5 API Injection Attacks

Every Developer Must Know

Explore :·

CREST. Accredited

certin Empanelled

sales@briskinfosec.com

SQL Injection

The Classic Database Threat

The Attack:

Malicious SQL commands inserted through API parameters to manipulate database queries. Attackers can bypass authentication, extract sensitive data, or delete entire database tables.

Example:

Instead of a valid user ID, an attacker sends '; DROP TABLE users; – to an unprotected API endpoint, potentially destroying critical user data.

Business Impact:

Complete database compromise, data breaches, regulatory violations,and potential business shutdown.

CREST Accredited

certin Empanelled

sales@briskinfosec.com

NoSQL Injection

MongoDB's Weak Spot

The Attack:

Exploits document-based databases by manipulating JSON parameters to bypass authentication or extract unauthorized data. Particularly dangerous as NoSQL databases gain popularity.

Technical Reality:

Attackers target MongoDB and similar systems through JSON parameter manipulation, circumventing access controls that rely solely on query structure validation.

Risk Factor:

Growing exponentially as organizations migrate to NoSQL solutions without proper security hardening.

CREST. Accredited

certin Empanelled

sales@briskinfosec.com

OS Command Injection

System Takeover

The Attack:

Executes arbitrary operating system commands through API endpoints that fail to sanitize user inputs. This grants attackers direct system access beyond the application layer.

Execution Method:

Malicious commands embedded in API requests target server infrastructure, potentially enabling complete system compromise.

Strategic Concern:

Transforms application vulnerabilities into infrastructure breaches, escalating impact severity.

CREST. Accredited

certin Empanelled

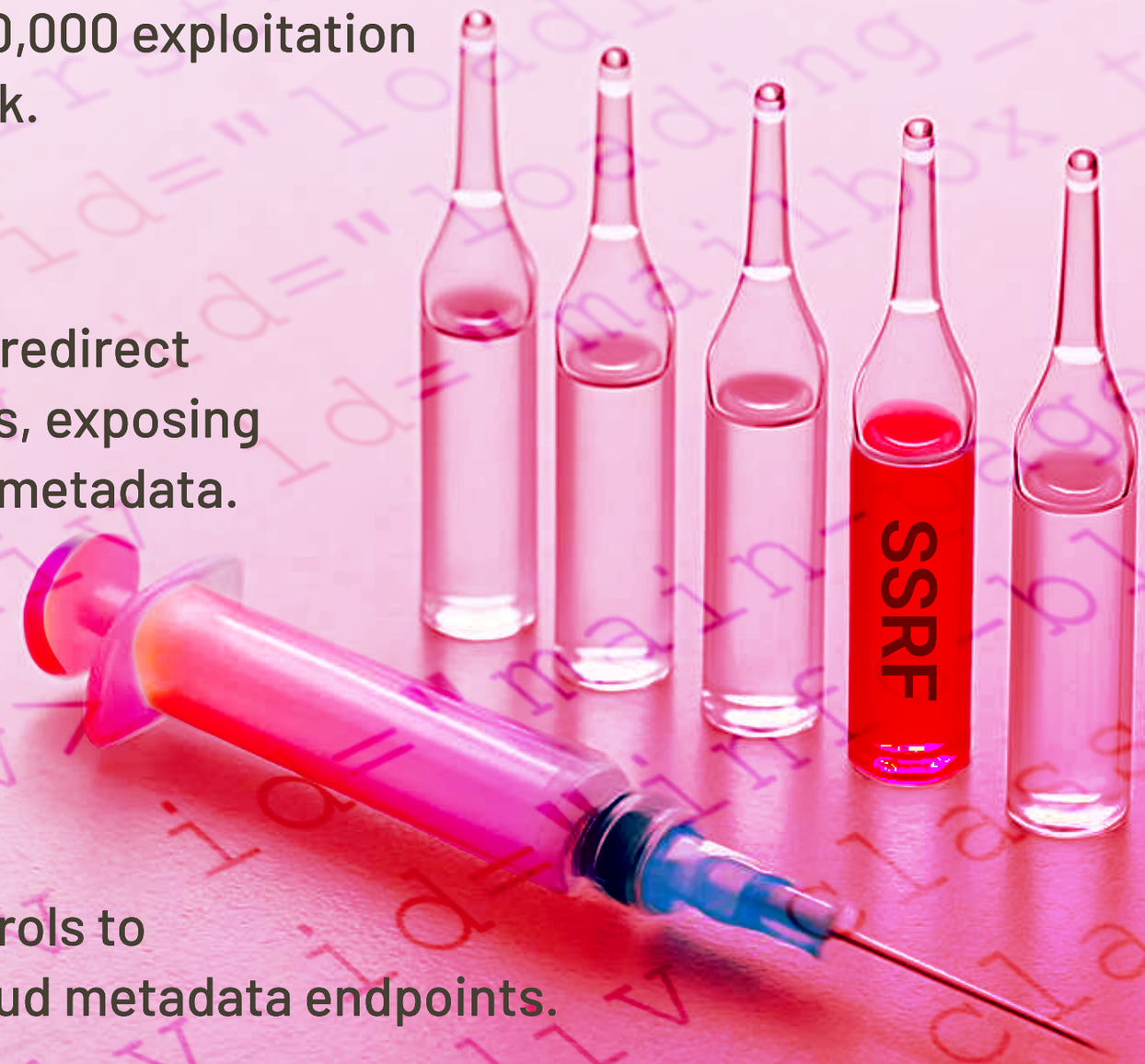
sales@briskinfosec.com

Server-Side Request Forgery (SSRF)

Internal Network Exploitation

The Attack:

Forces APIs to make unintended requests to internal systems or external malicious endpoints. The 2025 ChatGPT tool exploit demonstrates real -world SSRF impact, with over 10,000 exploitation attempts logged within one week.



Technical Mechanism:

Crafted URLs in API parameters redirect requests to unauthorized targets, exposing internal resourcesand sensitive metadata.

Enterprise Risk:

Bypasses network security controls to access internal services and cloud metadata endpoints.

CREST. Accredited

certin Empanelled

sales@briskinfosec.com

Cross-Site Scripting (XSS) via API

Client-Side Compromise

The Attack:

Malicious scripts injected through API responses are reflected on web pages, compromising user browsers and stealing credentials.

Modern Context:

As APIs increasingly serve dynamic content to web applications, XSS vulnerabilities multiply across the attack surface.

Cascading Impact:

User session hijacking, credential theft, and lateral movement within organizational networks.

CREST. Accredited

certin Empanelled

sales@briskinfosec.com

BriskInfosec™
VULNERABILITY TO VICTORY

Connect with us today to build stronger defenses.

BOOK A MEETING

CREST Accredited
certin Empanelled

sales@briskinfosec.com