

# **ETHICAL HACKING PLATFORM PRESENTATION(ANGULAR)**

**KAVYAA A K**

- THE COMMANDS TO RUN BEFORE STARTING ANGULAR

```
C:\Windows\System32\cmd.e  X  +  v

Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

D:\angular-project\nginx-1.27.4>nginx
|
```

```
C:\WINDOWS\system32\cmd.  X  +  v

Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

D:\angular-project\ethical-hacking>json-server --port 4500 api.json
JSON Server started on PORT :4500
Press CTRL-C to stop
Watching api.json...

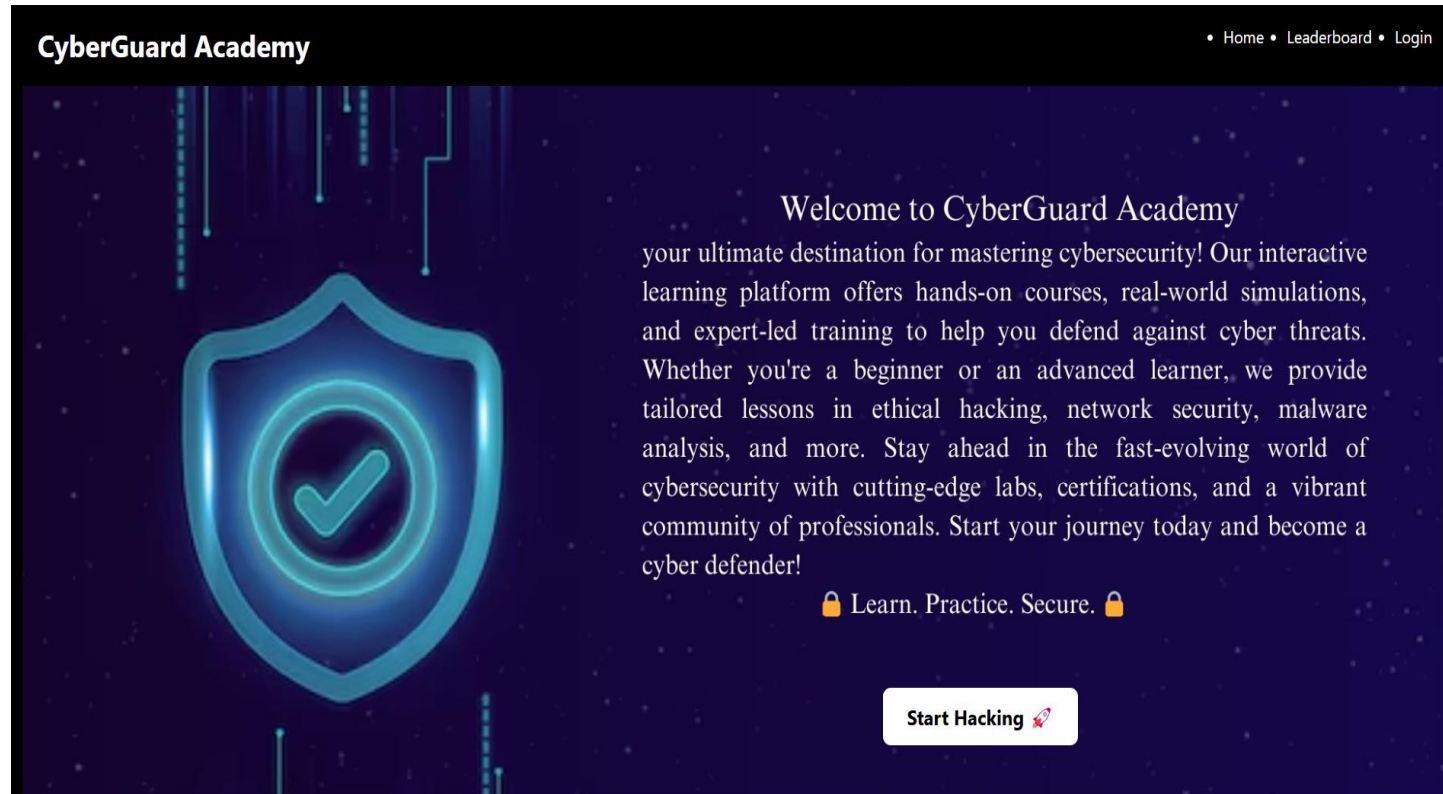
( ~^ ̣ ^~ )

Index:
http://localhost:4500/

Static files:
Serving ./public directory if it exists

Endpoints:
http://localhost:4500/challenges
|
```

# HOME PAGE



- **Built with Angular** – Ensures a dynamic, responsive, and modern UI.
- **Navigation Bar** – Includes Home, Leaderboard, and Login for easy access.
- **Visual Design** – Features a tech-themed background, security shield logo, and dark mode aesthetics.
- **Call-to-Action** – “**Start Hacking** 🚀” button encourages users to begin learning.

# CHALLENGE PAGE

This is the challenge page where it displays various challengs.

**CyberGuard Academy**

- Home
- Leaderboard
- Login

## Challenges

- **SQL Injection - Hard**

SQL Injection is a web security vulnerability that allows attackers to interfere with the queries an application makes to its database. By injecting malicious SQL code into input fields (e.g., login forms, search boxes, or URL parameters), attackers can manipulate the database to perform unauthorized actions.

[Start Challenge](#)
- **XSS Attack - Medium**

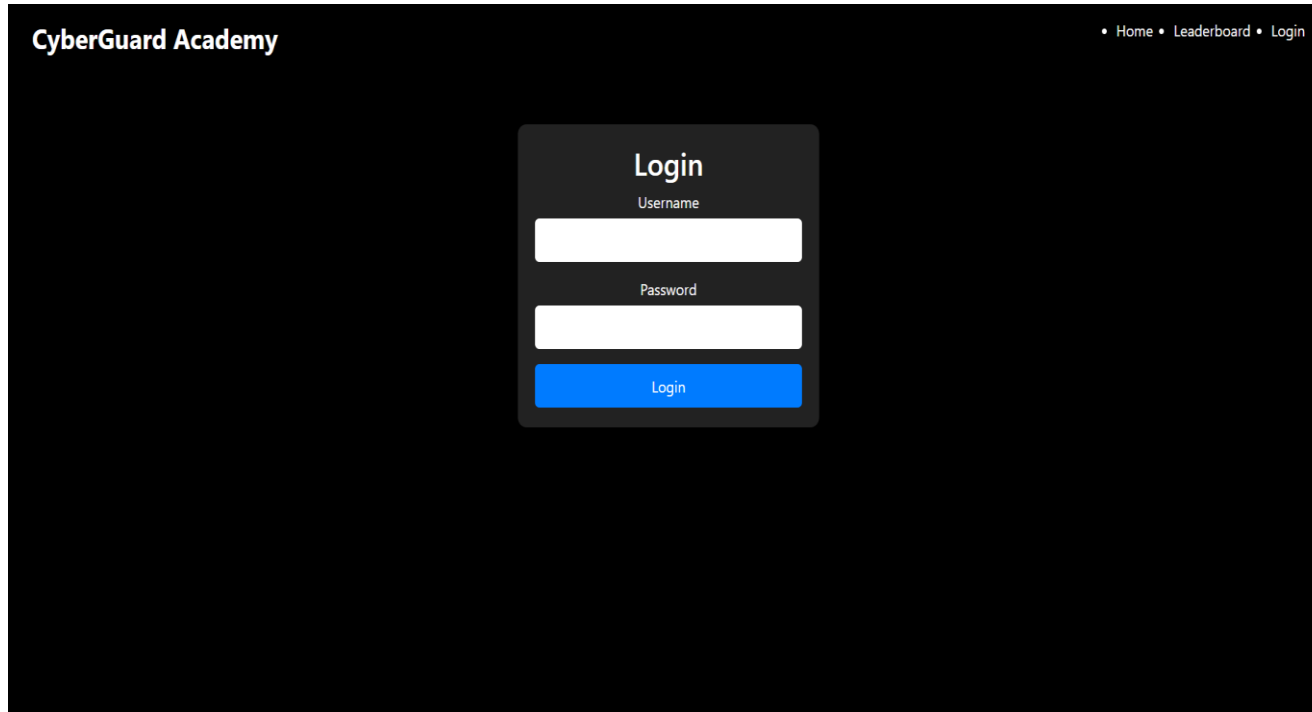
XSS is a web security vulnerability that allows attackers to inject malicious scripts (usually JavaScript) into web pages viewed by other users. This can lead to session hijacking, defacement of websites, or stealing sensitive information.

[Start Challenge](#)
- **Password Cracking - Easy**

Password cracking is the process of recovering passwords from data stored or transmitted by a system. Attackers use various techniques to guess or decrypt passwords, gaining unauthorized access to accounts or systems.

[Start Challenge](#)

# LOGIN PAGE

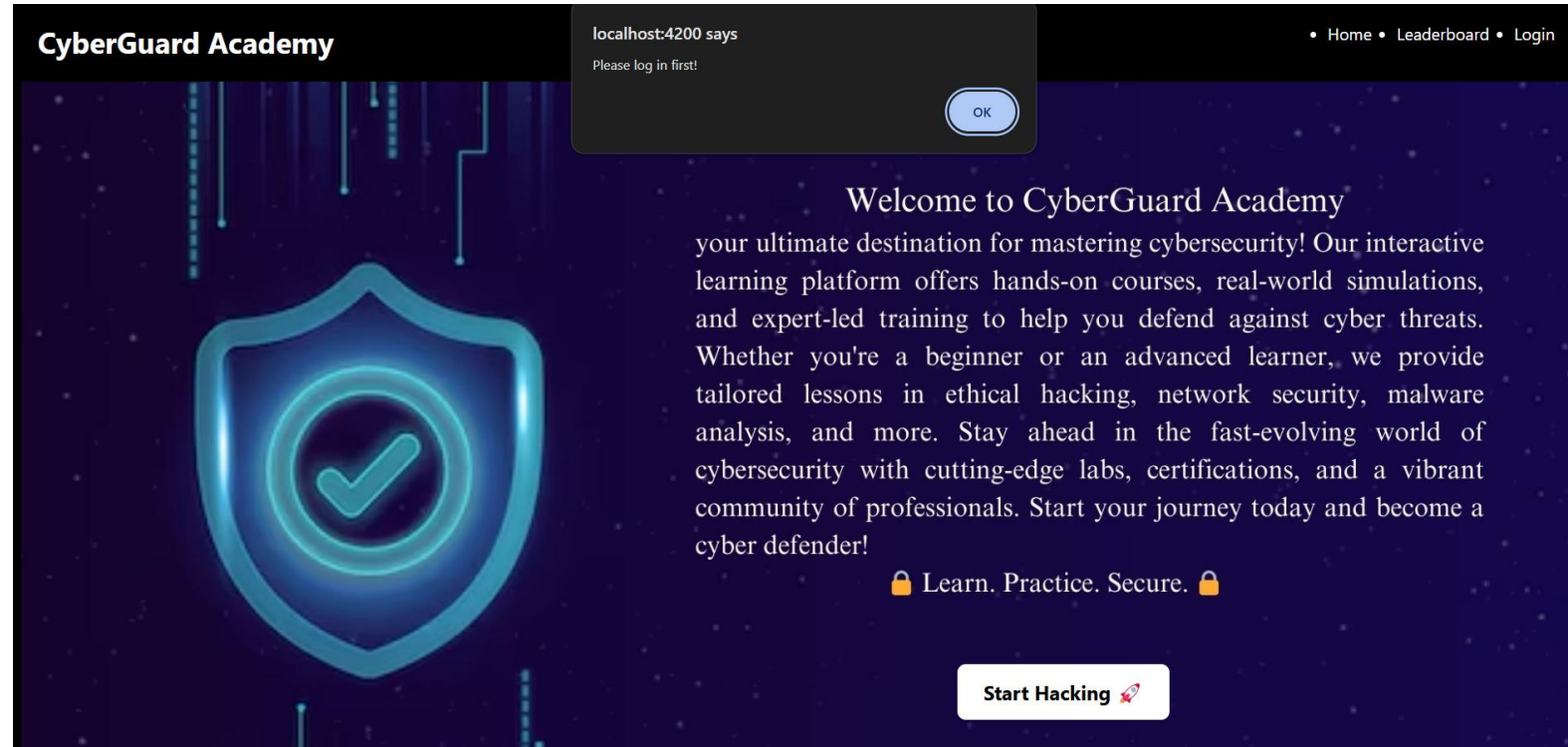


The screenshot displays a dark-themed login interface for 'CyberGuard Academy'. In the top-left corner, the text 'CyberGuard Academy' is visible. In the top-right corner, there is a navigation menu with links: '• Home • Leaderboard • Login'. The central focus is a light gray login form. At the top of this form is the word 'Login'. Below it is a label 'Username' followed by a white text input field. Underneath the username field is a label 'Password' followed by another white text input field. At the bottom of the form is a blue button with the text 'Login' in white.

- Secure login system with **username and password fields**.
- Dark-themed interface with a **clean and minimalistic login form**.
- Includes **Home, Leaderboard, and Login** for easy access.
- Ensures **restricted entry** to authorized users only.
- Provides a **responsive and dynamic** login experience.

# ALERT BOX

The alert box appears when a user tries to access the **Leaderboard** without logging in. It displays the message **"Please log in first!"**, ensuring that only authenticated users can view the leaderboard. This enhances security by restricting access to authorized users.




# LEADERBOARD PAGE

The **Leaderboard** page displays the top users based on their scores, ranking them from highest to lowest. It provides a competitive insight into user performance, motivating participants to improve their skills. Only logged-in users can access this page.

CyberGuard Academy

• Home • Leaderboard • Logout

 Leaderboard 

Rank	Username	Score
1	HackerX	9800
2	CyberNinja	8700
3	DarkWebWarrior	8500
4	RootUser	7900
5	PentestPro	7500

Once the user logs in, the **Login** button dynamically changes to **Logout**, indicating a successful authentication. This allows the user to securely log out when they have finished using the platform.