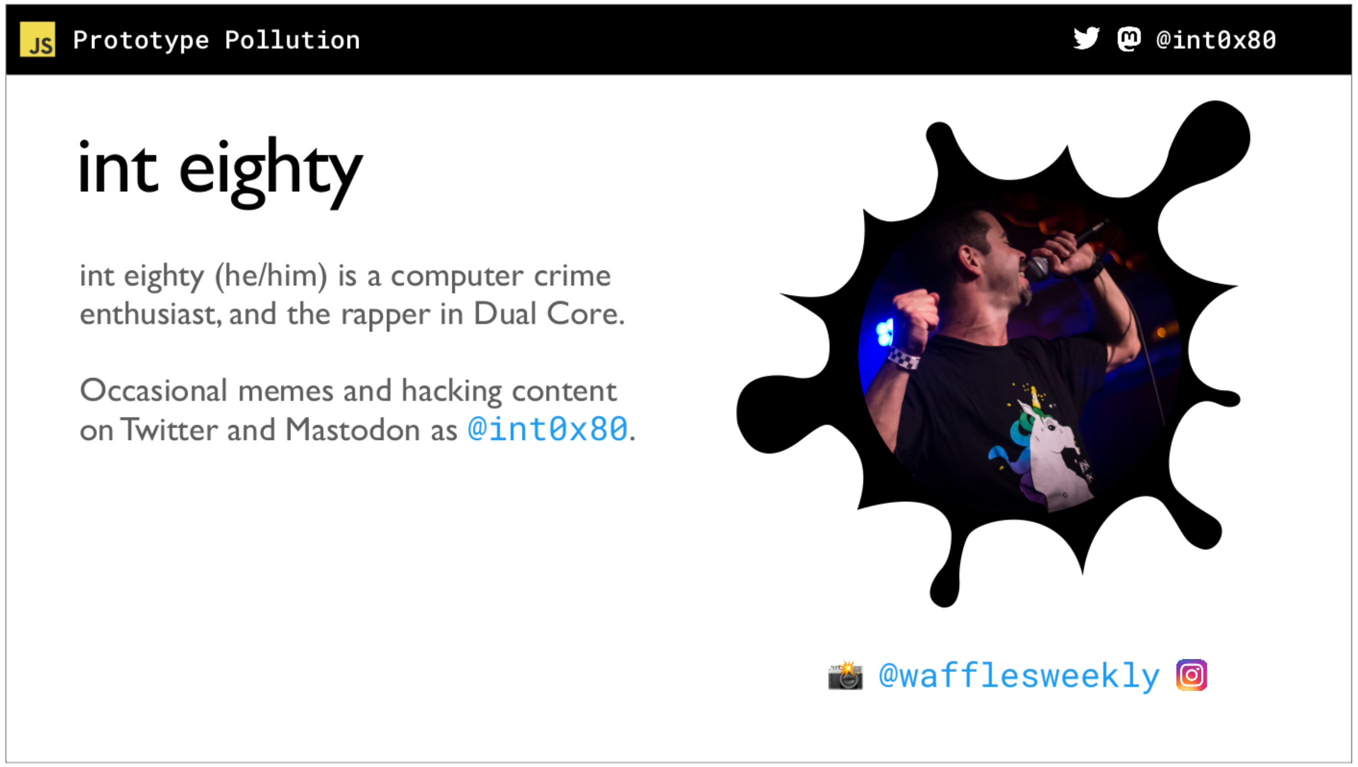
# Prototype Pollution

__proto__[governable]=false

@int0x80



JS Prototype Pollution

@int0x80

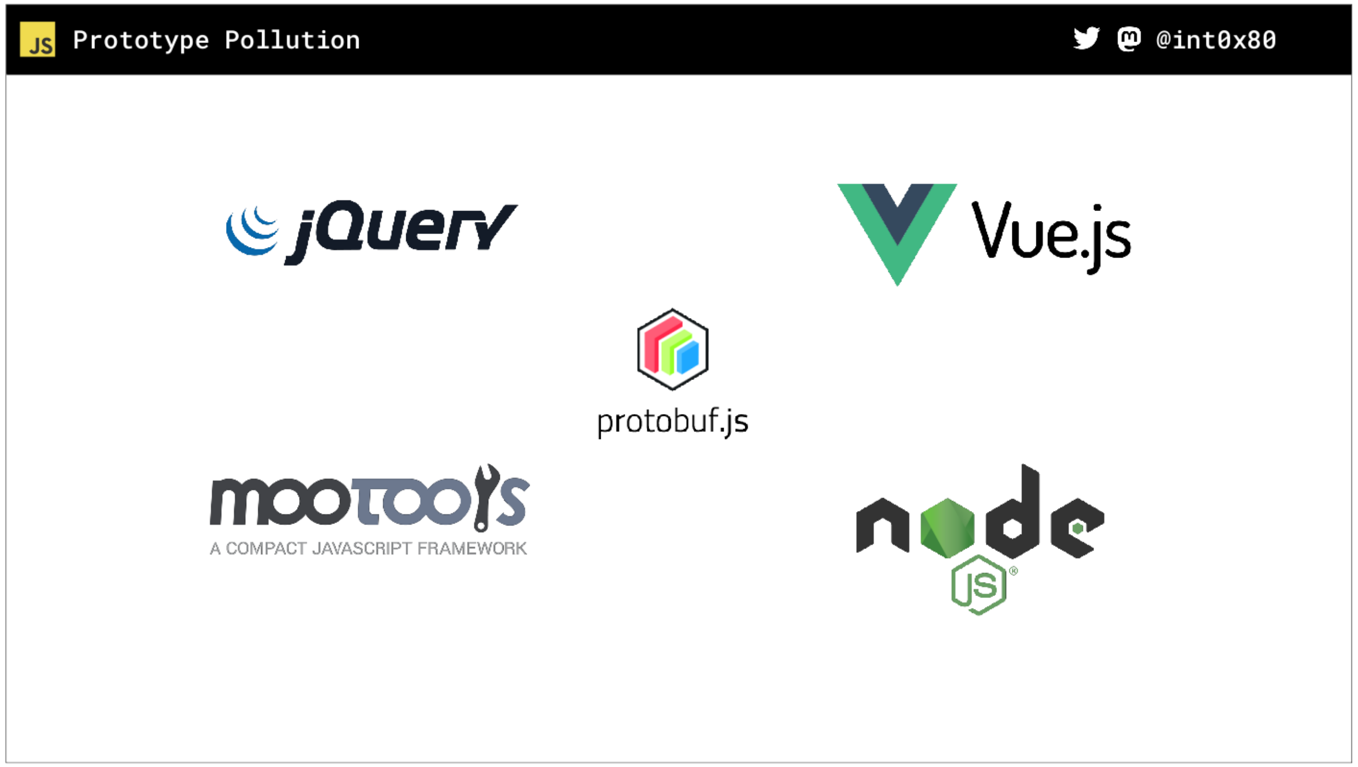
## int eighty

int eighty (he/him) is a computer crime enthusiast, and the rapper in Dual Core.

Occasional memes and hacking content on Twitter and Mastodon as `@int0x80`.

📸 @wafflesweekly

- Hack computers, rap music, internet memes



JS Prototype Pollution

@int0x80

jQuery

Vue.js

protobuf.js

mootools

A COMPACT JAVASCRIPT FRAMEWORK

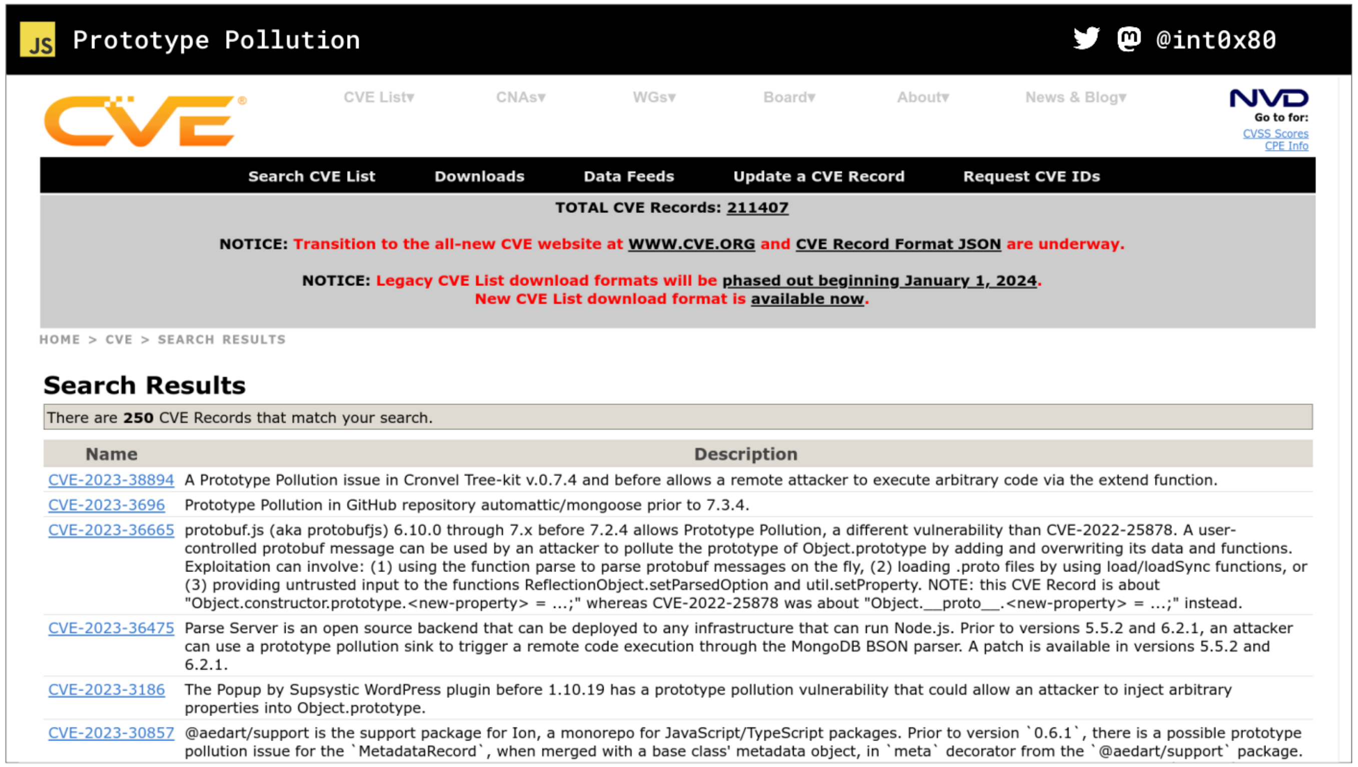
node

JS

- Priv esc
- Dangerous behaviors
- Somewhat widespread
    - Apps using a vetted library can still have vulns, even if lib not vuln

## Prototype Pollution

@int0x80



TOTAL CVE Records: 211407

**NOTICE:** Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

**NOTICE:** Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

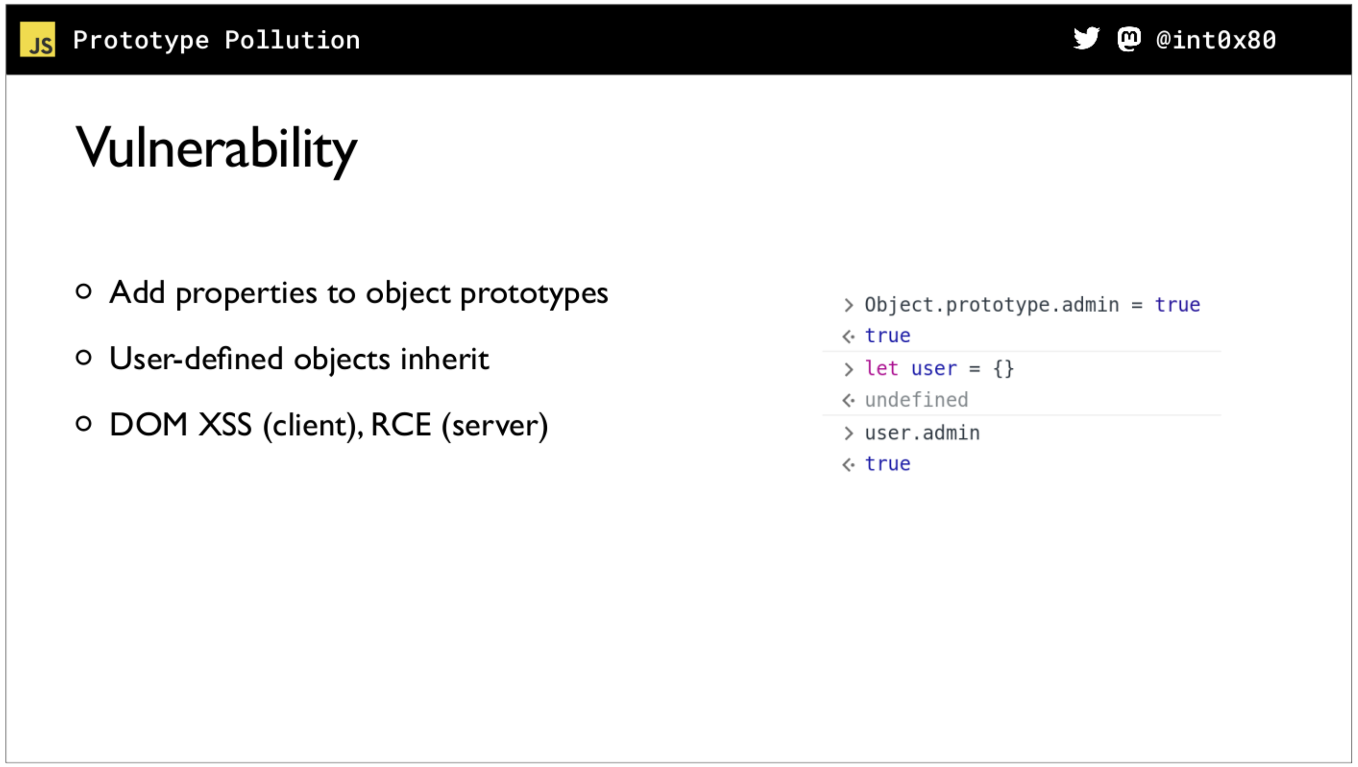
HOME > CVE > SEARCH RESULTS

### Search Results

There are **250** CVE Records that match your search.

| Name | Description |
|---|---|
| CVE-2023-38894 | A Prototype Pollution issue in Cronvel Tree-kit v.0.7.4 and before allows a remote attacker to execute arbitrary code via the extend function. |
| CVE-2023-3696 | Prototype Pollution in GitHub repository automattic/mongoose prior to 7.3.4. |
| CVE-2023-36665 | protobuf.js (aka protobufjs) 6.10.0 through 7.x before 7.2.4 allows Prototype Pollution, a different vulnerability than CVE-2022-25878. A user-controlled protobuf message can be used by an attacker to pollute the prototype of Object.prototype by adding and overwriting its data and functions. Exploitation can involve: (1) using the function parse to parse protobuf messages on the fly, (2) loading .proto files by using load/loadSync functions, or (3) providing untrusted input to the functions ReflectionObject.setParsedOption and util.setProperty. NOTE: this CVE Record is about "Object.constructor.prototype.<new-property> = ...;" whereas CVE-2022-25878 was about "Object.__proto__.<new-property> = ...;" instead. |
| CVE-2023-36475 | Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 5.5.2 and 6.2.1, an attacker can use a prototype pollution sink to trigger a remote code execution through the MongoDB BSON parser. A patch is available in versions 5.5.2 and 6.2.1. |
| CVE-2023-3186 | The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype. |
| CVE-2023-30857 | @aedart/support is the support package for Ion, a monorepo for JavaScript/TypeScript packages. Prior to version `0.6.1`, there is a possible prototype pollution issue for the `MetadataRecord`, when merged with a base class' metadata object, in `meta` decorator from the `@aedart/support` package. |

- No DVNA or Juice Shop???



## Vulnerability

- Add properties to object prototypes
- User-defined objects inherit
- DOM XSS (client), RCE (server)

```
> Object.prototype.admin = true
<· true
> let user = {}
<· undefined
> user.admin
<· true
```

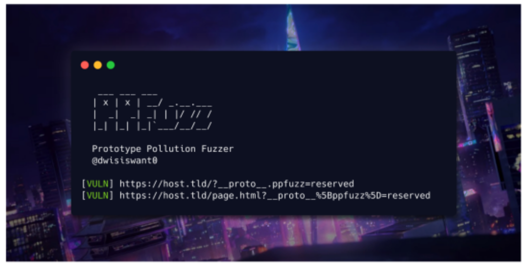
- Add arbitrary properties (and their values) to global object prototypes
- User-defined objects can then inherit those properties and values
- Client-side can be used to chain for DOM XSS
- Server-side can result in RCE and priv esc

# Demo

# Tooling

https://github.com/dwisiswant0/ppfuzz

https://github.com/kleiton0x00/ppmap

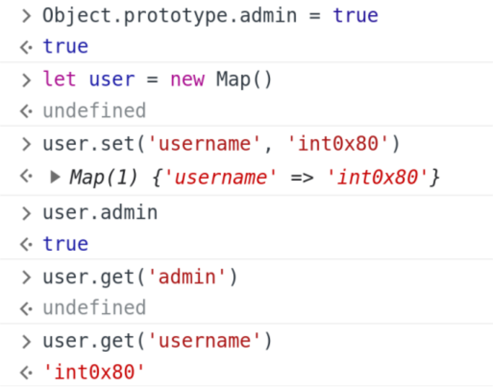


```
 ___ ___ ___
| x | x | __/ _.__.___
|  _|  _| _| | |/ // /
|_| |_| |_|`___/__/__/

Prototype Pollution Fuzzer
@dwisiswant0

[VULN] https://host.tld/?__proto__.ppfuzz=reserved
[VULN] https://host.tld/page.html?__proto__%5Bppfuzz%5D=reserved
```

- Only a few public tools
- Not aggressively developed/maintained
- Opportunity to write something better with more gadgets, or contribute PRs

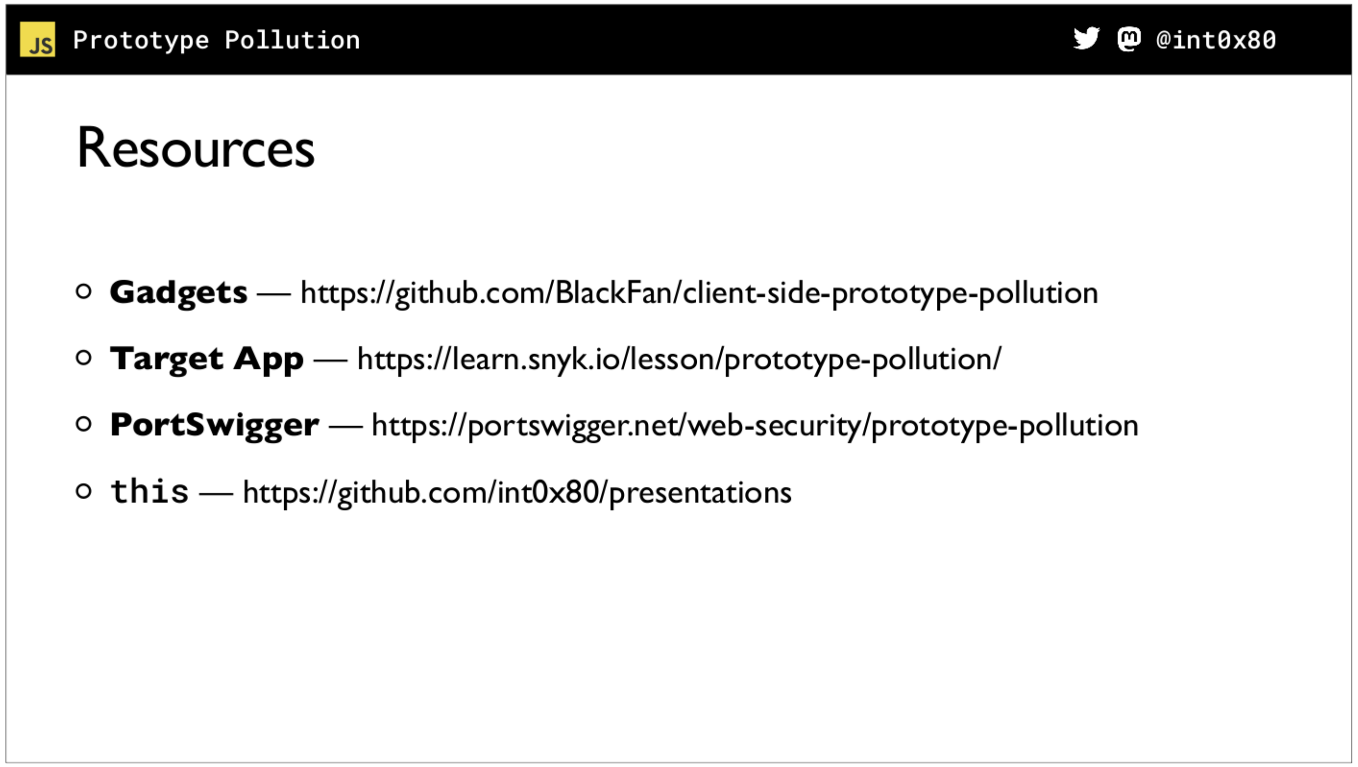
# Mitigation

- Patch/upgrade vuln libraries
- https://github.com/snyk-labs/nopp
- `Object.freeze()`
- Use `Map()` with `get()`
- Use `Set()` with `has()`



```
> Object.prototype.admin = true
< true
> let user = new Map()
< undefined
> user.set('username', 'int0x80')
< ▶ Map(1) {'username' => 'int0x80'}
> user.admin
< true
> user.get('admin')
< undefined
> user.get('username')
< 'int0x80'
```

- Patching: Evergreen vuln management advice
- nopp does Object.freeze() for you



# Resources

- **Gadgets** — https://github.com/BlackFan/client-side-prototype-pollution
- **Target App** — https://learn.snyk.io/lesson/prototype-pollution/
- **PortSwigger** — https://portswigger.net/web-security/prototype-pollution
- `this` — https://github.com/int0x80/presentations

- Folks doing it better than me