CYBERSAFE BANGALORE

CONTENT

NODE JS SECURITY TOOLS

Web Framework Hardening

Input Validation & Output Encoding

Static Code Analysis

Secure Composition

CSRF

Vulnerabilities and Security Advisories

Security Hardening

Security Incidents

CYBERSAFE BANGALORE

Node js Security Tools

Web Framework Hardening

HELMET

Helmet helps you secure your Express apps by setting various HTTP headers.

BLANKIE

CSP plugin for hapi.

CYBERSAFE BANGALORE

Node js Security Tools

Input Validation & Output Encoding

node-esapi

node-esapi is a minimal port of the ESAPI4JS (Enterprise Security API for JavaScript) encoder.

escape-html

Escape string for use in HTML

js-string-escape

Escape any string to be a valid JavaScript string literal between double quotes or single quotes.

CYBERSAFE BANGALORE

Node js Security Tools

Input Validation & Output Encoding

validator

An npm library of string validators and sanitizers

xss-filters

Just sufficient output filtering to prevent XSS!

CYBERSAFE BANGALORE

Node js Security Tools

Static Code Analysis

eslint-plugin-security

ESLint rules for Node Security. This project will help identify potential security hotspots, but finds a lot of false positives which need triage by a human.

safe-regex

detect potentially catastrophic exponential-time regular expressions by limiting the star height to 1.

vuln-regex-detector

This module lets you check a regex for vulnerability. In JavaScript, regular expressions (regexes) can be "vulnerable": susceptible to catastrophic backtracking. If your application is used on the client side, this can be a performance issue. On the server side, this can expose you to Regular Expression Denial of Service (REDOS).

git-secrets

Prevents you from committing secrets and credentials into git repositories.

CYBERSAFE BANGALORE

Node js Security Tools

Static Code Analysis

DevSkim

DevSkim is a set of IDE plugins and rules that provide security "linting" capabilities. Also has support for CLI so it can be integrated into CI/CD pipeline.

ban-sensitive-files

Checks filenames to be committed against a library of filename rules to prevent storing sensitive files in Git. Checks some files for sensitive contents (for example authToken inside .npmrc file).

vuln-regex-detector

A static security code scanner for Node.js applications. Including neat UI that can point where the issue is and how to fix it.

CYBERSAFE BANGALORE

Node js Security Tools

Secure Composition

pug-plugin-trusted-types

Pug template plugin makes it easy to securely compose HTML from untrusted inputs and provides CSP & CSRF automagic.

safesql

A tagged template (mysql`...`) that understands Postgres's & MySQL's query grammar to prevent SQL injection.

sh-template-tag

A tagged template (sh`...`) that understands Bash syntax so prevents shell injection.

CYBERSAFE BANGALORE

Node js Security Tools

CSRF

csurf

Node.js CSRF protection middleware.

crumb

CSRF crumb generation and validation for hapi.

CYBERSAFE BANGALORE

Node js Security Tools

Vulnerabilities and Security Advisories

auditjs

Audits an NPM package.json file to identify known vulnerabilities using the OSSIndex.

npm-audit

Runs a security audit based on your package.json using npm.

npm-audit-resolver

Manage npm-audit results, including options to ignore specific issues in clear and auditable way.

gammaray

Runs a security audit based on your package.json using the Node.js Security Working Group vulnerability data.

CYBERSAFE BANGALORE

Node js Security Tools

Vulnerabilities and Security Advisories

snyk

Snyk helps you find, fix and monitor known vulnerabilities in Node.js npm, Ruby and Java dependencies, both on an ad hoc basis and as part of your CI (Build) system.

npq

Safely install packages with npm or yarn by auditing them as part of your install process.

node-release-lines

Introspection API for Node.js release metadata. Provides information about release lines, their relative status along with details of each release.

CYBERSAFE BANGALORE

Node js Security Tools

Security Hardening

express-limiter

Rate limiting middleware for Express applications built on redis.

npq

Fast, flexible and friendly rate limiter by key and protection from DDoS and brute force attacks in process Memory, Cluster, Redis, MongoDb, MySQL, PostgreSQL at any scale. Express and Koa examples included.

limits

Simple express/connect middleware to set limit to upload size, set request timeout etc.

CYBERSAFE BANGALORE

Node js Security Tools

Security Incidents

EasyDEX-GUI

malicious code found in npm package event-stream.

event-stream

malicious code found in npm package event-stream.

eslint

malicious packages found in npm package eslint-scope and eslint-config-eslint.

CYBERSAFE BANGALORE

Node js Security Tools

Security Incidents

getcookies

malicious package getcookies gets embedded in higher-level express related packages

crossenv

malicious typosquatting package crossenv steals environment variables.


THANKYOU