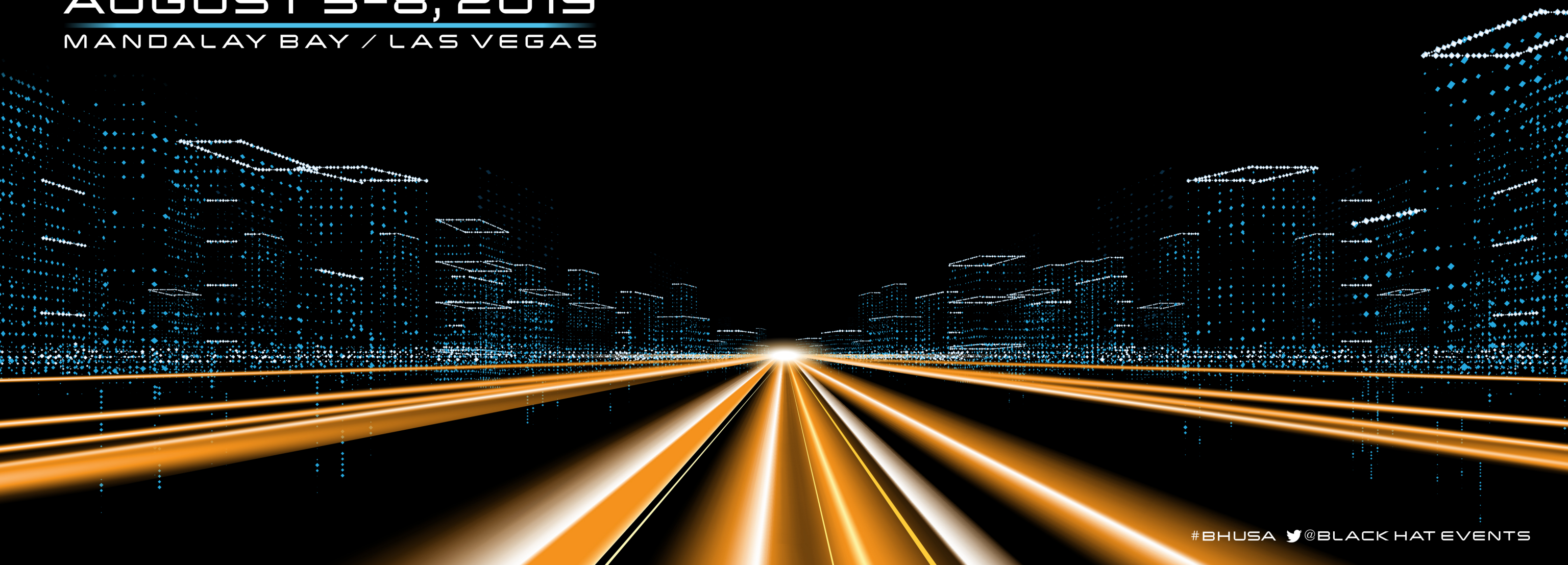




USA 2019

AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS



#BHUSA  @BLACKHATEVENTS

Electronegativity

Identify misconfigurations and security anti-patterns in Electron applications.

Lorenzo Stella @  Doyensec

Arsenal Station 1, August 7, from 4:00 pm to 5:20 pm

Try it now!

Available on:



<https://github.com/doyensec/electronegativity>

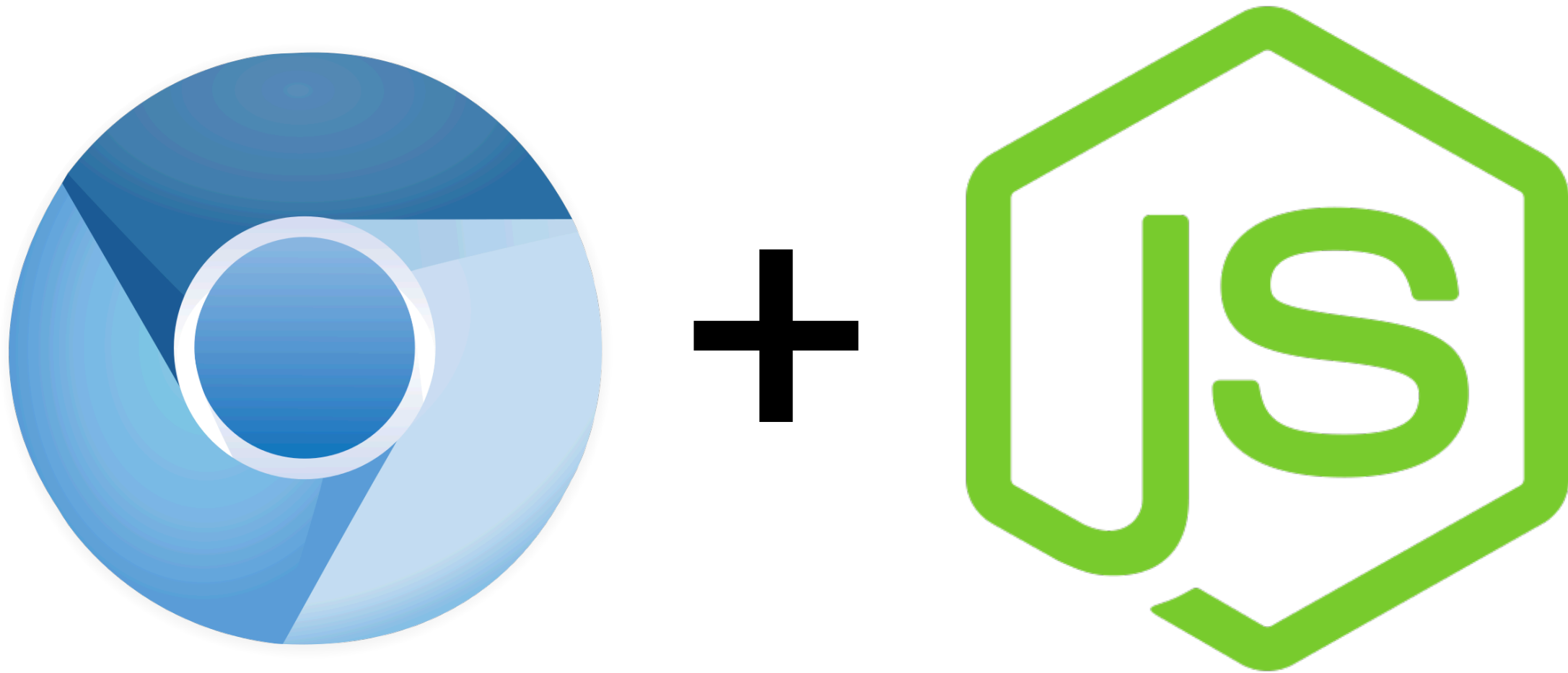


```
$ npm install @doyensec/electronegativity -g
```




Electron... *what?*

The Electron Stack





...and many others!

Security Audits on Electron Applications

- Large Attack Surface

Custom code, Dependencies, Electron Framework APIs and Foundation Libraries (Chromium/NodeJS)

- Rapidly Ever-Changing Framework Security

Frequent security patches, recent nodeIntegration bypasses or attacks, best webPreferences settings are always evolving.

- Lots of Things to Check

Electron Security Checklist by @ikkisoft, traditional web vulnerabilities, risky security anti-patterns, hardening best practices

How Do You Survive Through This?

Electronegativity can help you!

- Statically analyzes the code using AST and DOM parsing
- Looks for security-relevant Electron configurations
- Includes all the checks from the Electron Security Checklist wp (more than 40 and counting!)
- Checks if the Electron version used is vulnerable
- Suggests secure coding practices
- ...and much more!



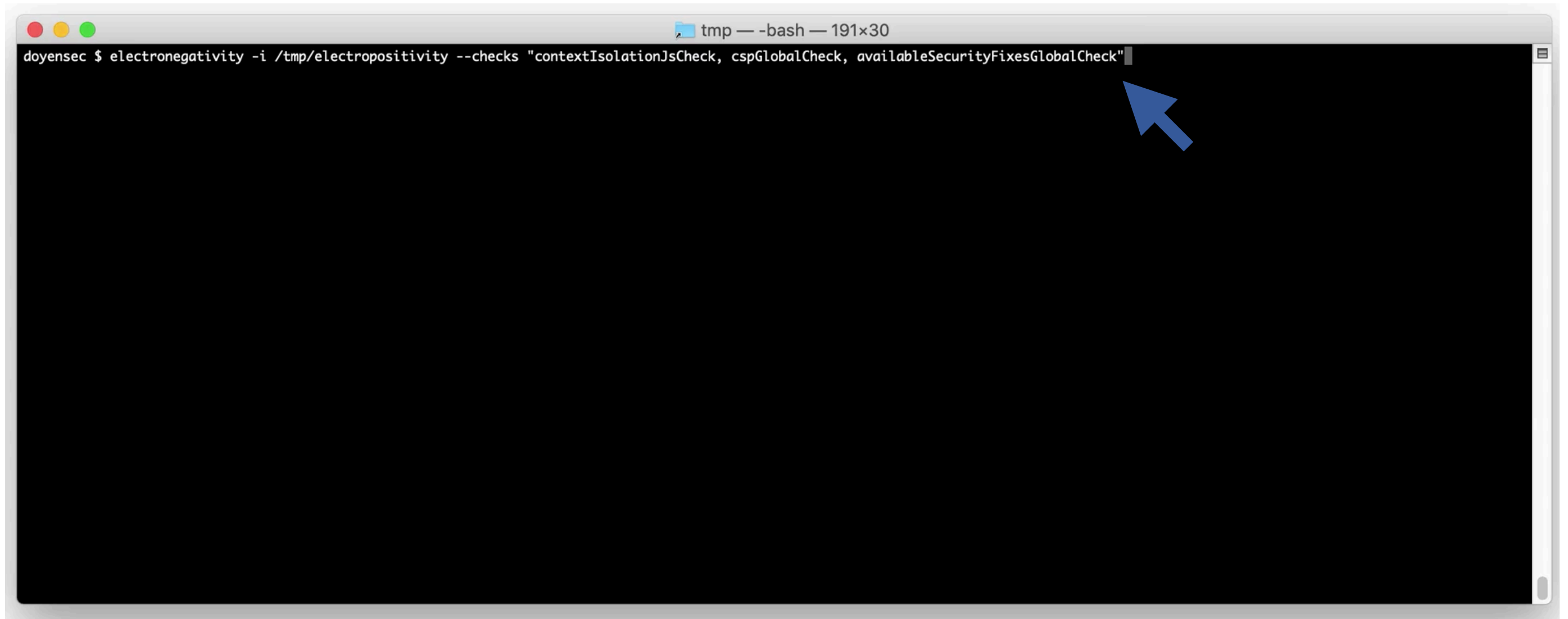
Usage

- Using it is as simple as pointing it to the repository directory or to the final .asar package.



```
electronegativity — -bash — 185x21
doyensec:electronegativity $ node dist/index.js -i /tmp/electropositivity/
```

Versatile Checks System



```
tmp — -bash — 191x30  
doyensec $ electronegativity -i /tmp/electropositivity --checks "contextIsolationJsCheck, cspGlobalCheck, availableSecurityFixesGlobalCheck"
```

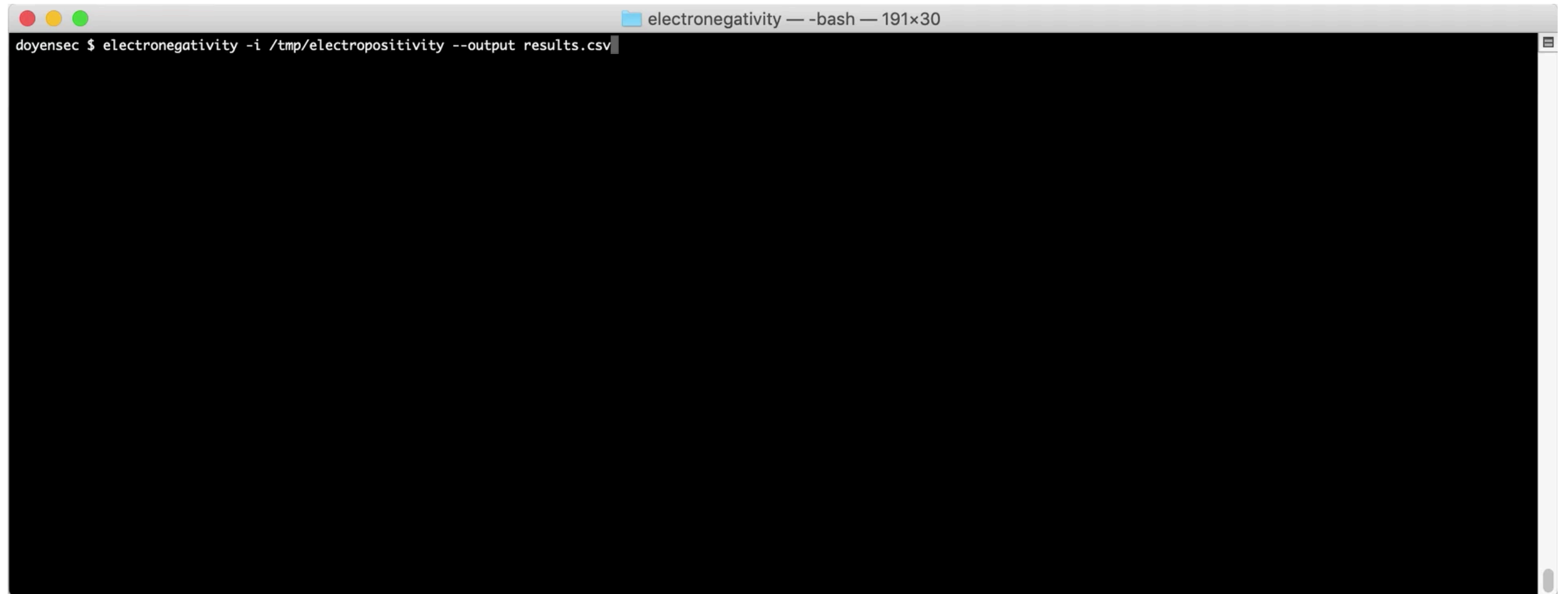
A screenshot of a terminal window with a dark background and light text. The window title bar shows 'tmp — -bash — 191x30'. The command entered is 'doyensec \$ electronegativity -i /tmp/electropositivity --checks "contextIsolationJsCheck, cspGlobalCheck, availableSecurityFixesGlobalCheck"'. A blue arrow points to the end of the command line.

Supported checks

- Affinity Global Check
- Allow Popup Check
- Auxclick JS/HTML Check
- Available Security Fixes Global Check
- Blink Features JS/HTML Check
- Certificate Error Event JS Check
- Certificate Verify Proc JS Check
- Context Isolation JS Check
- Custom Arguments JS/JSON Check
- CSP Global Check
- Dangerous Functions JS Check
- Electron Version JSON Check
- Experimental Features JS/HTML Check
- HTTP Resources JS/HTML Check
- Insecure Content JS/HTML Check
- Limit Navigation JS Check
- Node Integration JS/HTML Check
- Node Integration Attach Event JS Check
- Open External JS Check
- Permission Request Handler JS Check
- Preload JS Check
- Protocol Handlers JS Check
- Sandbox JS Check
- Security Warnings Disabled JS/JSON Check
- Web Security JS/HTML Check

...and more to
come!

CSV and Sarif Output Formats



```
electronegativity — -bash — 191x30  
doyensec $ electronegativity -i /tmp/electropositivity --output results.csv
```

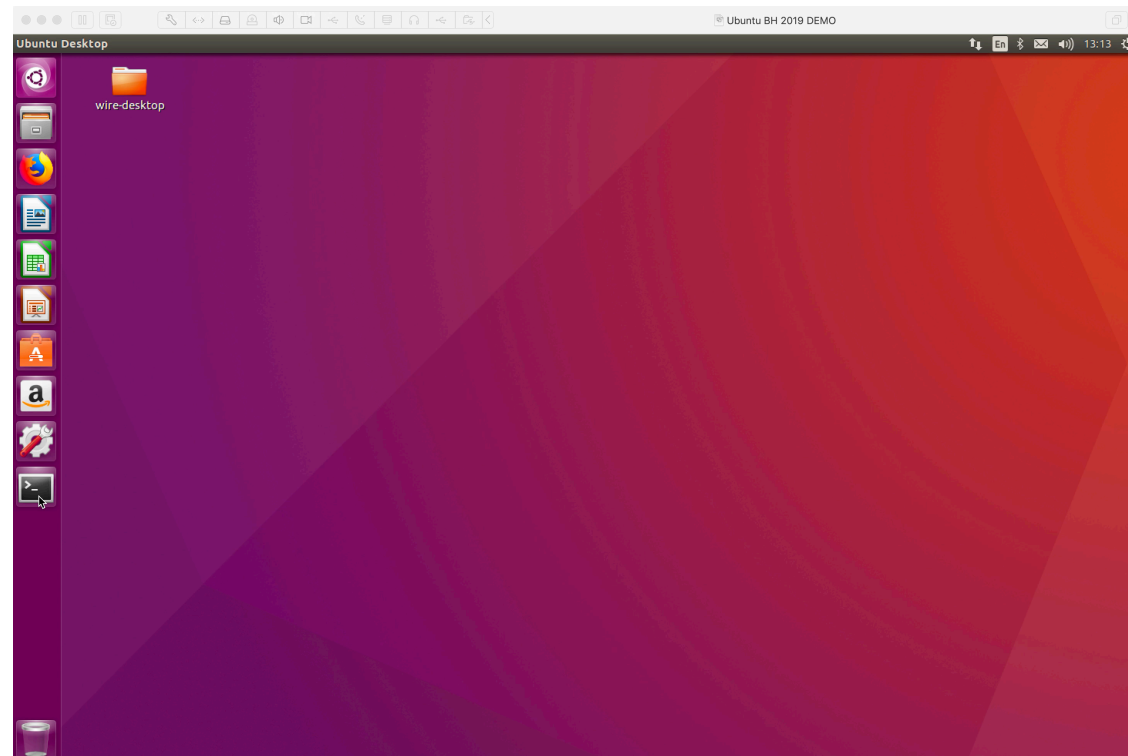
Demo Time: Electronegativity & Insecure Preload Detection



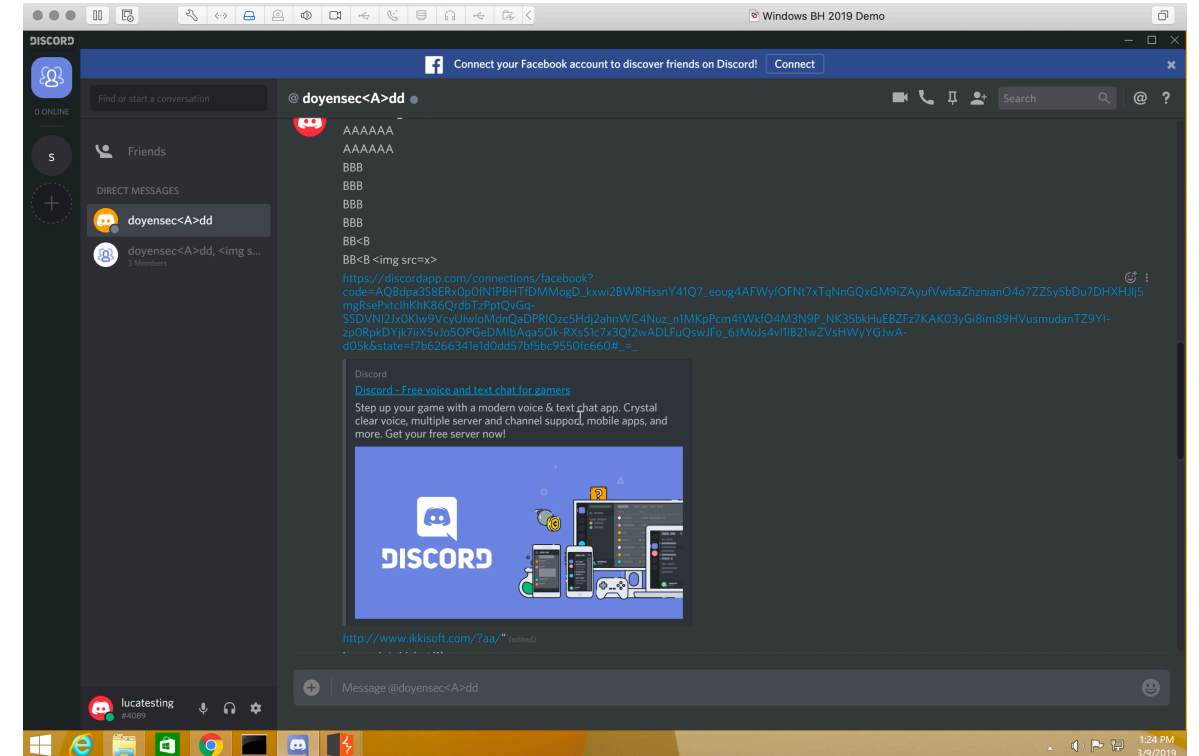
*Wire Arbitrary File Write
via Insecure Preload*

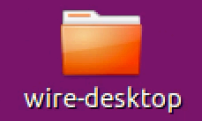


*Discord Arbitrary IPC
via Insecure Preload*



...Or





*Wire Arbitrary File Write
via Insecure Preload*



DISCORD

Connect your Facebook account to discover friends on Discord! [Connect](#)

Find or start a conversation

@ doyensec<A>dd

Search @ ?

0 ONLINE

Friends

DIRECT MESSAGES

doyensec<A>dd

doyensec<A>dd, <img s...
3 Members



AAAAAA

AAAAAA

BBB

BBB

BBB

BBB

BB<B

BB<B

https://discordapp.com/connections/facebook?code=AQBdpa3S8ERx0p0fN1PBHTfDMMogD_kxwi2BWRHssnY41Q7_eoug4AFWyfOFnt7xTqNnGQxGM9iZAyufVwbaZhznianO4o7ZZSy5bDu7DHXHJl5mgRsePxtclhKhK86QrdbTzPptQvGq-SSDVNI2Jx0Klw9VcyUlwoMdnQaDPRI0zc5Hdj2ahnWC4Nuz_n1MKpPcm4fWkfO4M3N9P_NK35bkHuEBZFz7KAK03yGi8im89HVusmudanTZ9YI-zp0RpkDYjk7iiX5vJo5OPGeDMIbAqa5Ok-RXsS1c7x3Qf2wADLFuQswJFo_6JMoJs4v1lB21wZVsHWyYGJwA-d05k&state=f7b6266341e1d0dd57bf5bc9550fc660#_=_

Discord

[Discord - Free voice and text chat for gamers](#)

Step up your game with a modern voice & text chat app. Crystal clear voice, multiple server and channel support, mobile apps, and more. Get your free server now!

<http://www.ikkisoft.com/?aa/> (edited)

Message @doyensec<A>dd

lucatesting #4089



Discord Arbitrary IPC via Insecure Preload

Electronegativity can help you detect this!
(thanks to a dedicated PRELOAD_JS_CHECK)



```
electronegativity — -bash — 182x23  
doyensec $ electronegativity -i wire-desktop/electron/ --checks=
```




Grab your
copy
today!

```
$ npm install @doyensec/electronegativity -g
```

Questions?
(lorenzo@doyensec.com)

