Security

i. Authentication.
ii. Authorization.

Tools are available to check code level security vulnerabilities.
examples : hard coded credentials exposed, techstack used, vulnerable versions of frameworks used.
Basically anything that is TMI to the end users.

Once a user is authenticated and authorized, they have access to whatever they are authorized to access.

Server side scripting attack. Attaching script to other files like .png. and when the server tries to regenerate the file, the attached script runs.

Authentication using - OAuth, JWT

Zero Trust : Trust no one. authenticate every request.