Introductory Lesson

Understanding http: the postcard problem

Browser sends info like a postcard that anyone can read

Hackers use tools like burp suite to See or change info

https enforces security making sealed envelopes

Defensive http response headers

Sites like twitter add special rules like only open certain file types or only open within current site

Stay within the platform (no redirecting) because the environment is controlled by the platform keeping users safer

Login pages: bank vault door

Hackers can try endless passwords (brute force)

Guess usernames

Steal session tokens and log in as you

Access controls across layers

UI – hide delete user buttons from regular staff

Code – check If user is actually admin before executing commands

Database – ensure users only see their own data

What is XSS (cross site scripting)

Website unknowingly delivers malicious code to users

How apps block XSS

Output encoding: emojis and symbols etc turn to code to show but code wont run

Avoid raw user data in scripts

Sanitization removes harmful code

CSRF

Website can’t tell real requests from forged ones so it accepts both

Session tokens used to mask as you

Defences to CSRF

Anti-CSRF tokens are secret codes in each request

X frame options are used so no one can frame checkout pages

Critical questions like are you sure are prompted

Cryptography

SQL injection