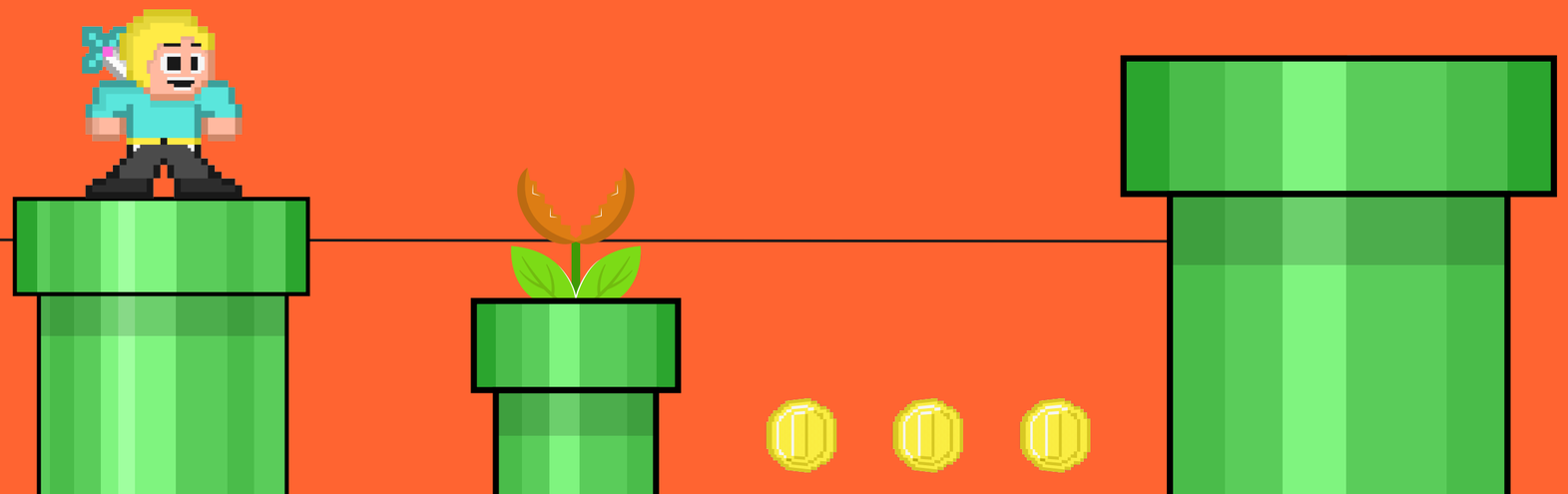
VIDEO GAME HACKING

PRESENTED BY:
SANCHAY SINGH



BSIDES MUMBAI
2024

WHOAMI

WHOAMI

A Gamer

WHOAMI

A Gamer

Game Hacker

WHOAMI

A Gamer

Game Hacker

Founder of HackersVilla Community

WHOAMI

A Gamer

Game Hacker

- Founder of HackersVilla Community
- Working with Upgrad, MakeIntern as SME

WHOAMI

A Gamer

Game Hacker

- Founder of HackersVilla Community
- Working with Upgrad, MakeIntern as SME
- Mentor at OWASP Delhi, BSides Noida

WHOAMI

A Gamer

Game Hacker

- Founder of HackersVilla Community
- Working with Upgrad, MakeIntern as SME
- Mentor at OWASP Delhi, BSides Noida
- Given Corporate Trainings at KPMG, Cognizant, etc

WHOAMI

A Gamer

Game Hacker

- Founder of HackersVilla Community
- Working with Upgrad, MakeIntern as SME
- Mentor at OWASP Delhi, BSides Noida
- Given Corporate Trainings at KPMG, Cognizant, etc
- Active Part of NULL and THM Community

BSIDES MUMBAI

MY JOURNEY

BSIDES MUMBAI

This is NOT a lecture

Please ASK questions

Share YOUR thoughts

BSIDES MUMBAI

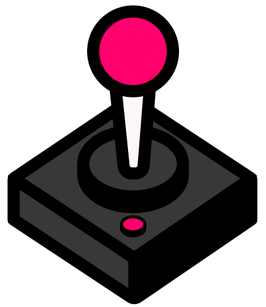
Welcome to the Game Hacking Workshop

START GAME

BSIDES MUMBAI

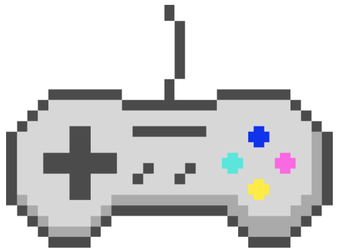
MENU

1. Understanding Video Game Architecture
2. Game Engines
3. Game Drivers
4. Binary, Executables and DLLs
4. Product Key Bypass DEMO
5. Memory Scanning & Res Hacking DEMO
6. DLL Injections
7. Wall Hacks / Aimbots DEMO
8. Valorant as a Spyware

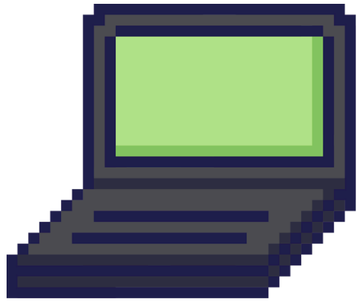


BSIDES MUMBAI

PREREQUISITES



Gamer's Instinct



Laptop to follow along

Enthusiasm & Curiosity


BSIDES
MUMBAI


BSIDES
MUMBAI

BSIDES MUMBAI

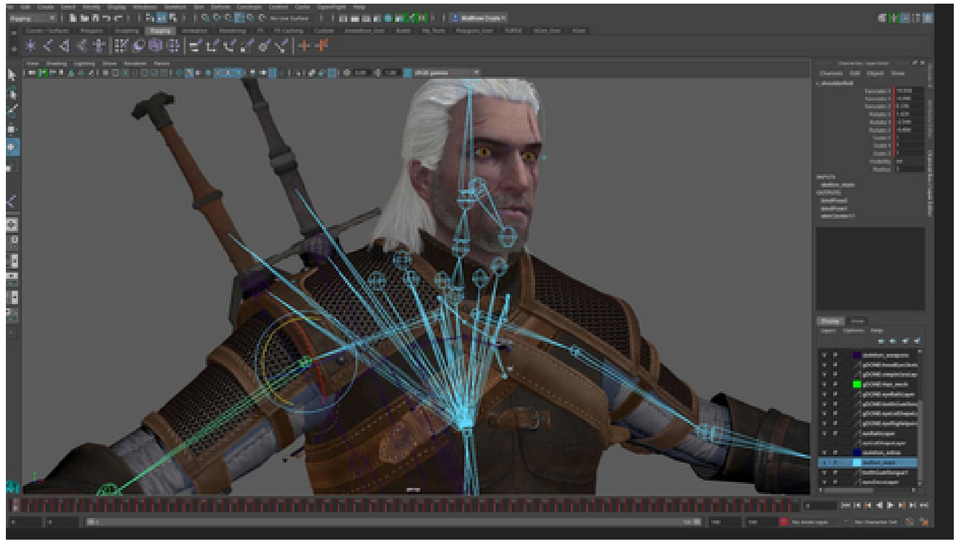
VIDEO GAME ARCHITECTURE

BSIDES MUMBAI

STAGES OF DEVELOPMENT

Design Phase

- Involves conceptualizing game mechanics, characters, and overall gameplay.
- Design decisions impact the security architecture, considering factors such as data flow and user interactions.

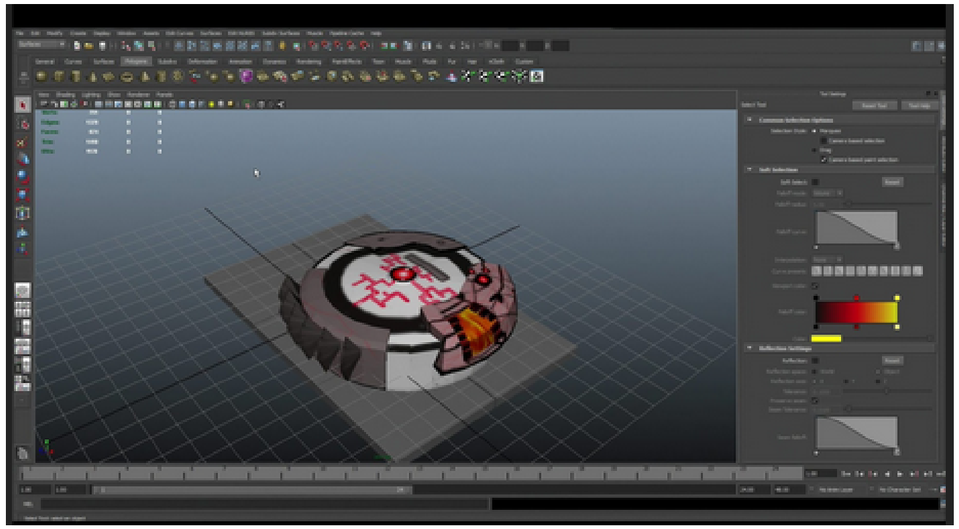


BSIDES MUMBAI

STAGES OF DEVELOPMENT

Programming Phase

- Developers write the code based on the design specifications
- Security considerations at this stage involve secure coding practices to mitigate vulnerabilities

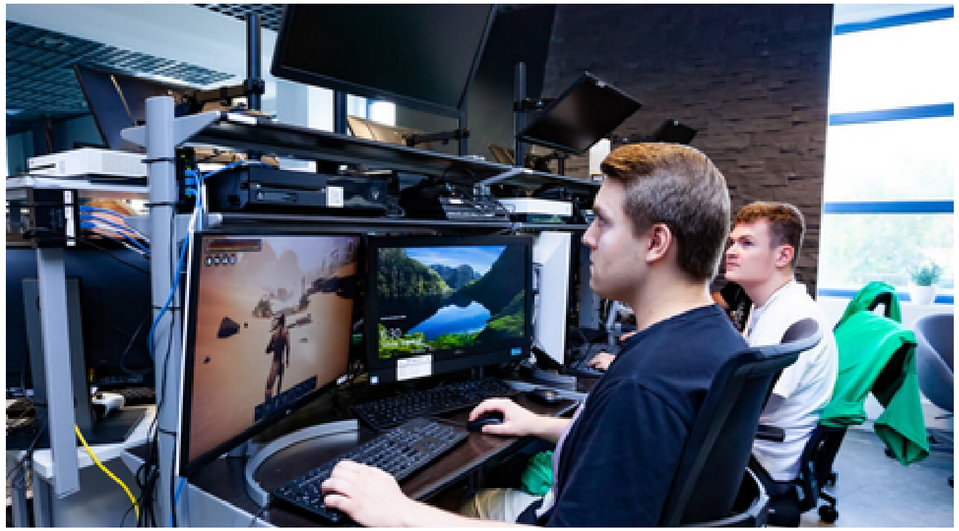


BSIDES MUMBAI

STAGES OF DEVELOPMENT

Testing and QA

- Rigorous testing to identify and fix bugs and security vulnerabilities
- Security testing ensures that the game is resilient against common threats



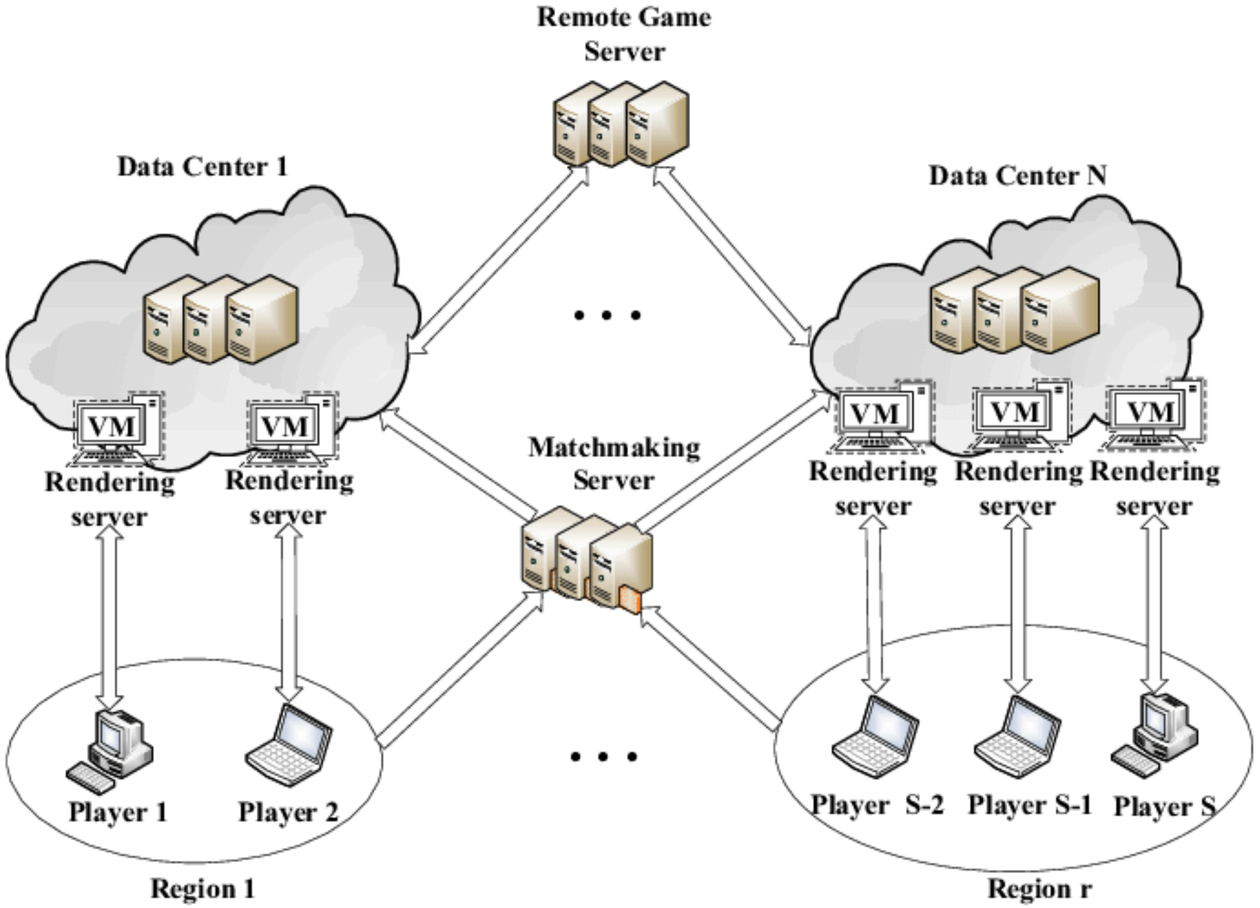
BSIDES MUMBAI

STAGES OF DEVELOPMENT

Deployment

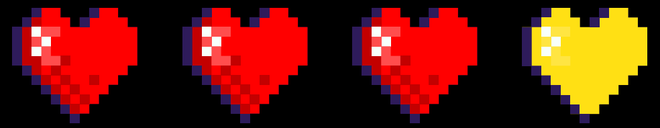
- The game is released to the public or a specific audience
- Security measures during deployment include securing servers, data transmission, and user authentication.

CLIENT-SERVER MODEL



BSIDES MUMBAI

LEVEL UP



LIFE 1 UP


BSIDES
MUMBAI

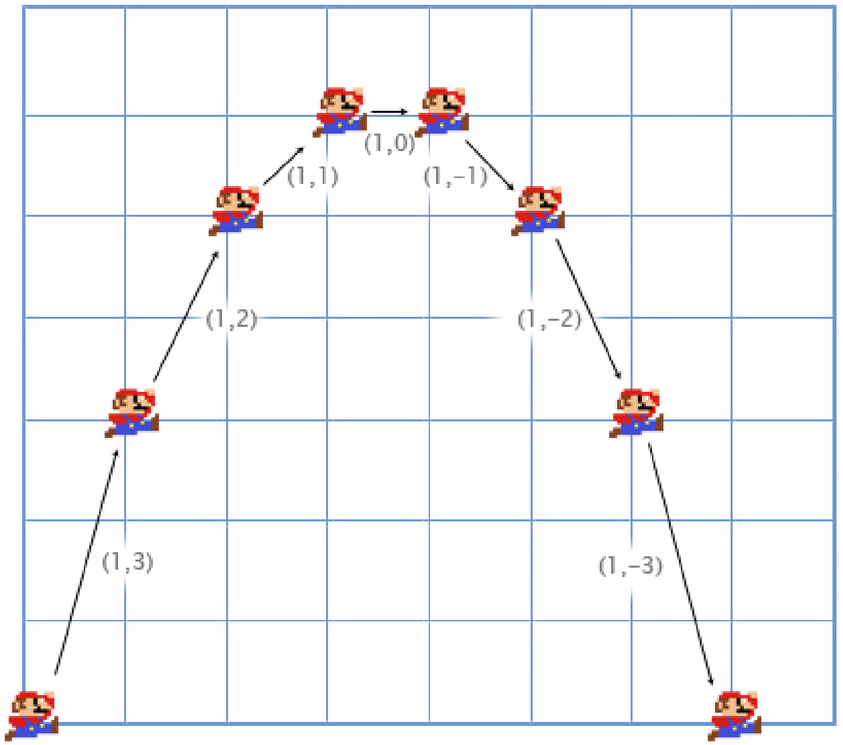

BSIDES
MUMBAI

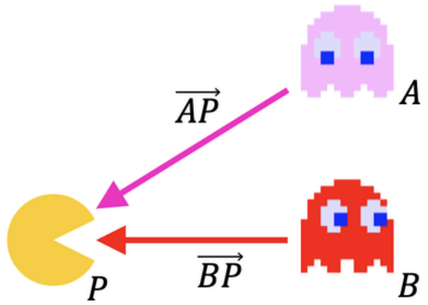
BSIDES MUMBAI

GAME ENGINES

BSIDES MUMBAI

MATH ENGINE





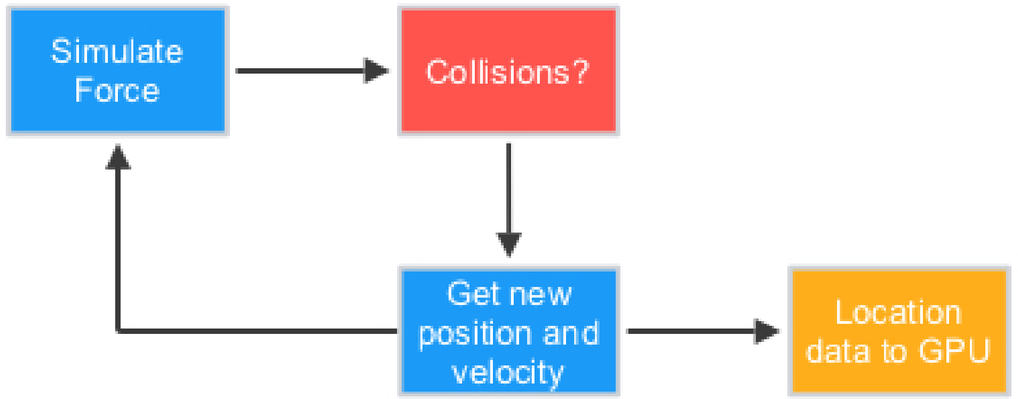
$$\|\overrightarrow{AP}\| = \sqrt{\overrightarrow{AP_x}^2 + \overrightarrow{AP_y}^2}$$

$$\|\overrightarrow{BP}\| = \sqrt{\overrightarrow{BP_x}^2 + \overrightarrow{BP_y}^2}$$

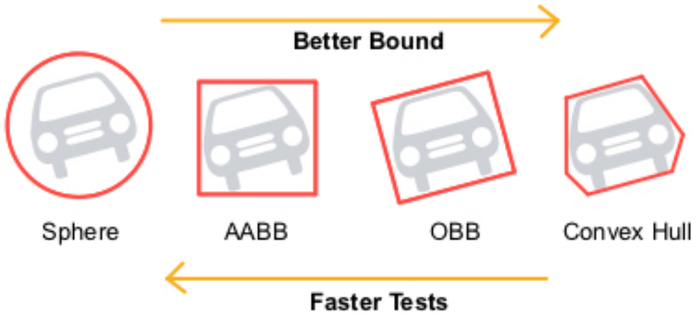
BSIDES MUMBAI

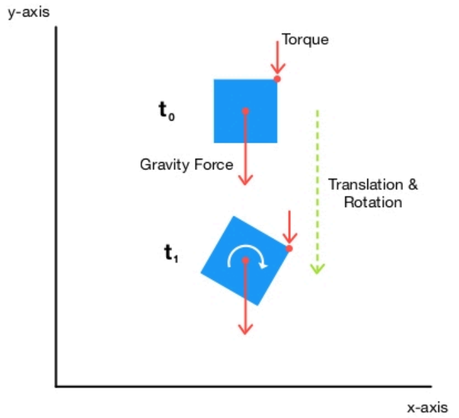
PHYSICS ENGINE

Physics Engine Loop



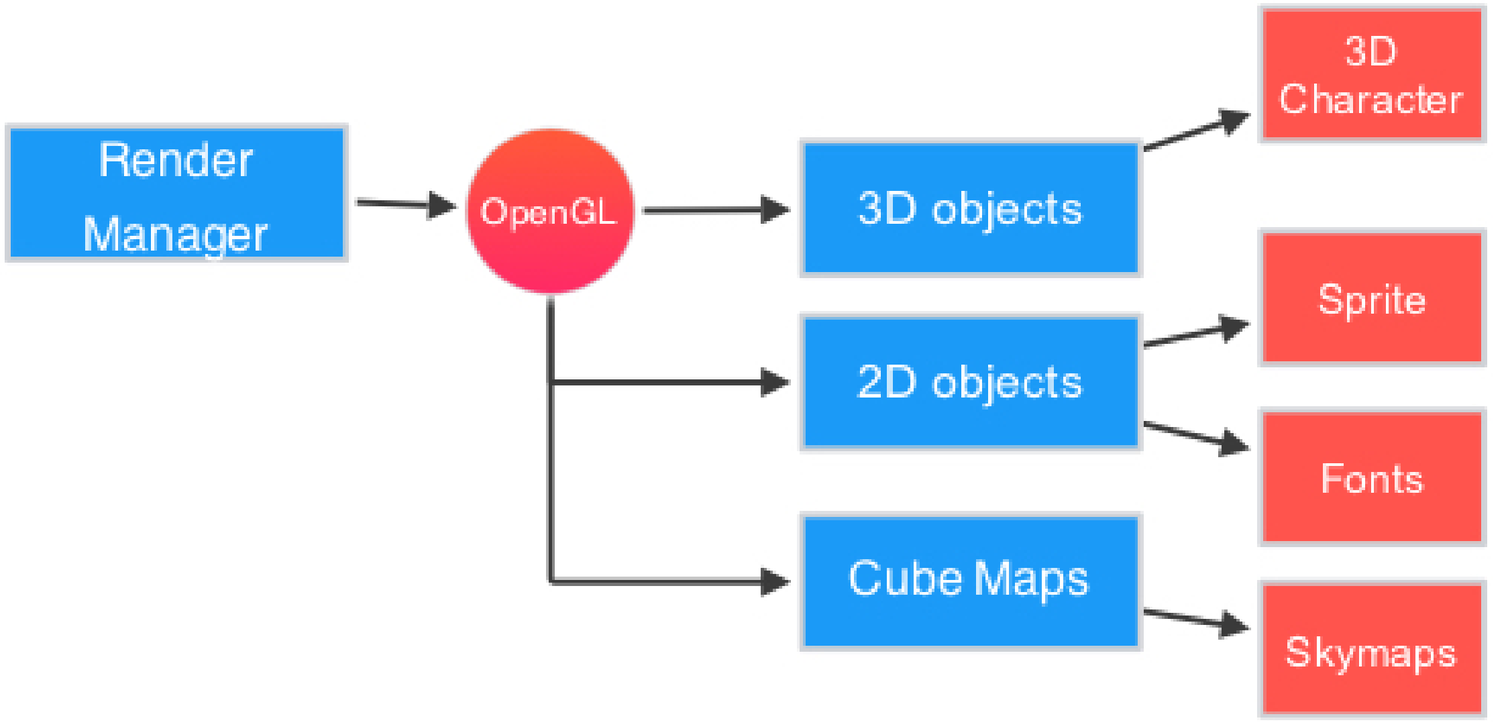
Bounding Volumes





BSIDES MUMBAI

RENDERING ENGINE



BSIDES MUMBAI

POTENTIAL VULNERABILITIES

Unreal Engine

- Code Injection
- Remote Code Execution (RCE)
- Exposed APIs
- Insecure File Handling

Unity

- Insecure Asset Store Content
- Data Exposure in WebGL Builds
- Cross-Site Scripting (XSS)
- Denial of Service (DoS) Attacks

BSIDES MUMBAI

LEVEL UP

LIFE 1 UP


BSIDES
MUMBAI

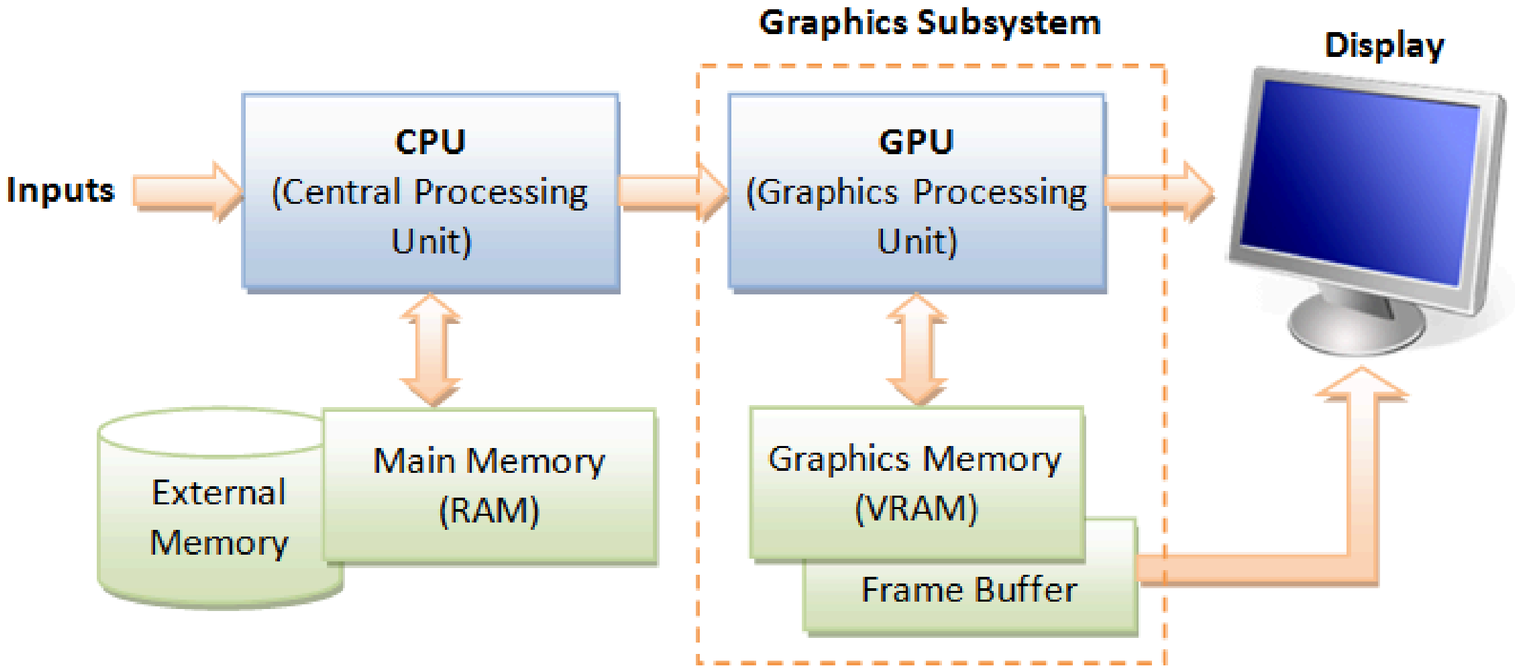

BSIDES
MUMBAI

BSIDES MUMBAI

GAME DRIVERS

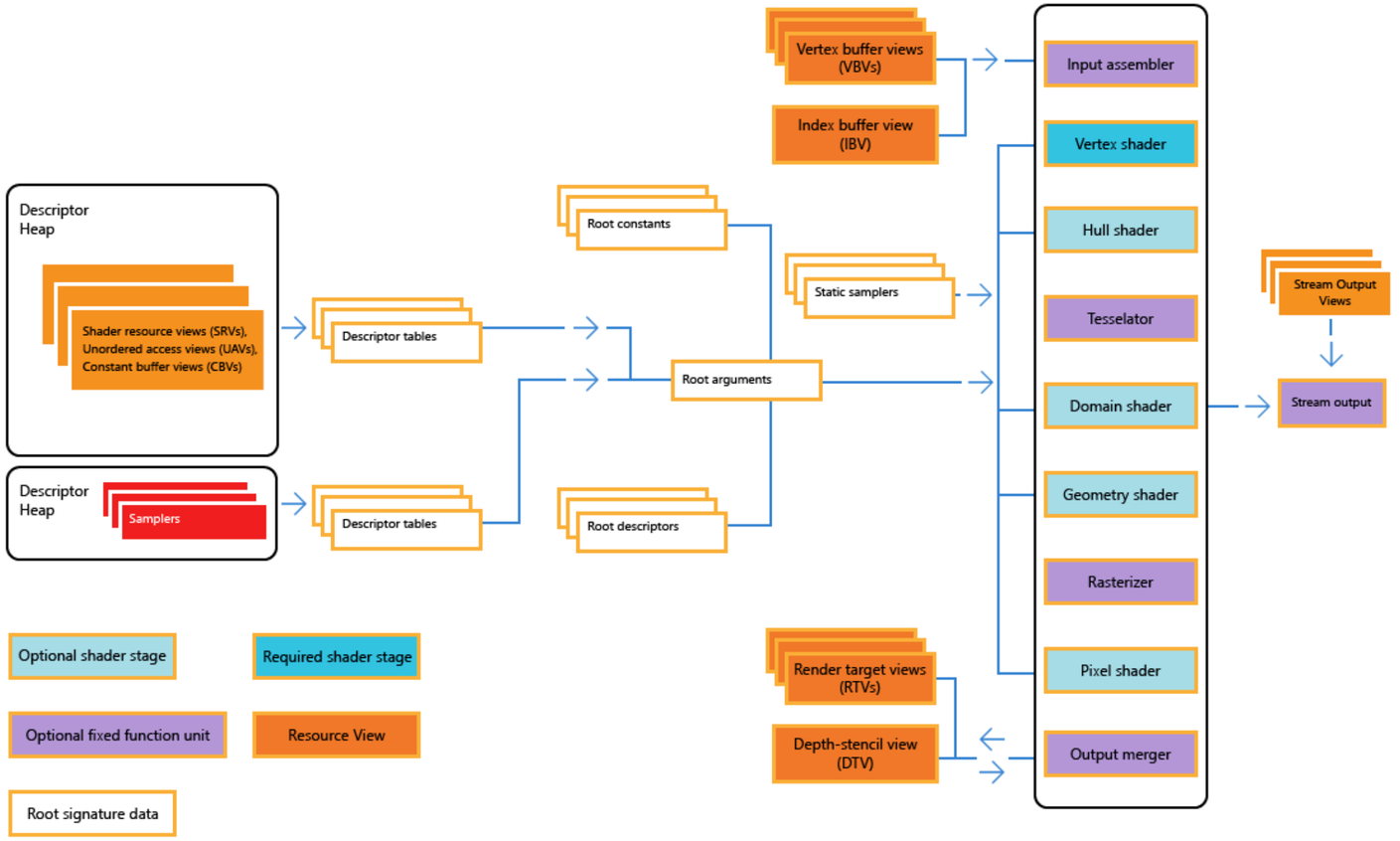
BSIDES MUMBAI

OPENGL



BSIDES MUMBAI

DIRECTX

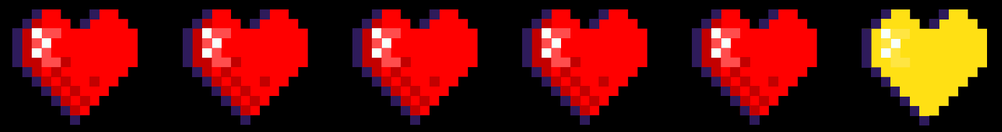


BSIDES MUMBAI

ESP WALL HACKS

BSIDES MUMBAI

LEVEL UP



LIFE 1 UP


BSIDES
MUMBAI


BSIDES
MUMBAI

BSIDES MUMBAI

BINARY/ EXECUTABLE/ DLL

BSIDES MUMBAI

BINARIES

A binary file is a computer file that is not a text file. The term "binary file" is often used as a term meaning "non-text file".

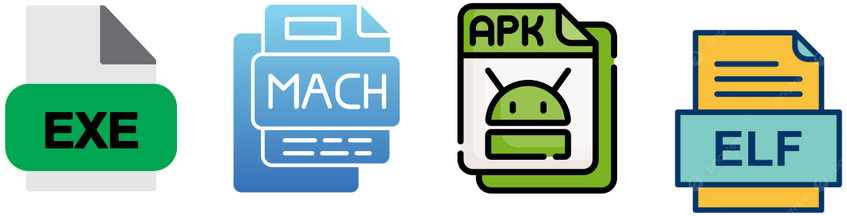
Let’s understand with example

BSIDES MUMBAI

EXECUTABLES

An executable causes a computer "to perform indicated tasks according to encoded instructions", as opposed to a data file that must be interpreted by a program to be meaningful.

Let’s understand with example



BSIDES MUMBAI

DLL FILES

A dynamic-link library is a shared library in the Microsoft Windows or OS/2 operating system. A DLL can contain executable code, data, and resources, in any combination.

Let’s understand with example

BSIDES MUMBAI

LEVEL UP

LIFE 1 UP

BSIDES
MUMBAI

BSIDES
MUMBAI

BSIDES MUMBAI

PRODUCT KEY BYPASS

BSIDES MUMBAI

PRODUCT KEY BYPASS

Start

BSIDES
MUMBAI

BSIDES
MUMBAI

BSIDES MUMBAI

MEMORY SCANNING & RES HACKING

BSIDES MUMBAI

MEMORY SCANNING & RES HACKING

Start

BSIDES
MUMBAI

BSIDES
MUMBAI

BSIDES MUMBAI

DLL INJECTIONS

BSIDES MUMBAI

DLL INJECTIONS

Start

BSIDES
MUMBAI

BSIDES
MUMBAI

BSIDES MUMBAI

WALLHACKS & AIMBOTS

BSIDES MUMBAI

WALLHACKS & AIMBOTS

Start

BSIDES
MUMBAI

BSIDES
MUMBAI

BSIDES MUMBAI

VALORANT DISSECTION

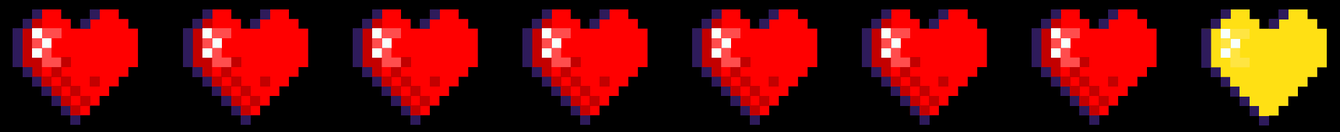
BSIDES MUMBAI

VALORANT DISSECTION

Start

BSIDES MUMBAI

LEVEL UP



LIFE 1 UP


BSIDES
MUMBAI

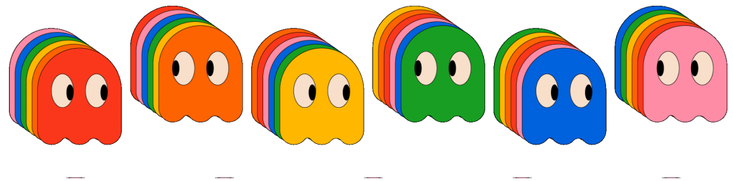

BSIDES
MUMBAI

FINAL COMMENTS

BSIDES MUMBAI

BEST PRACTICES

- Code Obfuscation
- Implementing Proper Access Controls
- 2FA
- Behavioral Analysis
- Encouraging Responsible Disclosures



BSIDES MUMBAI

RESOURCES

Reverse Engg Challenges

Game Hacking Resources

BSIDES MUMBAI

GAME OVER

EXIT

LET'S CONNECT

BSIDES MUMBAI

EMAIL ADDRESS

sanchayofficial@gmail.com

https://hackersvilla.xyz