RL4Eng

Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Omar Mohamed

Web Security

Co-funded by the Erasmus+ Programme of the European Union

INTRODUCTION

Web security involves protecting websites, servers, and data from unauthorized access and breaches.

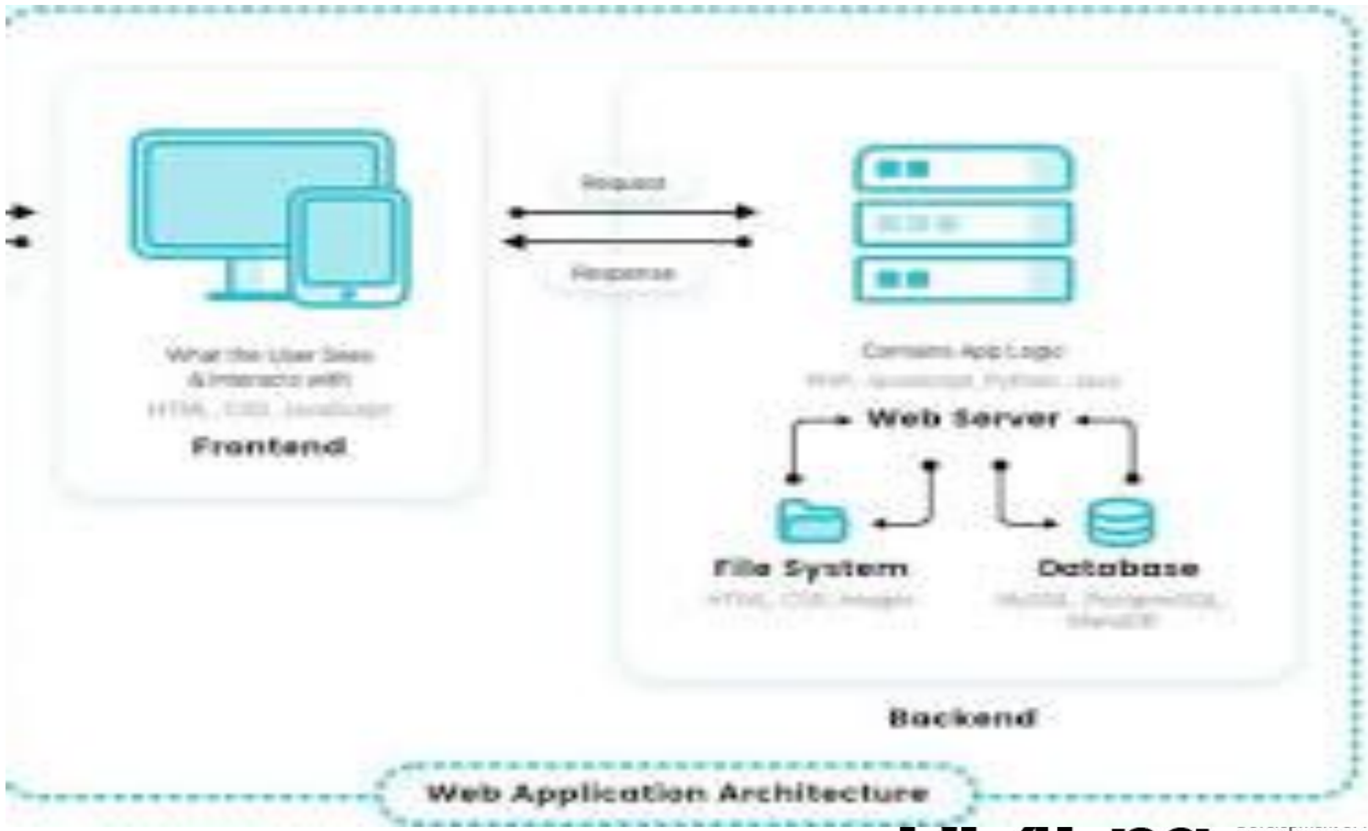
Key Concepts Covered in this presentation:

1. Web Architecture
2. Web Servers: Apache and Nginx
3. HTTP Protocol
4. Cookies
5. HTTP Requests and Responses

RL4Eng Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union

Web Architecture



RL4Eng
emote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union

Web Architecture

- Client: User's device (computer, smartphone, tablet)
- Browser: Software to interpret and display web pages (Chrome, Firefox, Safari)
- Server: Computer that stores and serves web content
- Web Server: Software on the server that handles requests and sends responses (Apache, Nginx)

RL4Eng Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union

WEB SEVERS

- A web server is software or hardware that serves web content.
- Apache:
  - Open-source, widely used
  - Highly configurable
  - Supports various modules for security, performance, and more
- Nginx:
  - High-performance, efficient
  - Often used as a reverse proxy or load balancer
  - Strong security features

HTTP Protocols

- HTTP (HyperText Transfer Protocol): Foundation of web communication.
    - Common HTTP Methods:
    - GET: Retrieve data.
    - POST: Submit data.
    - PUT: Update data.
    - DELETE: Remove data.
- HTTPS: Secure version of HTTP using SSL/TLS encryption.
- Importance:
    - Prevents data interception.
    - Ensures data integrity and authenticity

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union

COOKIES

- Cookies are small text files stored on the client-side by websites.
- Types:
    - Session Cookies: Temporary, deleted after the session ends.
    - Persistent Cookies: Stored until a specified expiration date.
- Usage:
    - Session management (e.g., logins).
    - Personalization (e.g., themes).
    - Tracking user behavior.
- Security:
    - Use HTTP-Only and Secure flags.
    - Regularly validate cookie content.

RL4Eng Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union

HTTP Requests and Responses

- HTTP Request Structure:
  1. Request Line: Method, URL, and HTTP version.
  2. Headers: Metadata (e.g., User-Agent, Content-Type).
  3. Body: Data sent to the server (e.g., form submissions).
- HTTP Response Structure:
  1. Status Line: HTTP version and status code (e.g., 200, 404).
  2. Headers: Metadata (e.g., Content-Type).
  3. Body: Content returned to the client.
- Common Status Codes:
  1. 200 OK: Request succeeded.
  2. 404 Not Found: Resource not found.
  3. 500 Internal Server Error: Server-side issue

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union

Security Implications

- Common Vulnerabilities:
  - Unsecured cookies.
  - Improper server configurations.
  - Open redirects.
- - Best Practices:
  - Use HTTPS to encrypt communications.
  - Sanitize and validate all inputs.
  - Configure secure HTTP headers (e.g., Content-Security-Policy).

RL4Eng Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union

Tools for Securing Web Basics

- Web Application Firewalls (WAFs): Protect against common threats.
- SSL/TLS Certificates: Secure web communications.
- Vulnerability Scanners: Detect potential flaws in web applications.
- Logging and Monitoring Tools: Track and respond to anomalies.

RL4Eng
Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions
Co-funded by the Erasmus+ Programme of the European Union

Q &A

RL4Eng Development of Remote and Virtual Laboratories for Teaching and Training Engineering Students in the South Mediterranean and Sub-Saharan Higher Education Institutions

Co-funded by the Erasmus+ Programme of the European Union