# 1 – Acciones posibles del atacante

El atacante intentará vulnerar el sistema con distintos métodos.  
Podemos listar algunas acciones realistas:

|  |  |  |
| --- | --- | --- |
| Tipo de ataque | Descripción breve | Consecuencia |
| SQL Injection | Inserta código malicioso en formularios o URLs. | Acceso no autorizado a base de datos. |
| Fuerza bruta (Brute force) | Prueba contraseñas de forma automatizada. | Compromete cuentas de usuario. |
| Cross-Site Scripting (XSS) | Inserta scripts en formularios para ejecutar en navegadores de otros usuarios. | Robo de cookies o datos de sesión. |
| Denegación de servicio (DoS) | Satura el servidor con peticiones. | Interrupción del servicio. |
| Phishing interno | Simula correos del sistema para robar credenciales. | Robo de información confidencial. |

# 2 – Funciones o tecnicas del sistema de detección

El **sistema de defensa** debe responder con distintas herramientas de detección o mitigación:

|  |  |  |
| --- | --- | --- |
| Función del sistema | Herramienta o técnica usada | Qué detecta / previene |
| Análisis de logs en tiempo real | SIEM / Splunk / Elastic | Detecta patrones anómalos de acceso. |
| Firewall de Aplicaciones Web (WAF) | ModSecurity, Cloudflare | Bloquea inyecciones SQL y XSS. |
| Autenticación multifactor (MFA) | Google Authenticator, SMS, biometría | Previene accesos por fuerza bruta. |
| Rate limiting y captchas | Nginx rate limit, reCAPTCHA | Reduce intentos de login masivos. |
| Monitor de tráfico | IDS/IPS (Snort, Suricata) | Detecta flujos sospechosos y los bloquea. |

# 3 – Aplicación de la poda alfa – beta

El **sistema (MAX)** busca **maximizar la detección de ataques**.

El **atacante (MIN)** busca **minimizar la probabilidad de detección**.

Cada **nodo** del árbol representa un **estado del sistema**, con un valor de evaluación (por ejemplo, probabilidad de detección).

La poda alfa-beta :

**α (alfa):** mejor valor garantizado para MAX (detección mínima esperada).

**β (beta):** mejor valor garantizado para MIN (riesgo máximo aceptable).

Si en algún punto se cumple **β ≤ α**, **se poda** la rama (no se explora más porque no mejorará la solución actual).

Supongamos que el sistema analiza tres escenarios posibles ante intentos de ataque:

1. **Escenario A:** Ataque por SQL Injection.
2. **Escenario B:** Ataque por fuerza bruta.
3. **Escenario C:** Ataque por XSS.

Cada uno tiene sub-opciones del sistema:

* **Bloquear IP**
* **Registrar evento y seguir monitoreando**
* **Activar defensa automática (WAF o MFA)**

La poda ocurre cuando una rama genera una **probabilidad de detección menor o igual** al mejor valor ya garantizado (es decir, no vale la pena explorarla).

# 4 – Arbol de decisiones

Diagrama

El contenido generado por IA puede ser incorrecto.