Penetration Testing Report on Dreadnought Video Game

Date: October 12, 2023

Introduction:
This report details the penetration testing performed on the video game called Dreadnought. Our team used a variety of tools, including Metasploit, to identify and exploit vulnerabilities in the game's infrastructure, network, and application. We discovered four critical vulnerabilities that could potentially lead to unauthorized access, data breaches, or other security risks.

SQL Injection Vulnerability:
Using the SQLMap tool, we identified an SQL injection vulnerability in the game's user registration system. Attackers could exploit this vulnerability to gain unauthorized access to the game's database, potentially exposing sensitive user information,modifying game data, or even deleting the entire database.

Mitigation:
We recommend implementing input validation, parameterized queries, and least-privileged access controls for the game's database. Additionally, consider using a Web Application Firewall (WAF) to protect against SQL injection attacks.

Remote Code Execution (RCE) Vulnerability:
Metasploit was employed to discover an RCE vulnerability in the game's custom web server. This vulnerability allows attackers to execute arbitrary code on the server, potentially compromising the entire system and accessing sensitive data.

Mitigation:
Patch the affected web server to the latest secure version and disable any unnecessary features or services. Implement proper input validation and ensure that the server only processes trusted data. Regularly update and monitor the server to prevent future RCE vulnerabilities.

Insecure File Upload:
We found that the game's file upload system does not validate user-uploaded content properly. This vulnerability allows attackers to upload malicious files, which could potentially lead to remote code execution, privilege escalation, or other security breaches.

Mitigation:
Implement strict file type and size restrictions, as well as server-side input validation for uploaded files. Additionally, store uploaded files in a separate server, isolated from the main application server, and run regular scans to detect and remove any malicious content.

Unencrypted Network Traffic:
During our network analysis, we discovered that the game's network traffic is not encrypted, making it vulnerable to Man-in-the-Middle (MITM) attacks. Attackers could potentially intercept and manipulate data transmitted between players and the game server, including login credentials and in-game transactions.

Mitigation:
Implement encryption protocols, such as TLS, to secure network traffic between the game client and server. Regularly update encryption certificates and enforce strong cipher suites to maintain secure connections.

Conclusion:
The penetration testing performed on the Dreadnought video game revealed four significant vulnerabilities that pose considerable security risks. We recommend addressing these vulnerabilities promptly and conducting regular security audits to ensure a safe and enjoyable gaming experience for all players. By prioritizing the security of the game, the developers can protect both their users and their reputation in the gaming industry.