Vulnerabilidades principales OWASP

Fundamentos de la ciberseguridad

ALBERTO MÉNDEZ NÚÑEZ

Contenido

Resumen no oficial

OWASP Top 10 – 2025: Resumen Ejecutivo

#	VULNERABILIDAD	CAMBIO VS 2021	IMPACTO	PREVALENCIA
A01	Broken Access Control	↔ Mantiene #1	Crítico	94% apps
A02	Cryptographic Failures	↔ (antes Sensitive Data)	Alto	60% apps
A03	Injection	↓ De #1 a #3	Crítico	40% apps
A04	Insecure Design	↔ Nueva categoría	Alto	55% apps
A05	Security Misconfiguration	↔	Alto	85% apps
A06	Vulnerable Components	↔	Crítico	70% apps
A07	Authentication Failures	↔	Crítico	45% apps
A08	Software & Data Integrity	NEW Nueva (supply chain)	Alto	30% apps
A09	Logging & Monitoring Failures	↔	Medio	75% apps
A10	Server-Side Request Forgery	NEW SSRF entra al Top 10	Alto	25% apps

A01:2025 - Broken Access Control (Control de Acceso Roto)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
40	20.15%	3.74%	100.00%	42.93%	7.04	3.84	1,839,701

Qué es:
Ocurre cuando un sistema no restringe correctamente qué usuarios pueden acceder a ciertos recursos o realizar acciones específicas, permitiendo que usuarios no autorizados obtengan acceso.

Impacto:

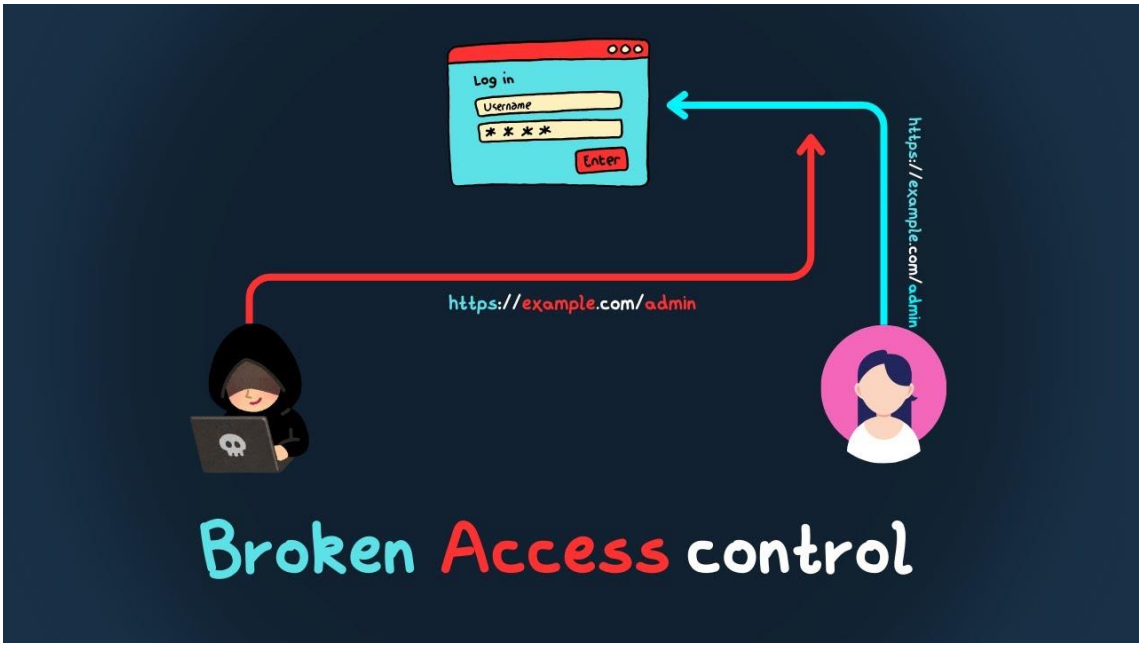
- Acceso a datos sensibles.
- Modificación de información crítica.
- Escalamiento de privilegios.

Mitigaciones:

- Implementar control de acceso basado en roles (RBAC) o atributos (ABAC).
- Validar los permisos en el servidor, no solo en el cliente.
- Revisar rutas y APIs para asegurar restricciones.

Herramientas:

- **OWASP ZAP**, **Burp Suite** (para pruebas de acceso).
- **Postman** (para testeo de APIs).
- **Access Control Testing Frameworks**.



A02:2025 - Security Misconfiguration (Mala Configuración de Seguridad)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
16	27.70%	3.00%	100.00%	52.35%	7.96	3.97	719,084

Qué es:
Cuando la configuración de seguridad de sistemas, servidores, aplicaciones o servicios es débil, incorrecta o por defecto, facilitando ataques.

Impacto:

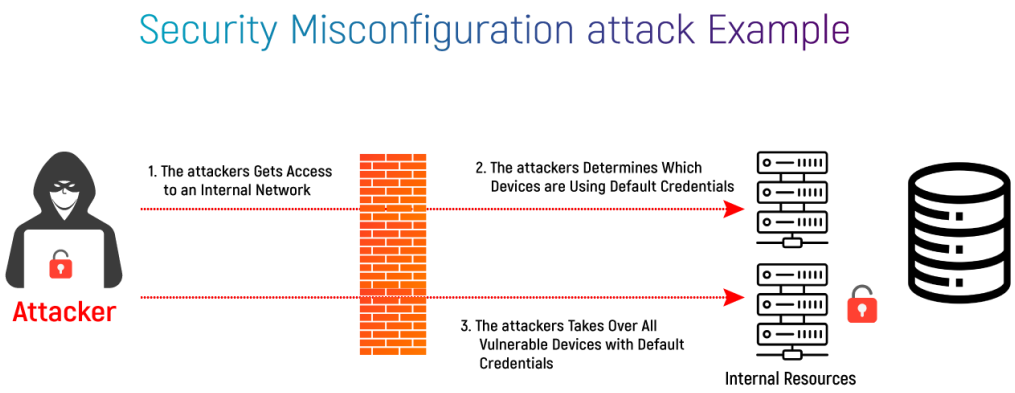
- Filtración de información.
- Acceso no autorizado.
- Exposición de interfaces de administración.

Mitigaciones:

- Desactivar servicios y puertos innecesarios.
- Usar configuraciones seguras por defecto.
- Revisar y automatizar configuraciones con políticas de hardening.

Herramientas:

- **Nmap**, **Nessus**, **OpenVAS** (escaneo de configuraciones).
- **Lynis** (auditoría de seguridad).



A03:2025 - Software Supply Chain Failures (Fallos en la Cadena de Suministro de Software)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
6	9.56%	5.72%	65.42%	27.47%	8.17	5.23	215,248

Qué es:
Vulnerabilidades introducidas a través de librerías de terceros, componentes de código abierto o dependencias externas comprometidas.

Impacto:

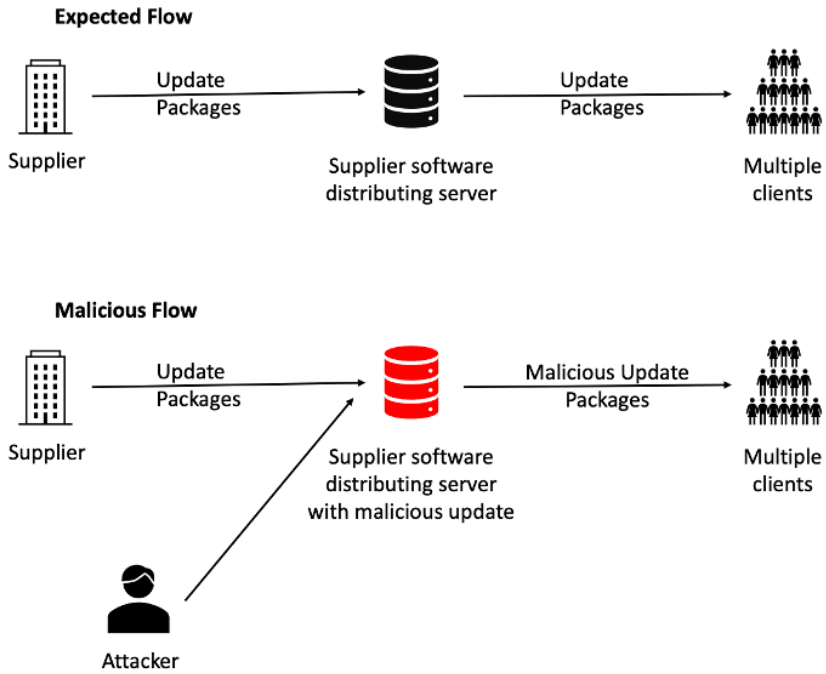
- Compromiso del sistema completo.
- Propagación de malware o ransomware.
- Pérdida de integridad de datos.

Mitigaciones:

- Verificar firmas y hashes de paquetes.
- Mantener dependencias actualizadas.
- Revisar proveedores y auditorías de componentes.

Herramientas:

- **Snyk**, **OWASP Dependency-Check**, **WhiteSource**.



A04:2025 - Cryptographic Failures (Fallos Criptográficos)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
32	13.77%	3.80%	100.00%	47.74%	7.23	3.90	1,665,348

Qué es:
Uso de algoritmos débiles, configuración incorrecta o almacenamiento inseguro de datos sensibles.

Impacto:

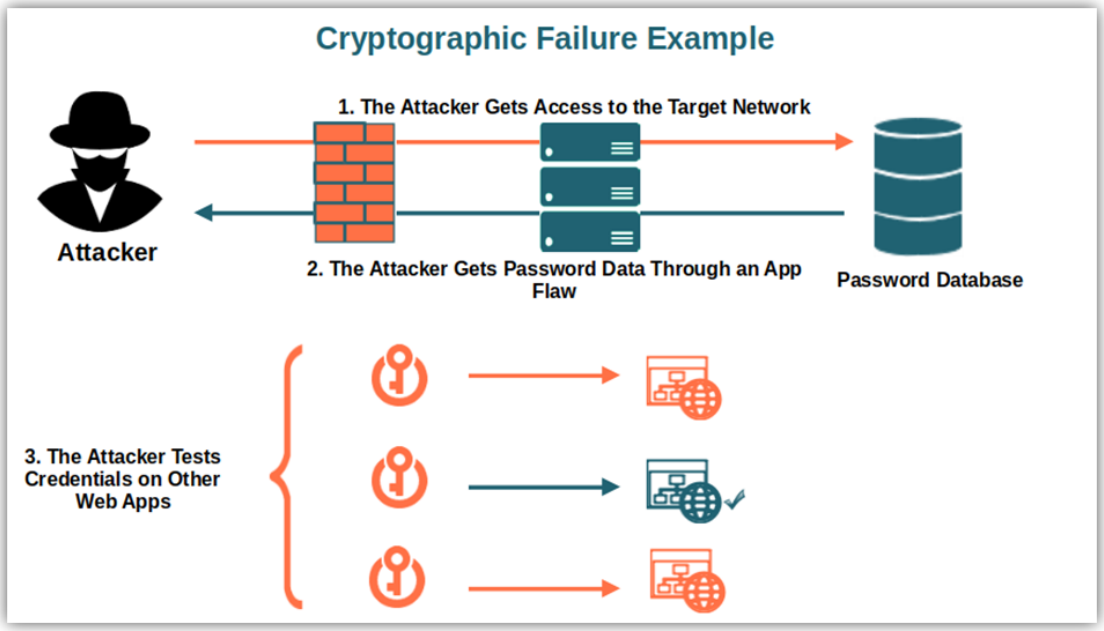
- Exposición de datos confidenciales.
- Robo de credenciales o información financiera.
- Posibilidad de ataques de fuerza bruta o descifrado.

Mitigaciones:

- Usar algoritmos modernos y fuertes (AES, RSA 2048+, SHA-256+).
- Encriptar datos en tránsito y en reposo.
- Evitar almacenamiento de contraseñas sin hashing seguro (usar bcrypt, Argon2).

Herramientas:

- **Hashcat**, **OpenSSL**, **GPG**, **Burp Suite** (testing de cifrado).



A05:2025 - Injection (Inyección)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
37	13.77%	3.08%	100.00%	42.93%	7.15	4.32	1,404,249

Qué es:
Cuando un atacante envía datos maliciosos que son interpretados por la aplicación como comandos, como SQL, NoSQL, OS o LDAP injection.

Impacto:

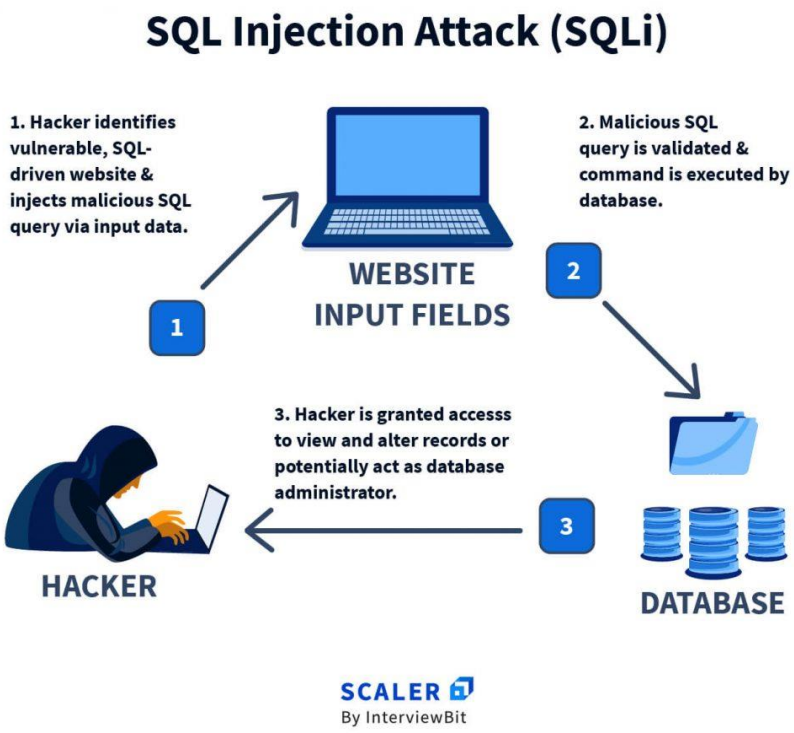
- Robo o manipulación de datos.
- Ejecución de comandos en el servidor.
- Compromiso completo del sistema.

Mitigaciones:

- Usar consultas parametrizadas y ORM.
- Validar y sanear todas las entradas de usuario.
- Limitar privilegios de la base de datos.

Herramientas:

- **SQLMap**, **Burp Suite**, **OWASP ZAP**, **NoSQLMap**.



A06:2025 - Insecure Design (Diseño Inseguro)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
39	22.18%	1.86%	88.76%	35.18%	6.96	4.05	729,882

Qué es:
Fallos en la arquitectura o diseño de la aplicación que crean vulnerabilidades, antes incluso de la codificación.

Impacto:

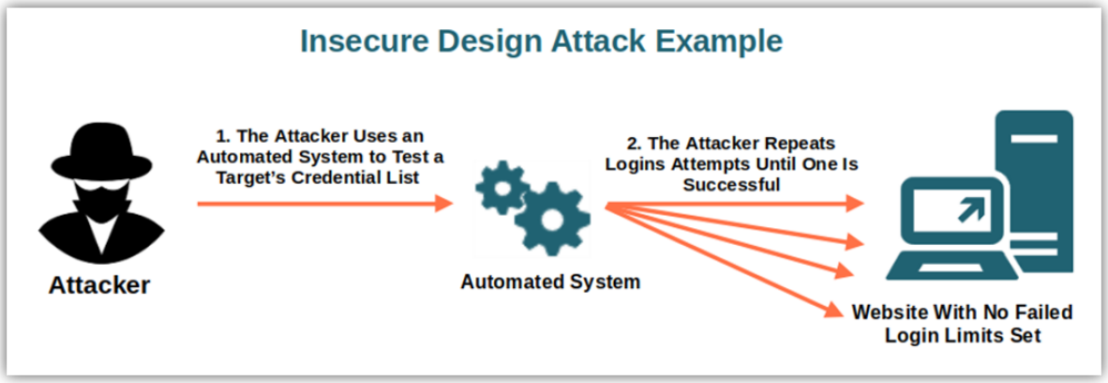
- Vulnerabilidades persistentes.
- Exposición de datos y recursos críticos.
- Difícil mitigación post-desarrollo.

Mitigaciones:

- Revisiones de seguridad desde diseño (Threat Modeling).
- Seguir principios de seguridad como mínimo privilegio y defensa en profundidad.
- Integrar seguridad en DevSecOps.

Herramientas:

- **OWASP Threat Dragon**, **Microsoft Threat Modeling Tool**, **Archimate Security Modelling**.



A07:2025 - Authentication Failures (Fallos de Autenticación)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
36	15.80%	2.92%	100.00%	37.14%	7.69	4.44	1,120,673

Qué es:
Fallas en la verificación de identidad del usuario que permiten accesos no autorizados.

Impacto:

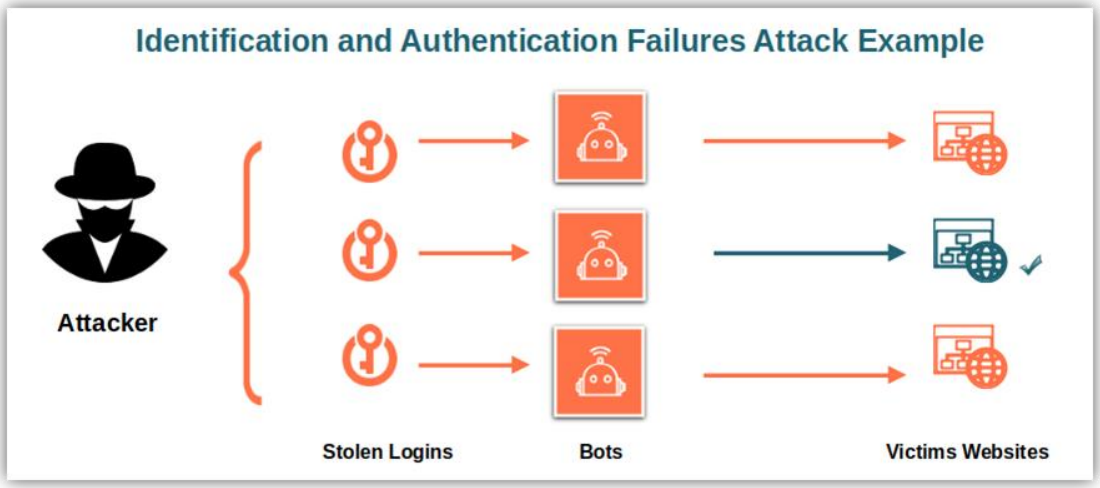
- Robo de cuentas.
- Suplantación de identidad.
- Acceso a datos privados y funciones críticas.

Mitigaciones:

- Implementar autenticación multifactor (MFA).
- Evitar contraseñas débiles o reutilizadas.
- Monitorear intentos de login y bloquear ataques de fuerza bruta.

Herramientas:

- **OWASP ZAP**, **Burp Suite**, **Hydra**, **John the Ripper** (testing de autenticación).



A08:2025 - Software or Data Integrity Failures (Fallos de Integridad de Software o Datos)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
14	8.98%	2.75%	78.52%	45.49%	7.11	4.79	501,327

Qué es:
Cambios no autorizados en el software o datos, ya sea por corrupción, manipulación o instalación de software comprometido.

Impacto:

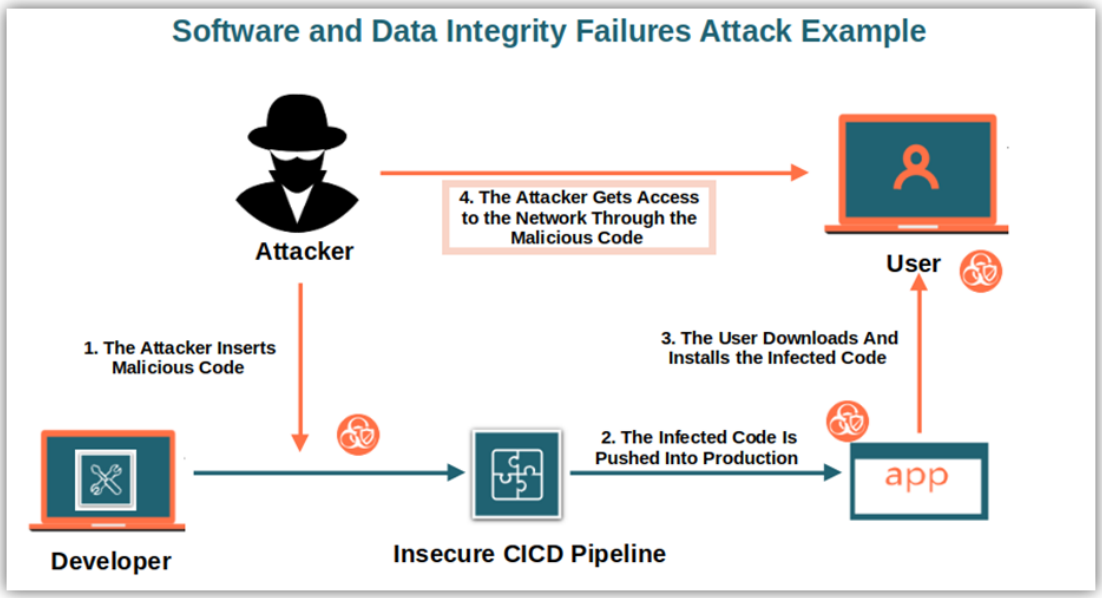
- Ejecución de código malicioso.
- Pérdida de confiabilidad del sistema.
- Manipulación de datos críticos.

Mitigaciones:

- Validar firmas digitales y hashes.
- Revisar integridad de dependencias.
- Monitorear cambios en archivos críticos.

Herramientas:

- **Tripwire**, **AIDE**, **Sigstore**, **Hash-based integrity tools**.



A09:2025 - Security Logging and Alerting Failures (Fallos en Registro y Alerta de Seguridad)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
5	11.33%	3.91%	85.96%	46.48%	7.19	2.65	260,288

Qué es:
Falta de registro o alertas de actividades sospechosas, lo que dificulta la detección de ataques o incidentes.

Impacto:

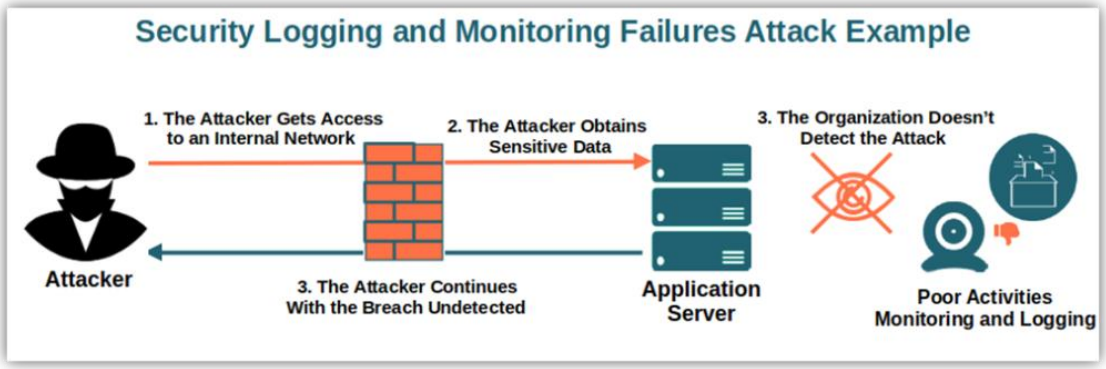
- Incapacidad para responder a incidentes.
- Persistencia de intrusiones sin ser detectadas.
- Daños prolongados y pérdida de datos.

Mitigaciones:

- Implementar logging centralizado y seguro.
- Monitorizar eventos críticos y anomalías.
- Configurar alertas en tiempo real y revisión periódica.

Herramientas:

- **ELK Stack (Elasticsearch, Logstash, Kibana)**, **Splunk**, **Graylog**, **Prometheus + Grafana**.



A10:2025 - Mishandling of Exceptional Conditions (Manejo Incorrecto de Condiciones Excepcionales)

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Max Coverage	Avg Coverage	Avg Weighted Exploit	Avg Weighted Impact	Total Occurrences
24	20.67%	2.95%	100.00%	37.95%	7.11	3.81	769,581

Qué es:
Errores o excepciones no manejadas correctamente que pueden revelar información sensible o dejar la aplicación en estado vulnerable.

Impacto:

- Fugas de información (stack traces, detalles internos).
- Bloqueo o denegación de servicio.
- Posibilidad de explotación de fallos no controlados.

Mitigaciones:

- Capturar y manejar excepciones de manera segura.
- No mostrar información sensible al usuario final.
- Registrar los errores de forma segura y monitorizada.

Herramientas:

- **Sentry**, **LogRocket**, **New Relic**, frameworks de manejo de errores (dependen del lenguaje).

Comparación 2023-2025