SHATTERED

LIVE BREAKING 3h ago CYBERSECURITY SQL Injection Prevention in Node.js: 12 Steps [2026]

NEWSROOM Live TODAY 5 new ARCHIVE 62 stories LAST FILED 3h ago LANGUAGES 10

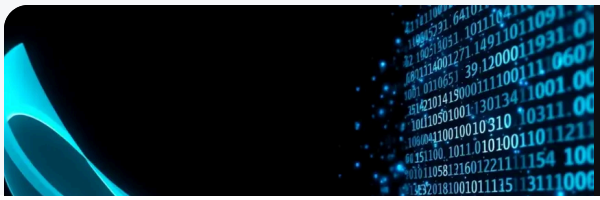
UTC 20:05:14

SQL Injection Prevention in Node.js: 12 Steps [2026]

SQL injection remains the most reliably exploited web vulnerability in 2026. According to the Verizon 2025 Data Breach Investigations Report, injection attacks account for 17% of all confirmed data breaches, and Node.js applications are frequently targeted...

3h ago · Jun 21, 2026

Read the brief →



Ed25519 vs RSA: 50x Faster, 8x Smaller Keys [2026]

Ed25519 signs a message in roughly 20 microseconds. RSA-2048 takes 667 microseconds for the same operation. That 33x...

7h ago

FortiBleed: 86,644 Fortinet Firewalls Exposed in 194 Countries [2026]

A Russian-speaking cybercriminal syndicate has quietly harvested verified administrator and VPN credentials from 86,644 Fortinet FortiGate firewalls across...

11h ago

THE DESKS

// editorial departments

01 **Cybersecurity**
Breaches, CVE post-mortems and zero-day reporting
38 stories →

02 **Cryptography**
Hash functions, signatures and the SHA family
15 stories →

03 **Privacy**
VPNs, Tor, encrypted messaging, surveillance
7 stories →

04 **Cryptocurrency**
Blockchain hashing, wallets and on-chain incidents
2 stories →

LATEST

// fresh from the editors

Palo Alto GlobalProtect CVE-2026-0257: CVSS 7.8 Auth Bypass Exploited [2026]

Palo Alto Networks confirmed on May 13, 2026 that CVE-2026-0257, a high-severity authentication bypass in its GlobalProtect VPN portal and gateway, was...

Jun 21, 2026 Read →

npm audit: 12 Steps to Fix Node.js Vulnerabilities [2026]

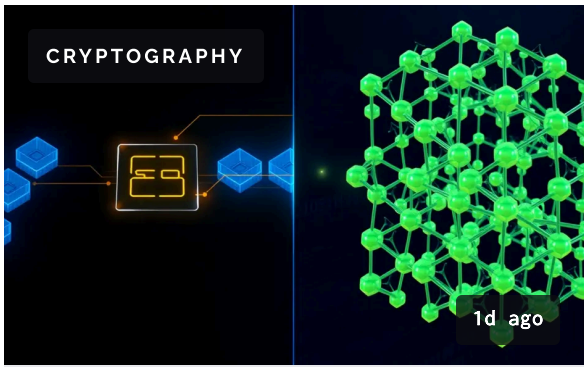
Every Node.js project accumulates vulnerable dependencies. The npm registry holds over 2.5 million packages, and researchers found 454,000 malicious or vulnerable packages...

Jun 20, 2026 Read →

TLS 1.3 in Node.js: 12 Steps to Secure HTTPS in 30 Min [2026]

Every HTTPS connection your Node.js server makes starts with a TLS handshake. That handshake negotiates which cipher to use, verifies the server...

Jun 20, 2026 Read →



SHA-256 vs SHA3-256: 3.5x Speed Gap, Same 128-bit Security [2026]

Pick the wrong hash function today and you may face a painful migration before 2030. SHA-256 vs SHA3-256 is the most consequential...

Jun 20, 2026 Read →

Foxconn Hit by Nitrogen Ransomware: 8TB Stolen, Apple and Nvidia Data Exposed [2026]

On May 11, 2026, the Nitrogen ransomware group posted Foxconn to its dark web leak site, NitroBlog, claiming to have stolen 8...

Jun 20, 2026 Read →

FBI DCSNet Hack: Salt Typhoon Exposes Wiretap Data on 80 Nations

On the night of February 17, 2026, FBI analysts noticed something wrong with the logs on one of the bureau's most sensitive...

Jun 20, 2026 Read →

MORE FROM THE DESKS

// keep digging

01 **CrowdStrike vs SentinelOne: 99.7% vs 97.5% Detection [2026]** CYBERSECURITY · JUN 19

02 **OWASP Top 10 in Node.js: 12 Steps to Secure Your API [2026]** CYBERSECURITY · JUN 19

03 **VeraCrypt vs BitLocker: Free, Open-Source, 5 Ciphers [2026]** CYBERSECURITY · JUN 19

04 **Oracle WebLogic Zero-Day: CVSS 10.0, 140K Attacks in 12 Days [2026]** CYBERSECURITY · JUN 19

// ABOUT

About Shattered.io

This domain has been home to the SHAttered SHA-1 collision project since 2017, and is now a hub for cryptography, security and privacy reporting. The full origin story of the project, the two proof PDFs and the research credits live below.

The SHAttered project — origin, proof files and research credits +

What you'll find on shattered.io today +

SHATTERED.IO

Independent explainers on cryptography, security, privacy and the technology behind provably-fair systems. Home of the original SHA-1 collision research.

18+ Some topics cover gambling. Play responsibly and only where it is legal for you.

TOPICS

Cryptocurrency

Cryptography

Cybersecurity

Privacy

COMPANY

About Us

Contact

Terms

Privacy

Responsible Use

LANGUAGE

English | Deutsch | Deutsch (AT) | Français | Italiano | Dansk | Svenska | Suomi | Norsk | Português

The SHA-1 collision paper and colliding PDFs remain available on this site.