### introducción

Acá les quiero hablar como funciona la tabla de amenazas (stride) en servidores online en videojuegos, en temas de la identidad el jugador y el mismo no haga un caos el servidor con los errores, hagan trampas, hackeos. también que hace la compañía con el tema.

### 

### 

### 1. Spoofing (Suplantación de identidad)

Amenaza:

Un atacante se hace pasar por otro jugador (por ejemplo, usando credenciales robadas o manipulando paquetes).

Falsificación de identidad para acceder a cuentas premium.

Mitigación:

Autenticación segura (por ejemplo, tokens JWT, OAuth2).

Autenticación de dos factores (2FA).

Validación criptográfica de mensajes entre cliente y servidor.

### 2. Tampering (Manipulación de datos)

Amenaza:

Alterar paquetes enviados al servidor (por ejemplo, modificando el daño o velocidad en un shooter).

Hackers modifican el cliente para enviar información ilegal (cheats, aimbots).

Mitigación:

Validación estricta del lado del servidor.

Uso de canales cifrados (TLS).

Anticheat en cliente + detección en servidor de patrones anómalos.

### 

### 

### 3. Repudiation (Negación de acciones)

Amenaza:

Jugadores niegan haber hecho trampas, usado exploits, o enviado ciertos mensajes ofensivos.

Mitigación:

Logging detallado en el servidor (acciones, IP, timestamps).

Firmado de logs o eventos críticos.

### 4. Information Disclosure (Divulgación de información)

Amenaza:

Filtración de datos de usuarios (correos, contraseñas, estadísticas privadas).

Exposición de detalles técnicos del servidor que puedan usarse para ataques.

Mitigación:

Cifrado en tránsito y en reposo.

Control de acceso a datos sensibles.

Minimizar información expuesta en errores o APIs.

5. Denial of Service (DoS)

Amenaza:

Atacar el servidor para que deje de responder (saturación de conexiones, spam de solicitudes).

Uso excesivo de recursos por scripts maliciosos o jugadores bots.

Mitigación:

Firewalls y sistemas de detección de intrusos.

Rate limiting.

Balanceadores de carga y escalado automático.

### 6. Elevation of Privilege (Elevación de privilegios)

Amenaza:

Un jugador normal obtiene acceso a comandos de administración.

Vulnerabilidades que permiten cambiar estadísticas o recursos.

Mitigación:

Separación clara de roles (administrador, moderador, jugador).

Revisión del código para prevenir inyecciones o exploits.

Autorización estricta en cada acción.

paso 1: owasp mutillidae II