MENTORING PROGRAM

Web Server

2024

/* Where there is a shell, there is a way*/

Table of contents

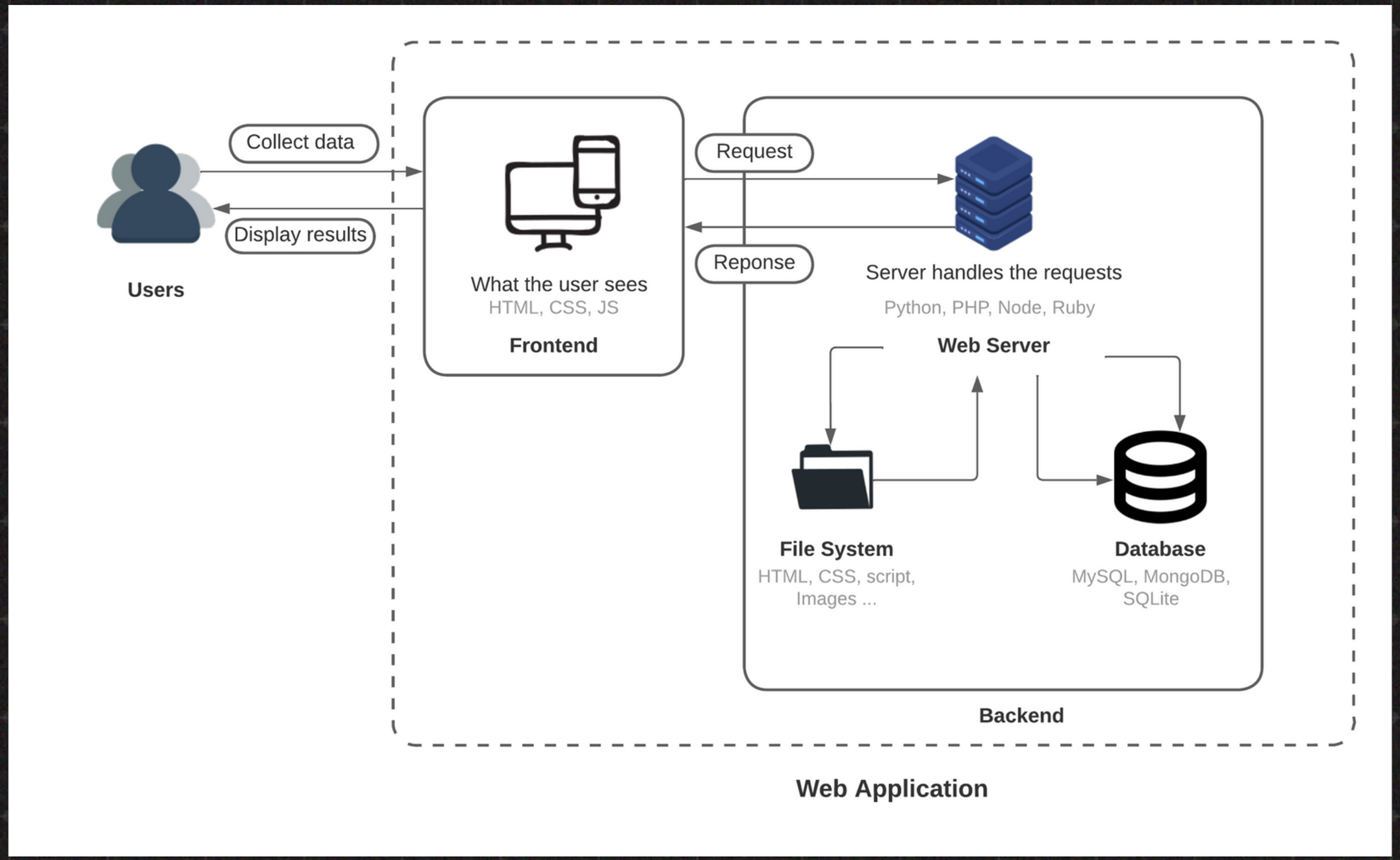
/* Where there is a shell, there is a way*/

Shellmates

Defnitions

/* Where there is a shell, there is a way*/

Web Applications Architecure



HTTP

HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message.

HTTP - Methods

- GET: **Retrieve document identified by URL**
  - GET https://school.com/students/12588
- POST:**Give information to server**
  - POST https://school.com/student/mark
    {“Student”: 123,“Mark”: 14}
- PUT: **Store document identified by URL**
  - POST https://school.com/student
    {“Name”: “Mokrane”}
- Delete: **Delete Document identified by URL**
  - DELETE https://school.com/student/1255

HTTP - Headers

HTTP Headers: Pass additional information between client and server

- Host
- User agent
- Content type
- Cookies

HTTP - Status Code

- 1xx: **Informational responses**
  - 102 Processing
- 2xx: **Successful responses**
  - 200 OK
- 3xx: **Redirection messages**
  - 301 Moved Permanently
- 4xx: **Client error responses**
  - 401 Unauthorized
- 5xx: **Server error responses**
  - 500 Internal Server Error

Shellmates

LFI

/* Where there is a shell, there is a way*/

LFI

Local File Inclusion is an attack technique in which attackers trick a web application into exposing files on a web server.

Shellmates

Command injection

/* Where there is a shell, there is a way*/

Command Injection

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.

Shellmates

SQLI

/* Where there is a shell, there is a way*/

Relational database

A relational database is a type of database that stores and provides access to data points that are related to one another.

SQL

Structured query language (SQL) is a programming language for storing and processing information in a relational database.

SQL

```sql

-- create
CREATE TABLE characters (
  character_id INTEGER PRIMARY KEY,
  name TEXT NOT NULL,
  appeared_in TEXT NOT NULL
);

-- insert
INSERT INTO characters VALUES (0001, 'Edward Elric', 'Fullmetal Alchemist');
INSERT INTO characters VALUES (0002, 'Edward Norton', 'Fight Club');
INSERT INTO characters VALUES (0003, 'Severus Snape', 'Harry Potter');

-- fetch
SELECT * FROM characters;
```

STDIN

Input for the program (Optional)

Output:

```
+--------------+---------------+----------------------+
| character_id | name          | appeared_in          |
+--------------+---------------+----------------------+
|            1 | Edward Elric  | Fullmetal Alchemist |
|            2 | Edward Norton | Fight Club           |
|            3 | Severus Snape | Harry Potter         |
+--------------+---------------+----------------------+
```

SQL

```sql

-- create
CREATE TABLE characters (
  character_id INTEGER PRIMARY KEY,
  name TEXT NOT NULL,
  appeared_in TEXT NOT NULL
);

-- insert
INSERT INTO characters VALUES (0001, 'Edward Elric', 'Fullmetal Alchemist');
INSERT INTO characters VALUES (0002, 'Edward Norton', 'Fight Club');
INSERT INTO characters VALUES (0003, 'Severus Snape', 'Harry Potter');

-- fetch
SELECT * FROM characters where appeared_in='Fight CLub';


```

STDIN

Input for the program (Optional)

Output:

```
+--------------+---------------+-------------+
| character_id | name          | appeared_in |
+--------------+---------------+-------------+
|            2 | Edward Norton | Fight Club  |
+--------------+---------------+-------------+
```

SQLI

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

Shellmates

SSTI

/* Where there is a shell, there is a way*/

Template Engines

Template engines are used when you want to rapidly build web applications that are split into different components. Templates also enable fast rendering of the server-side data that needs to be passed to the application.

SSTI

Server-side template injection is when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side.

Shellmates

Resources

/* Where there is a shell, there is a way*/

Other Vulnerabilities

- GraphQL injection
- XXE
- Xpath injection
- RFI
- Insecure Deserialization
- Ldap injection
- NoSQL injection
- Insecure File Upload
- SSRF
- Type juggling

Resources

1- Platforms: PicoCTF, Rootme, Over The Wire: natas

2- Channels: LiveOverFlow, PWN function

3- Websites: Hacktricks, PortSwigger, OWASP

4- Books: The Hacker Playbook 3 (that’s all I got)

5- Etc: @ouxs, Shellmates

Shellmates

THANK YOU

/* Where there is a shell, there is a way*/