Installation

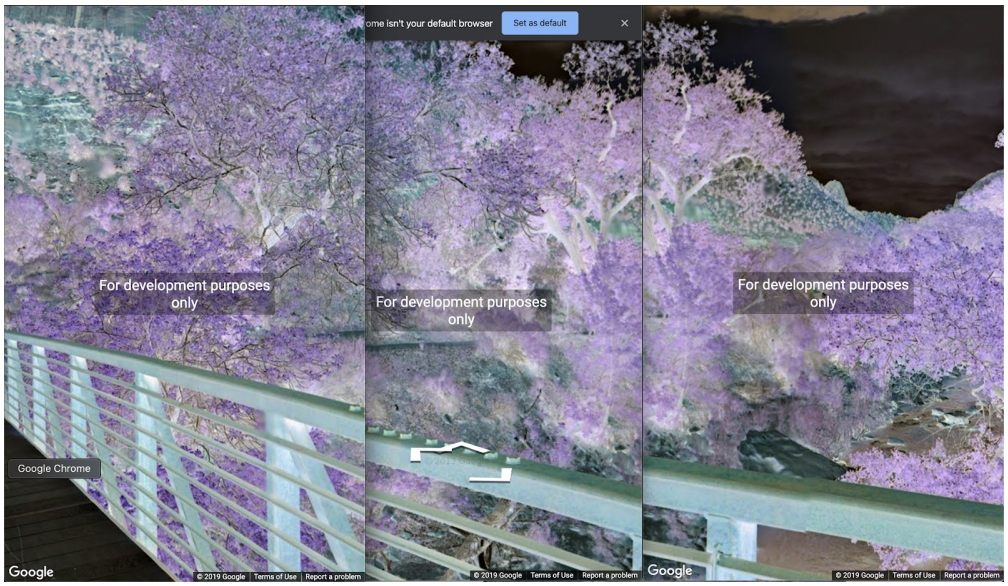
1. Go to https://nodejs.org/en/download/ and download the relevant version of node.js.
2. Go to the github and download/clone the repository to your computer.
3. Opening terminal, enter the directory where the code is located (for example, /Documents/lg-peruse-a-rue-master) and run the command `npm install`.

```
5. node
kripak@uwu-central ~ % cd Documents/gci/lg-peruse-a-rue-master
kripak@uwu-central lg-peruse-a-rue-master % npm install
npm WARN deprecated connect@2.30.2: connect 2.x series is deprecated

> ws@0.4.32 install /Users/kripak/Documents/gci/lg-peruse-a-rue-master/node_modu
les/ws
> (node-gyp rebuild 2> builderror.log) || (exit 0)

npm notice created a lockfile as package-lock.json. You should commit this file.
npm WARN lg-peruse-a-rue@0.6.4 license should be a valid SPDX license expression

added 125 packages from 102 contributors and audited 222 packages in 6.623s
found 23 vulnerabilities (12 low, 3 moderate, 8 high)
  run `npm audit fix` to fix them, or `npm audit` for details
```

4. Run the command `npm install`. If you open http://localhost:8086/display/?master=true in your browser, you should get this image or a similar one.

5. By opening http://localhost:8086/display/?yawoffset=-1 and http://localhost:8086/display/?yawoffset=+1 you can simulate the left and right screens in Liquid

Galaxy, respectively.



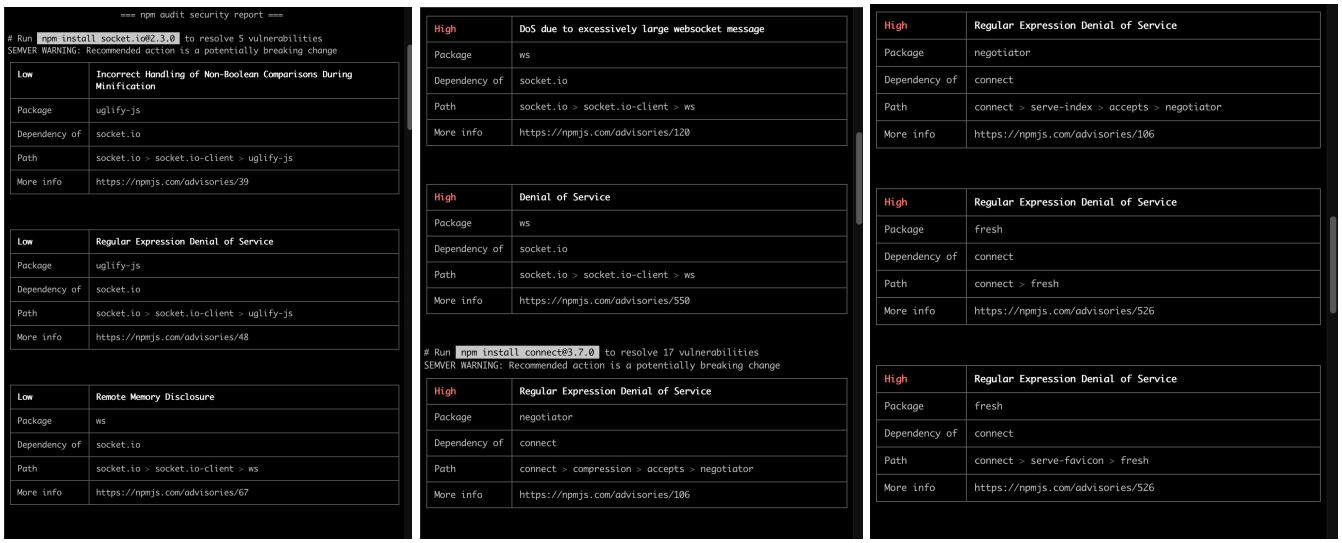
Findings

Before Auditing

Peruse-a-Rue was run in Firefox 71.0 and Chrome 79.0.3945.79. Installation took 5 minutes, as I already had node installed. There were no problems during the installation.

```
5. node
kripak@uwu-central ~ % cd Documents/gci/lg-peruse-a-rue-master
kripak@uwu-central lg-peruse-a-rue-master % npm install
npm WARN deprecated connect@2.30.2: connect 2.x series is deprecated

> ws@0.4.32 install /Users/kripak/Documents/gci/lg-peruse-a-rue-master/node_modu
les/ws
> (node-gyp rebuild 2> builderror.log) || (exit 0)

npm notice created a lockfile as package-lock.json. You should commit this file.
npm WARN lg-peruse-a-rue@0.6.4 license should be a valid SPDX license expression

added 125 packages from 102 contributors and audited 222 packages in 6.623s
found 23 vulnerabilities (12 low, 3 moderate, 8 high)
  run `npm audit fix` to fix them, or `npm audit` for details
```

However, there were vulnerabilities found.



```
=== npm audit security report ===

# Run  npm install socket.io@2.3.0  to resolve 5 vulnerabilities
SEMVER WARNING: Recommended action is a potentially breaking change
```

Low	Incorrect Handling of Non-Boolean Comparisons During Minification
Package	uglify-js
Dependency of	socket.io
Path	socket.io > socket.io-client > uglify-js
More info	https://npmjs.com/advisories/39

Low	Regular Expression Denial of Service
Package	uglify-js
Dependency of	socket.io
Path	socket.io > socket.io-client > uglify-js
More info	https://npmjs.com/advisories/48

Low	Remote Memory Disclosure
Package	ws
Dependency of	socket.io
Path	socket.io > socket.io-client > ws
More info	https://npmjs.com/advisories/67

High	DoS due to excessively large websocket message
Package	ws
Dependency of	socket.io
Path	socket.io > socket.io-client > ws
More info	https://npmjs.com/advisories/120

High	Denial of Service
Package	ws
Dependency of	socket.io
Path	socket.io > socket.io-client > ws
More info	https://npmjs.com/advisories/550

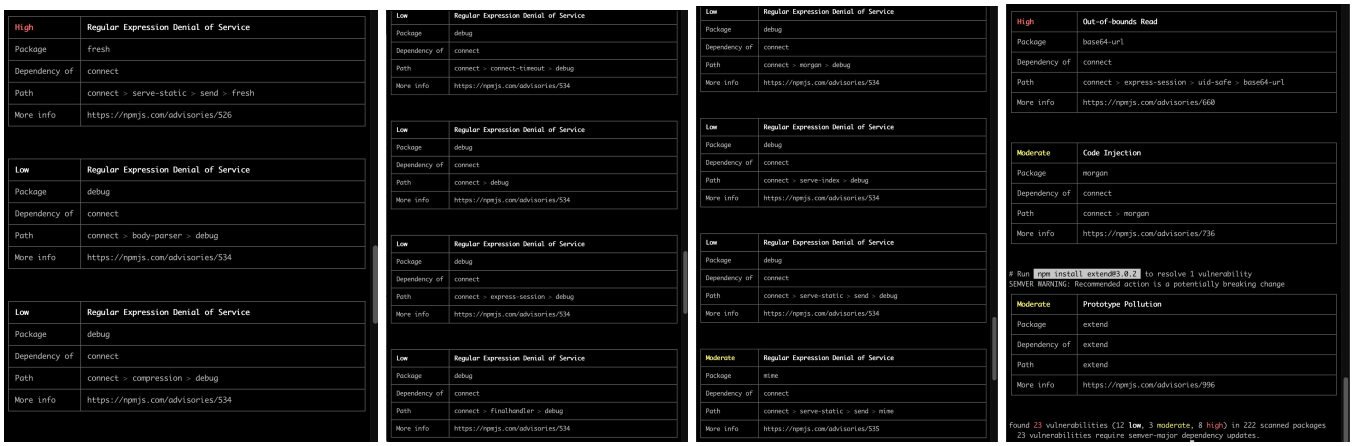
```
# Run  npm install connect@3.7.0  to resolve 17 vulnerabilities
SEMVER WARNING: Recommended action is a potentially breaking change
```

High	Regular Expression Denial of Service
Package	negotiator
Dependency of	connect
Path	connect > compression > accepts > negotiator
More info	https://npmjs.com/advisories/106

High	Regular Expression Denial of Service
Package	negotiator
Dependency of	connect
Path	connect > serve-index > accepts > negotiator
More info	https://npmjs.com/advisories/106

High	Regular Expression Denial of Service
Package	fresh
Dependency of	connect
Path	connect > fresh
More info	https://npmjs.com/advisories/526

High	Regular Expression Denial of Service
Package	fresh
Dependency of	connect
Path	connect > serve-favicon > fresh
More info	https://npmjs.com/advisories/526



High	Regular Expression Denial of Service
Package	fresh
Dependency of	connect
Path	connect > serve-static > send > fresh
More info	https://npmjs.com/advisories/526

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > body-parser > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > compression > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > connect-timeout > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > express-session > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > finalhandler > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > morgan > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > serve-index > debug
More info	https://npmjs.com/advisories/534

Low	Regular Expression Denial of Service
Package	debug
Dependency of	connect
Path	connect > serve-static > send > debug
More info	https://npmjs.com/advisories/534

Moderate	Regular Expression Denial of Service
Package	mime
Dependency of	connect
Path	connect > serve-static > send > mime
More info	https://npmjs.com/advisories/535

High	Out-of-bounds Read
Package	base64-url
Dependency of	connect
Path	connect > express-session > uid-safe > base64-url
More info	https://npmjs.com/advisories/660

Moderate	Code Injection
Package	morgan
Dependency of	connect
Path	connect > morgan
More info	https://npmjs.com/advisories/736

```
# Run  npm install extend@3.0.2  to resolve 1 vulnerability
SEMVER WARNING: Recommended action is a potentially breaking change
```

Moderate	Prototype Pollution
Package	extend
Dependency of	extend
Path	extend
More info	https://npmjs.com/advisories/996

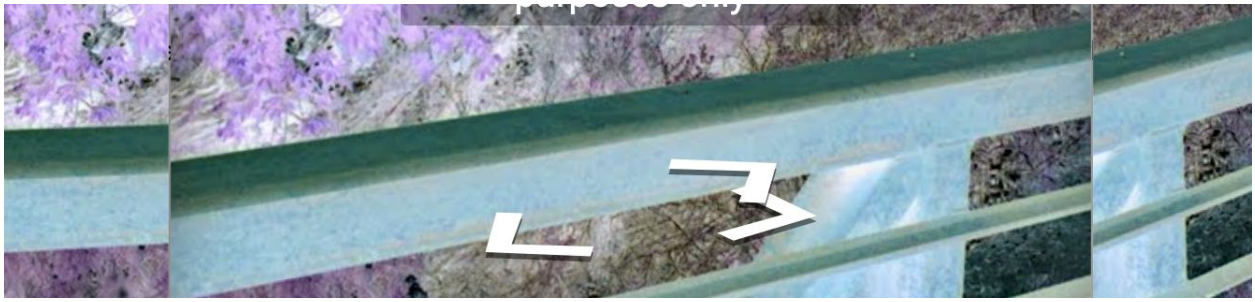
```
Found 23 vulnerabilities (12 low, 3 moderate, 8 high) in 222 scanned packages
  23 vulnerabilities require semver-major dependency updates.
```

All of them require semver-major dependency updates, so changes to the code will be required if updated. Most of the vulnerabilities lie in connect and socket, with 1 in extend. However, the application works fine without any updates. By examining the npmjs advisories page, I have found the following vulnerabilities.

Vulnerability	Problem	Recommended Solution
Incorrect Handling of Non-Boolean Comparisons During Minification	functioning of some Javascript may altered after minification	upgrade UglifyJS to version >= 2.4.24
Regular Expression Denial of Service	malicious inputs can be passed to parse()	upgrade UglifyJS to version >= 2.6.0
Remote Memory Disclosure	client.ping() can be manipulated to get sensitive data	upgrade ws to version >= 1.0.1
DoS due to excessively large websocket message	size of incoming websocket payloads not limited	upgrade ws to version >= 1.1.1

Denial of Service	crash when Sec-WebSocket-Extensions header containing Object.prototype property names as extension or parameter names is sent	upgrade ws to version >= 3.3.1
Regular Expression Denial of Service	malicious inputs can be passed	upgrade negotiator to version >= 0.6.1
Regular Expression Denial of Service	malicious inputs can be passed	upgrade fresh to version >= 0.5.2
Regular Expression Denial of Service	malicious inputs can be passed	upgrade debug to version >= 2.6.9 or 3.1.0
Regular Expression Denial of Service	malicious inputs can be passed	upgrade mime to version >= 2.0.3
Out-of-bounds Read	out-of-bounds read possible because uninitialized buffers allocated	upgrade base-64 to version >= 2.0.0
Code Injection	malicious inputs can be passed	upgrade morgan to version >= 1.9.1
Prototype Pollution	prototype of Object can be modified	upgrade extend to version >= 2.0.2 or 3.0.2

There was a slight delay between the windows, but that was likely to the network connection. I did, however see some offset between the windows.



Additionally, I tested the application in Firefox, Chrome, and Safari, all of which worked. The documentation states that it only works on Chromium, which is outdated.

After Auditing

Using `npm audit fix` was ineffective, so I had to use `npm audit fix --force`. However, this completely broke the app.

```
kripak@uwu-central lg-peruse-a-rue-master % node index.js
config INFO: file could not be imported, using defaults
/Users/kripak/Documents/gci/lg-peruse-a-rue-master/index.js:67
      .use( connect.static( docRoot ) )
                            ^

TypeError: connect.static is not a function
    at Object.module.exports.main (/Users/kripak/Documents/gci/lg-peruse-a-rue-m
aster/index.js:67:27)
    at Object.<anonymous> (/Users/kripak/Documents/gci/lg-peruse-a-rue-master/in
dex.js:115:18)
    at Module._compile (internal/modules/cjs/loader.js:776:30)
    at Object.Module._extensions..js (internal/modules/cjs/loader.js:787:10)
    at Module.load (internal/modules/cjs/loader.js:653:32)
    at tryModuleLoad (internal/modules/cjs/loader.js:593:12)
    at Function.Module._load (internal/modules/cjs/loader.js:585:3)
    at Function.Module.runMain (internal/modules/cjs/loader.js:829:12)
    at startup (internal/bootstrap/node.js:283:19)
    at bootstrapNodeJSCore (internal/bootstrap/node.js:622:3)
kripak@uwu-central lg-peruse-a-rue-master %
```