What is prototype pollution?

Prototype pollution is a JavaScript vulnerability where an attacker injects properties into `Object.prototype`, the base object every other object inherits from, by abusing keys like `__proto__` in user-controlled data. Because the polluted property then appears on all objects, it can change application logic, bypass security checks, cause denial of service, and, combined with the right gadget, reach remote code execution (notably in Node.js). It is caused by unsafe recursive merges of untrusted input, and the fix is safe key handling and object hygiene.

HOW IT WORKS

01 How it works and example

The attacker supplies crafted keys to a vulnerable merge or property setter:

- Inject a property: a JSON body `{"__proto__":{"polluted":"yes"}}` passed to an unsafe deep-merge makes `({}).polluted === "yes"` true everywhere.
- Bypass logic: pollute a flag the app checks (for example an access or configuration default).
- Denial of service: pollute a property that breaks application assumptions.
- Remote code execution: in Node.js, chaining prototype pollution with a suitable gadget (such as a template engine or child-process option) has reached RCE.

Examples shown for defensive context.

> IT IS JAVASCRIPT-SPECIFIC
>
> *Prototype pollution is unique to JavaScript's prototype model. The dangerous keys are* `__proto__`*,* `constructor`*, and* `prototype`*. Any code that recursively merges untrusted input must refuse them.*

HOW TO DEFEND

- Reject dangerous keys (`__proto__`, `constructor`, `prototype`) when merging or assigning untrusted data.
- Use safe operations: `Object.create(null)` for maps, `Map` instead of plain objects, and `Object.freeze(Object.prototype)` to harden it.
- Use vetted, patched libraries for deep merge and object handling (many historical CVEs were merge utilities).
- Validate input against a strict schema so unexpected keys are dropped.
- Test JSON-handling endpoints for prototype pollution.

SOURCES

[1] OWASP Top 10

[2] MITRE CWE-1321: Improperly Controlled Modification of Object Prototype Attributes

[3] OWASP Web Security Testing Guide

Test your application for prototype pollution and 30+ other classes.
securelayer7.net/learn/application-security/prototype-pollution

Open online