BUILDING SECURE ELECTRON APPLICATIONS

Naz Gayoom
@ngayoom
Agenda

- What is Electron
- Node Access
- Permissions
- The Webview Tag
- Demo
- A few other things...
- Q & A
What is Electron?

- A framework for building cross-platform desktop applications
Coffee with Alexandria was originally planned for tomorrow. I have 2 alternative suggestions:

1. This one is best:
   Tomorrow November 7 at 10:00am
2. This could work nicely:
   Tomorrow November 7 at 7:00am

- desktop option 1
- desktop option 2
- show in calendar
- cancel

Coffee with Alexandria
Tomorrow November 7 at 10:00am

Start a new conversation

Jason Stewart 2:22 PM
Thanks Johnny!

Message #culture
Access to Node.js

- Disable Node.js
- Use a preload script
- Don’t expose node handles on your preload scripts.
webPreferences: {
  nodeIntegration: false,
  preload: path.join(__dirname, 'preload.js')
}
Permissions handling

- HTML5 API: Geolocation, Camera, Microphone, Notifications
- Browser normally asks the user, electron does not
- We want to have custom validations.
const currentSession = mainWindow.webContents.session

currentSession.setPermissionRequestHandler((webContents, permission, callback) => {
    const resultOfSomeCondition = false;
    return callback(resultOfSomeCondition);
});
The `<Webview>` tag

- Has its own process and memory allocation
- Configurable like the browser window
- Always validate dynamically created Webviews
Local Content

External Content

Browser Window

The Webview Element
<body>
    <button onclick="getDirectory()">Get the directory from here...</button>
    <p id="list-of-directories"></p>
    <webview id="pineapple-machine"
        src=http://localhost:8080/ preload=./preload.js
        nodeIntegration></webview>
</body>
app.on('web-contents-created', (event, contents) => {
  contents.on('will-attach-webview', (event, webPreferences, params) => {
    webPreferences.nodeIntegration = false
  })
})
}
Demo...
A few other things...

- Using context isolation for JS global objects
- Allowing popups on a webview
- Mixed content (insecure content loaded on a securely loaded page)
- Setup a content security policy
Demo repo and other links

- https://slack.engineering/
- https://electronjs.org/docs/tutorial/security
WE ARE HIRING DEVELOPERS!
THANKS FOR LISTENING