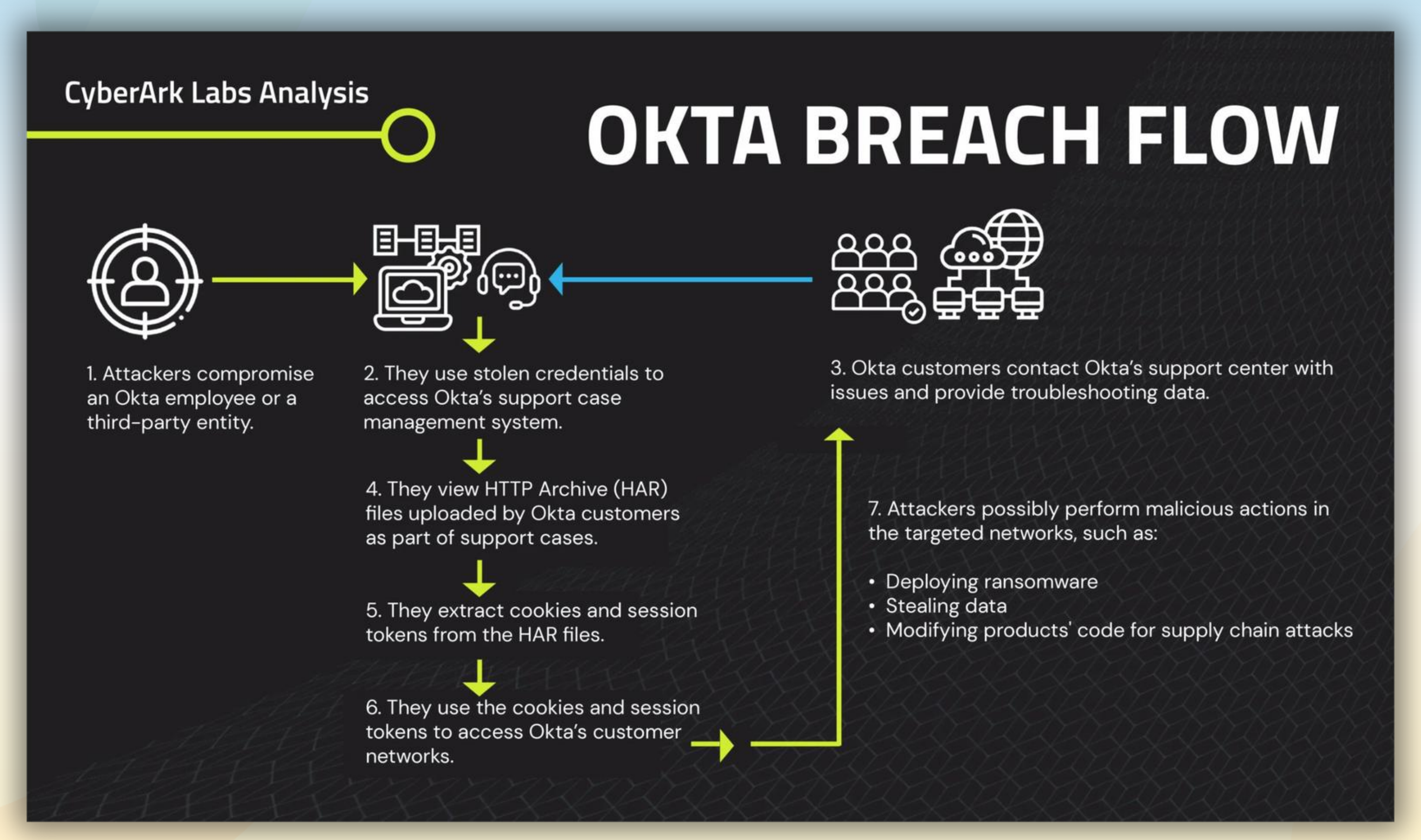
In 2021, Facebook took a massive hit due to session hijacking vulnerability via an android Trojan named Flytrap. The worst part was that it spread across 140 countries. It primarily attacked the user's social profile by hijacking Facebook ID, IP address, cookies and tokens, location, and email addresses.

Reference:
https://www.zimperium.com/blog/flytrap-android-malware-compromises-thousands-of-facebook-accounts/



🟧 Countries Exposed to Facebook Hijacking Vulnerability in 2021

OKTA'S SUPPORT SYSTEM BREACH



CyberArk Labs Analysis

OKTA BREACH FLOW

1. Attackers compromise an Okta employee or a third-party entity.

2. They use stolen credentials to access Okta's support case management system.

3. Okta customers contact Okta's support center with issues and provide troubleshooting data.

4. They view HTTP Archive (HAR) files uploaded by Okta customers as part of support cases.

5. They extract cookies and session tokens from the HAR files.

6. They use the cookies and session tokens to access Okta's customer networks.

7. Attackers possibly perform malicious actions in the targeted networks, such as:

- Deploying ransomware
- Stealing data
- Modifying products' code for supply chain attacks

Three of those affected include 1Password, BeyondTrust, and Cloudflare. 1Password was the first company to report suspicious activity on September 29, 2023.

Reference: https://www.cyberark.com/resources/blog/piecing-together-the-attack-on-oktas-support-unit

SESSION EXPLOITATION

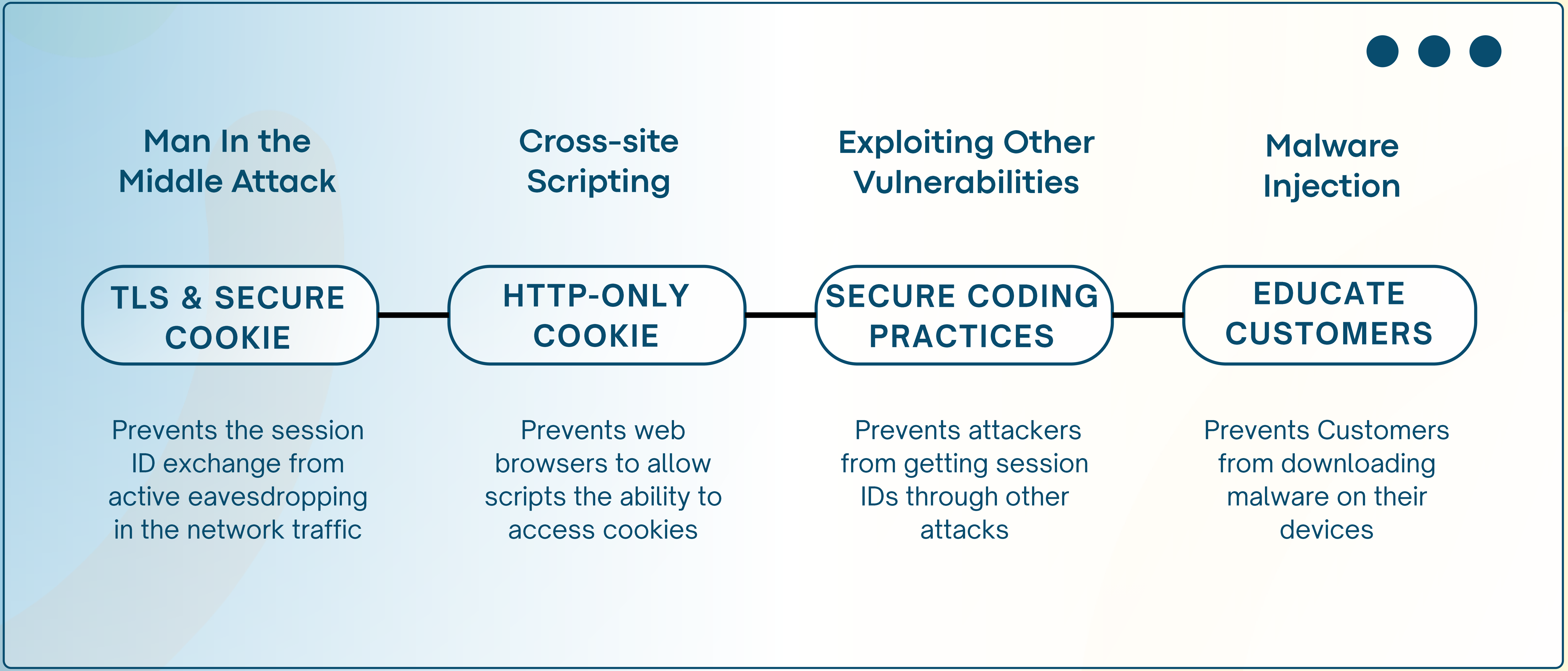
- Brute Force
- Predict / Calculate
- Steal

SESSION ID

Pass The Cookie Technique

SESSION HIJACKING

COMMON SESSION HIJACKING TECHNIQUES AND THEIR MITIGATION



Man In the Middle Attack	Cross-site Scripting	Exploiting Other Vulnerabilities	Malware Injection
TLS & SECURE COOKIE	HTTP-ONLY COOKIE	SECURE CODING PRACTICES	EDUCATE CUSTOMERS
Prevents the session ID exchange from active eavesdropping in the network traffic	Prevents web browsers to allow scripts the ability to access cookies	Prevents attackers from getting session IDs through other attacks	Prevents Customers from downloading malware on their devices

DEVELOPING A SESSION SECURE WEB APPLICATION

WHAT IF SESSION ID IS OBTAINED?

PROPER SESSION EXPIRATION

Implement Automatic and Manual Session Expiry

BINDING SESSION ID TO OTHER USER PROPERTIES

To detect user misbehavior, the session ID can be bound with client IP address, User-Agent, or client-based digital certificate

SESSION ATTACKS DETECTION

Detect multiple sequential requests from a single (or set of) IP address(es) and block them

KEY TAKEAWAYS

RECAP

1. What are Sessions?
2. Use of Sessions in Applications
3. Session Lifecycle
4. Session Exploitation
5. How to develop a Session Secure Web Application?

- Secure, HTTP-Only, and SameSite Strict Cookies
- Bind Session ID to other properties
- Proper Session Expiry
- Session Attacks Detection
- Secure Coding Practices + Vulnerability Detection
- Educate your customers

THANK YOU

Presented by: Anukasha Singh