hackersvilla.xyz

Game Hacking 101

A workshop on videogame pentesting

Presenter – Sanchay Singh

@ BSides Pune 2024

13-14 January, 2024

>_whoami

hackersvilla.xyz

-> ***Co-founder of HackersVilla CyberSecurity***

-> *Security Consultant/Trainer at MakeIntern*

-> *Worked as SME at UpgradCampus*

-> *Trained Employees of KPMG, Cognizant, etc*

-> *Security Mentor/Speaker at OWASP Delhi*

-> *Security Mentor at BSides Noida*

-> *Active part of NULL and THM Delhi Chapter*

Sanchay Singh

CYBERSECURITY EXPERT | CORPORATE TRAINER | PUBLIC SPEAKER

sanchayofficial

sanchayofficial@gmail.com

My Journey

Welcome to the Game Hacking Workshop!

hackersvilla.xyz

Agenda Overview

1. Brief on the gaming industry's exponential growth
2. Understanding Video Game Architecture
3. Common Security Challenges
4. Reverse Engineering and Analysis using Live Demonstrations
5. Countermeasures and Best Practices

Objectives

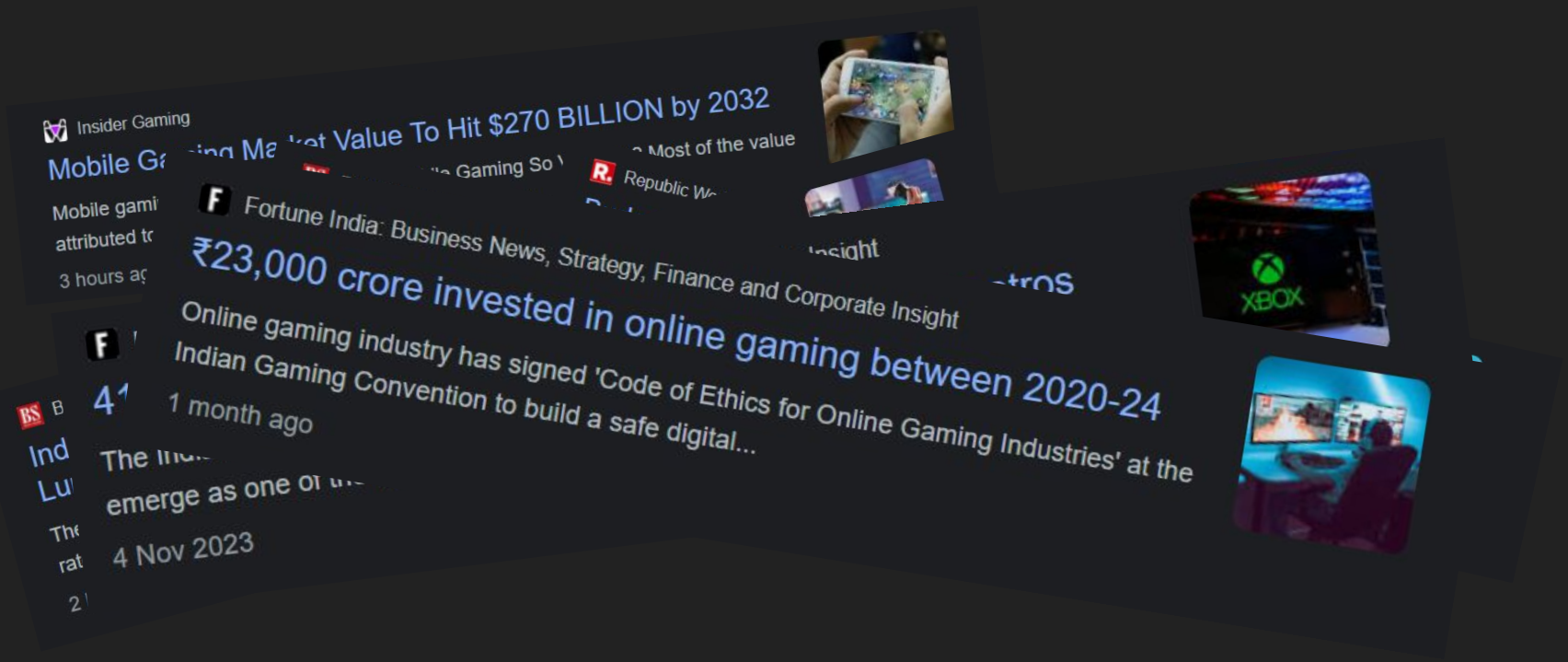
- Understand how modern days video games are engineered
- Understanding of Game Engines: What they are and how they work
- To learn about Unity, Unreal, etc
- Understand Reverse Engineering and role of RE in Game Hacking
- What loopholes to check and how can we dive deep into the code
- Best practices and understanding a sense of responsibility

hackersvilla.xyz

Exponential Growth of the Gaming Industry

hackersvilla.xyz

Remarkable Expansion



hackersvilla.xyz

Diverse Platforms

Games are not confined to consoles but have expanded across PC, mobile, and cloud gaming.

This diversification contributes to a more expansive and diverse gaming community.

Implications of Growth

Economic Impact:
The industry's expansion has led to a substantial economic impact globally. Increased job opportunities, revenue generation, and technological innovation have become hallmark features.

Technological Advancements:
Technological innovations, such as virtual reality (VR), augmented reality (AR), and high-quality graphics, have become more prevalent.

These advancements enhance user experiences but also present new challenges in terms of security.

Security Considerations

As the gaming ecosystem grows, so do security concerns.

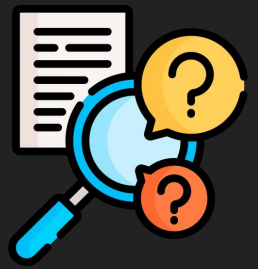
This workshop addresses the critical need for understanding and implementing security measures in the dynamically growing gaming industry.

By delving into video game architecture and security challenges, we can contribute to creating a secure gaming environment.

hackersvilla.xyz

Prerequisites for Participants

- Basic Cybersecurity Knowledge
- A working laptop/system
- Curiosity and Enthusiasm



hackersvilla.xyz

Importance of Security in Gaming

hackersvilla.xyz

Protecting Intellectual Property

hackersvilla.xyz

Safeguarding User Data

hackersvilla.xyz

Ensuring Fair Play

hackersvilla.xyz

Reputation and User Retention

hackersvilla.xyz

Legal and Regulatory Compliance

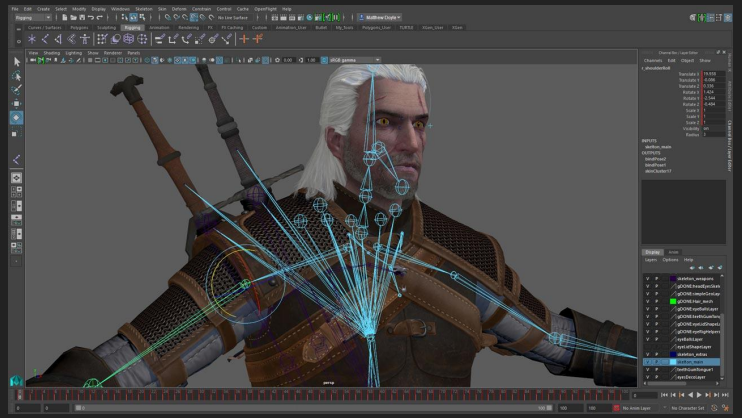
Video Game Architecture

hackersvilla.xyz

Game Development Stages

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.

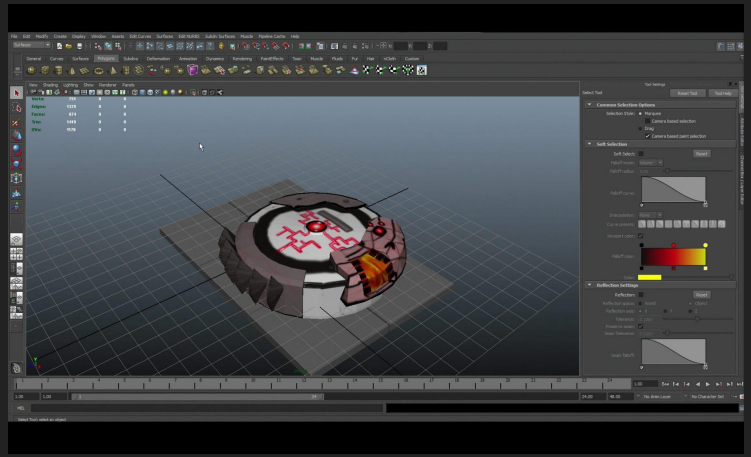


hackersvilla.xyz

Game Development Stages

Programming Phase

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

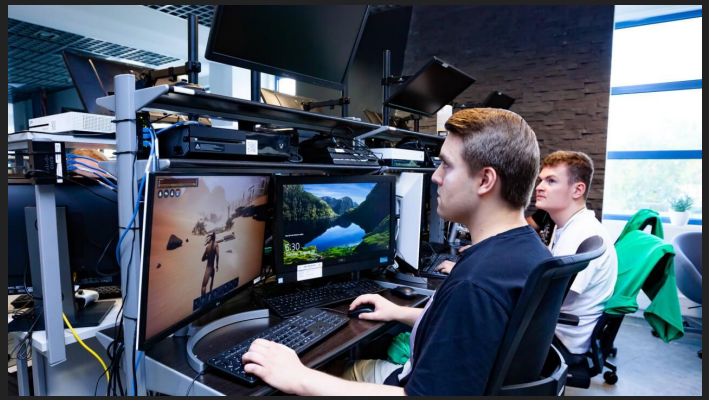


hackersvilla.xyz

Game Development Stages

Testing and Quality Assurance

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



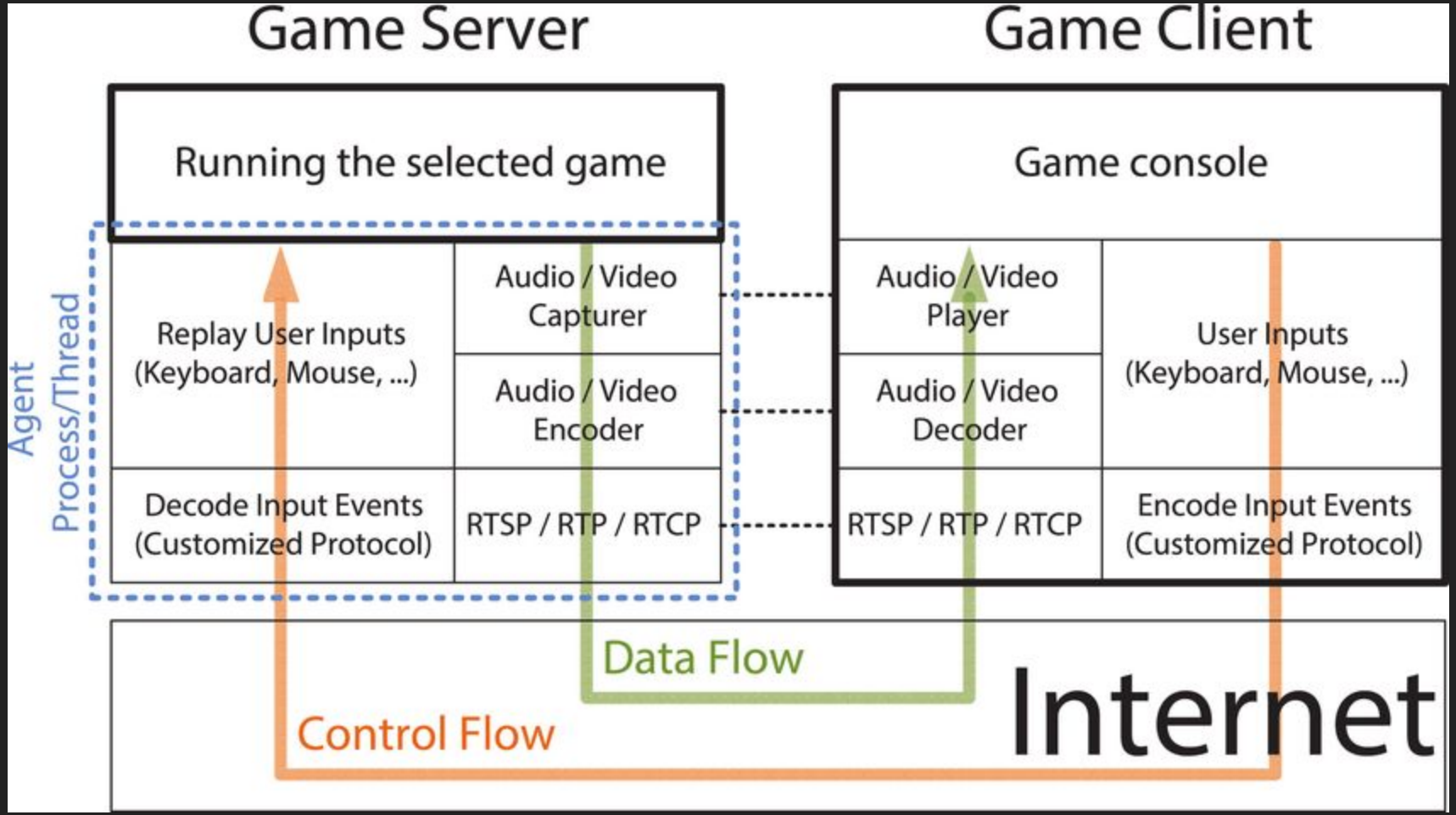
hackersvilla.xyz

Game Development Stages

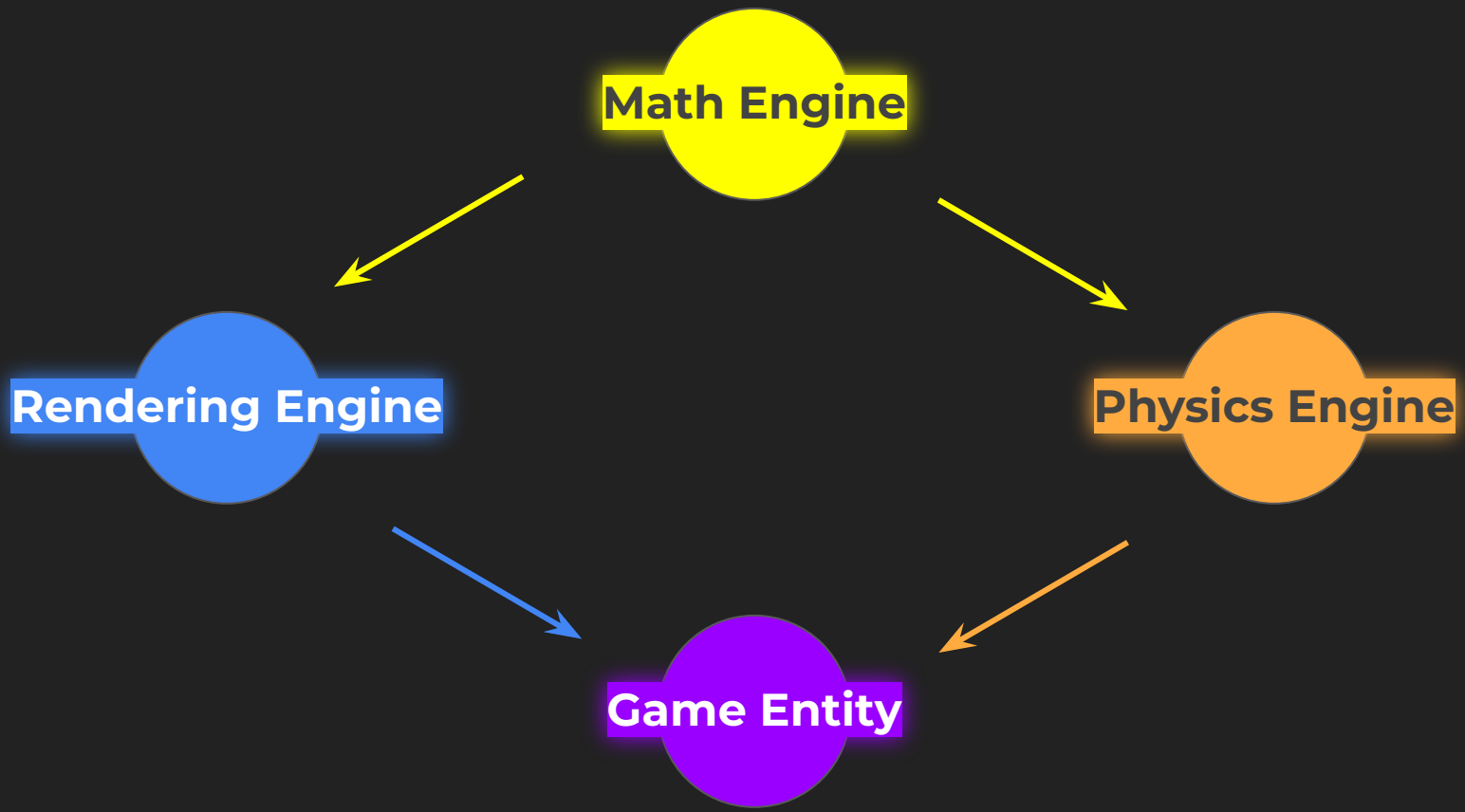
Deployment

- 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


Game Server
Game Client
Running the selected game
Game console
Agent Process/Thread
Replay User Inputs (Keyboard, Mouse, ...)
Audio / Video Capturer
Audio / Video Encoder
Decode Input Events (Customized Protocol)
RTSP / RTP / RTCP
Audio / Video Player
Audio / Video Decoder
RTSP / RTP / RTCP
User Inputs (Keyboard, Mouse, ...)
Encode Input Events (Customized Protocol)
Data Flow
Control Flow
Internet

Game Engines



Potential Vulnerabilities

hackersvilla.xyz

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

Common Security Challenges in Video Games

hackersvilla.xyz

Analysis of Common Threats

Aimbots and Wallhacks:

- Players using aimbots and wallhacks disrupt fair play.
- Real-world example: A popular first-person shooter faced widespread cheating issues, impacting the gaming experience for honest players.

hackersvilla.xyz

Analysis of Common Threats

Risks of User-Generated Content

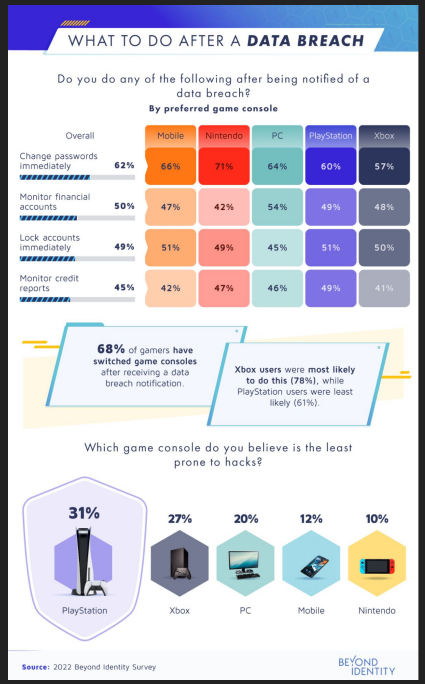
- User-generated content, while enriching the gaming experience, poses risks
- Example: A modding community unintentionally introduced a mod that compromised player privacy by accessing unintended game data

hackersvilla.xyz

Analysis of Common Threats

Account Breaches and Privacy Concerns

- Unauthorized access to player accounts can lead to data breaches and privacy concerns.
- Example: A major gaming platform experienced a security incident resulting in unauthorized access to millions of user accounts.



Reverse Engineering and Analysis

Let’s do some practical...

hackersvilla.xyz

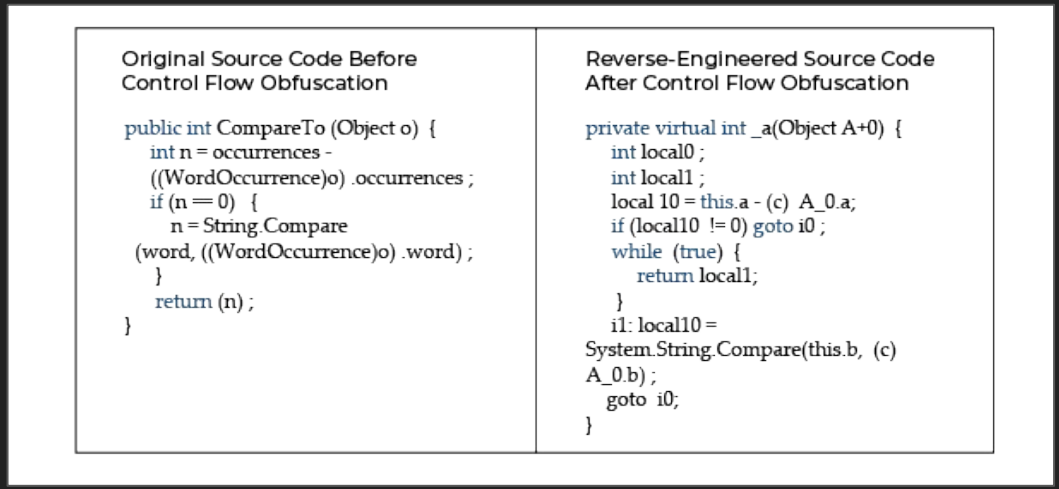
Scan the QR

hackersvilla.xyz

Countermeasures and Security Best Practices

Code Obfuscation and Encryption

Code obfuscation and encryption can deter attackers by making it harder to understand and manipulate the game code.



Original Source Code Before Control Flow Obfuscation

```
public int CompareTo (Object o)  {
    int n = occurrences -
    ((WordOccurrence)o) .occurrences ;
    if (n == 0)   {
        n = String.Compare
  (word, ((WordOccurrence)o) .word) ;
    }
    return (n) ;
}
```

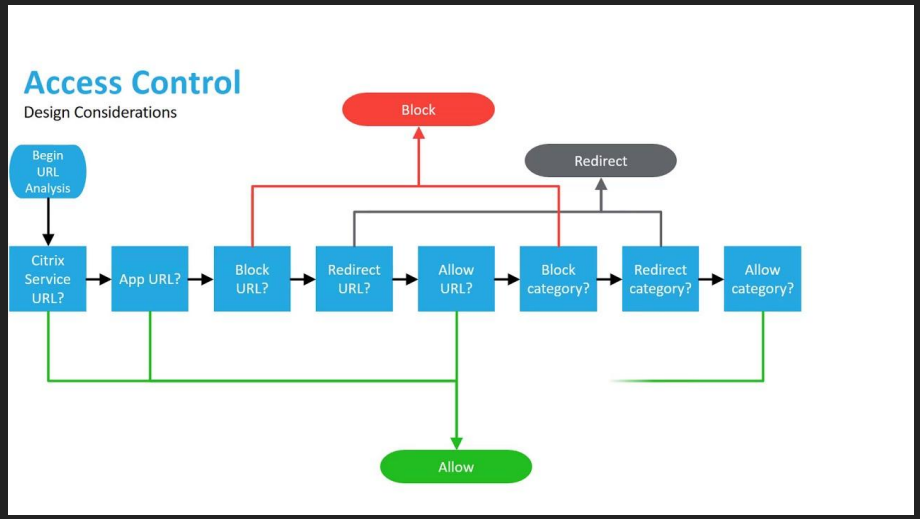
Reverse-Engineered Source Code After Control Flow Obfuscation

```
private virtual int _a(Object A+0)  {
    int local0 ;
    int local1 ;
    local 10 = this.a - (c)  A_0.a;
    if (local10  != 0) goto i0 ;
    while  (true)  {
        return local1;
    }
    i1: local10 =
System.String.Compare(this.b,  (c)
A_0.b) ;
    goto  i0;
}
```

hackersvilla.xyz

Implementing Proper Access Controls

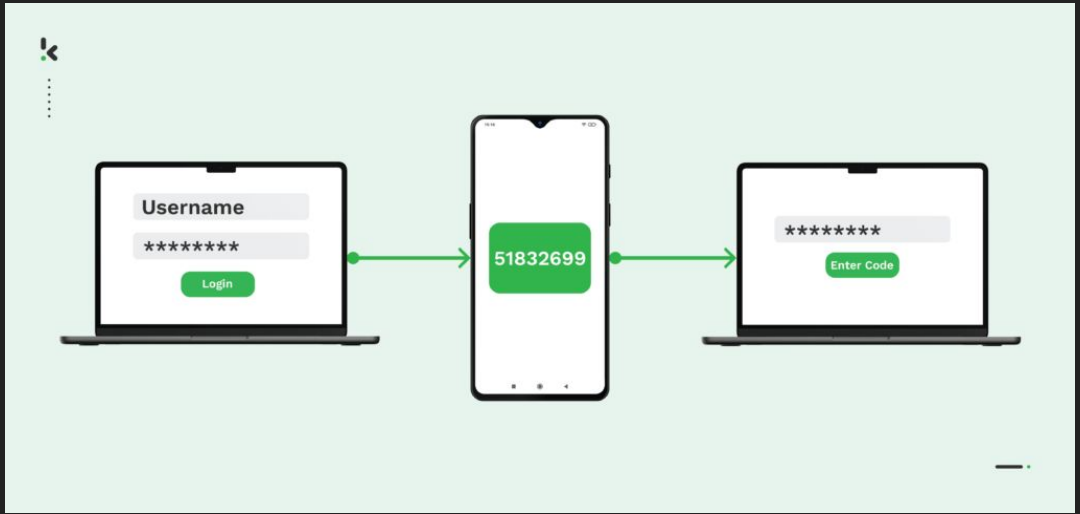
Restricting access to critical server components to authorized entities.



hackersvilla.xyz

Two-Factor Authentication (2FA)

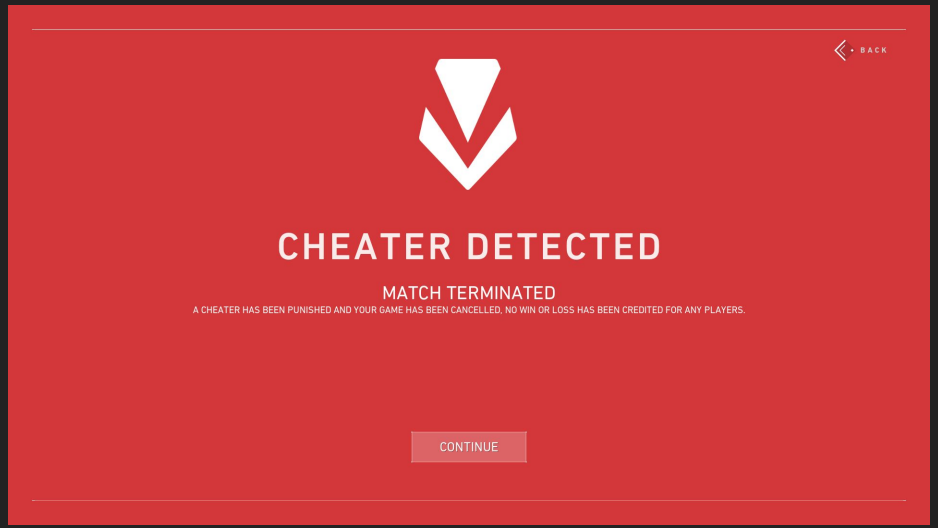
2FA adds an extra layer of security to user accounts,
preventing unauthorized access



hackersvilla.xyz

Behavioral Analysis for Cheat Detection:

Concept of monitoring player behavior to identify anomalies indicative of cheating.



hackersvilla.xyz

Encouraging Responsible Disclosure

Establishing channels for ethical hackers to report vulnerabilities.

So....
Lets Interact?

Thank you for your active engagement in the workshop.

Now, I invite **any questions** or discussions you may have.

Thank You