

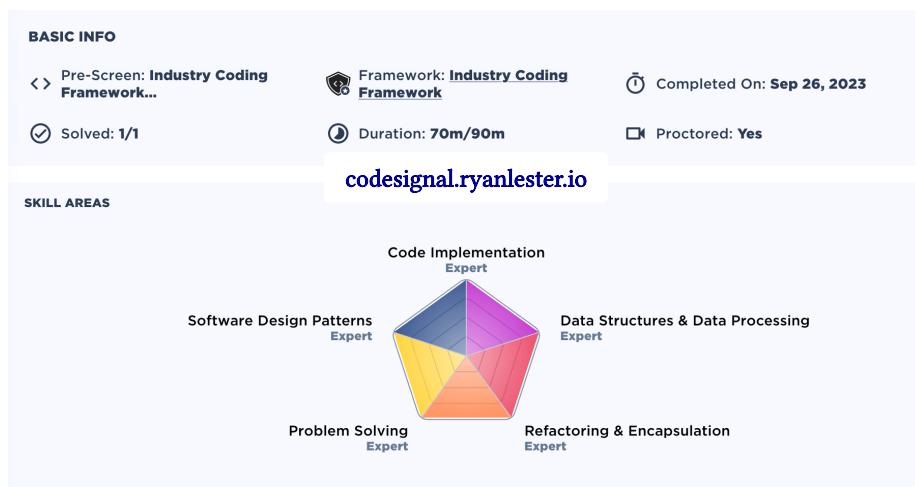
# RYAN LESTER

HACKER@LINUX.COM  
+1(337) 935 0016

Highly productive full-stack engineer and startup veteran  
with 15 years of experience and AppSec background

LINKEDIN.RYANLESTER.IO  
GITHUB.RYANLESTER.IO

## Programming Skill Assessment



## Skill Highlights

### Expert

TypeScript / JavaScript, Bash, Node.js, regex, crypto, GCP, Firebase, Angular, rxjs, webpack

### Proficient

Go, C#, Python, Java, SQL, React, Vue, AWS, Docker, CircleCI, nginx, Express, protobuf

## Education

**MACH37 Cyber Accelerator** 2014  
Curriculum focused on startups and business

**Carnegie Mellon University** 2010 – 2012  
Intended Computer Science major (left early)

**Certifications** 2009  
Microsoft Certified Systems Administrator, et al.

## Employment History

- Cyph** *Principal Engineer* [github.com/cyph](https://github.com/cyph) • [cyph.com/castle-platform](https://cyph.com/castle-platform) • [cyph.com](https://cyph.com) 2014 – Present  
Developed the Cyph tech stack and product suite
- **Cyph:** Quantum-resistant end-to-end encrypted super-app (*TypeScript, JS / Node.js, Go, Angular, Cordova, Electron*)
    - Cross-platform suite of easy-to-use messaging, video meeting, social media, storage vault, and crypto wallet functionality
    - Combines the advantages of user-friendly non-E2EE apps and secure E2EE apps, while further improving security
  - **WebSign:** Static website host with patented end-to-end client-side security (code signing) (*TypeScript, JS / Node.js*)
    - Significantly enhances Cyph's user experience by allowing it to run as a web app, which would otherwise break its security model
    - Standalone product builds on core tech with a cloud service and developer CLI tooling, opening a significant new revenue stream
  - **Castle:** Friendly real-time database and messaging API with automatic private data encryption and public data signing (*TypeScript*)
    - Builds on Firebase with zero-knowledge security model and developer experience enhancements (e.g. support for complex types)
  - **Air Gapped Signing Environment:** Highly secure certificate authority for Castle and WebSign (like a hardware wallet) (*JS / Node.js*)
    - Uses keys from encrypted cold storage to perform signing over temporary unidirectional fiber optic UDP networks
  - Built on GCP (App Engine, Cloud Functions, Compute Engine, Datastore, Firebase, Storage) and AWS (SES; also previously used SQS)
- HackerOne / PullRequest** *Code Reviewer & Security Auditor (part-time)* [hackerone.com](https://hackerone.com) 2022 – Present  
Reviewer for projects in a variety of tech stacks, including Bash, C#, Java, Node.js, Python, React, Ruby, Rust, Solidity, Swift, and Vue; often #1 on the leaderboard, with findings typically including security flaws and significant cleanup and optimization opportunities
- PlusMinus** *Full-Stack Developer (fixed-term)* [plusminus.ryanlester.io](https://plusminus.ryanlester.io) 2019  
Added features to an Angular/React/ASP.NET application for a Fortune 100 client, focusing on pixel perfection with Figma design specs
- SpaceX** *Software Design Engineer in Test* [spacex.com](https://spacex.com) 2012 – 2013  
Built automation that enabled small QA/DevOps team to support a large dev team for SpaceX and Tesla's internal ERP system, Warp Drive
- **Holodeck:** Integrated test recorder and powerful web UI testing framework (*C# / .NET, HTML / CSS / JS, Selenium, TFS*)
    - High-level DSL made generated code easy to read and maintain, with advanced features such as concurrent test composition
    - Recorder UI polished by months of user testing, handling everything up through check-in to version control
    - Allowed entire team to contribute tests, rapidly scaling up coverage
  - **Starfleet:** Distributed testing system (*C# / .NET, Redis, Selenium Grid*)
    - Handled load balancing, dynamically spinning up infrastructure, and coordination between test agents
    - Dramatically sped up CI, which had become slow due to all the new tests, and added load testing as a side effect
  - **Holodeck Macros:** Windows GUI tool to run tests with the local user's account and leave browser open (*PowerShell / .NET, WPF*)
    - Used by business analysts to automate the setup for complex manual functional testing scenarios
  - My products saved millions in potential wasted factory floor time by catching major regressions pre-production
  - Productivity ranked in top 5% during performance review
- ComVibe** *Software Developer (part-time)* [comvibe.com](https://comvibe.com) 2010 – 2011  
Helped develop property management startup MVP with CodeIgniter, MySQL, PHP, and HTML/CSS/JS
- Robin Hood Camp** *Counselor & Reports Director (seasonal)* [robinhoodcamp.com](https://robinhoodcamp.com) 2008 – 2010  
Taught chess and Rubik's Cube (my record was 26 seconds); developed simple administrative software in FileMaker Pro

## Talks

- HackerOne Security@** *"Lessons Learned in the Race to Secure Open Source"* [securityat.ryanlester.io](https://securityat.ryanlester.io) 2022  
Discussed open source software security topics, the role of organizations, and potential future ecosystem developments
- W3BX** *"Building a Secure Bridge from Web2 to Web3 is a Fundamental Infrastructure Investment for the Ecosystem"* [w3bx.ryanlester.io](https://w3bx.ryanlester.io) 2022  
Walked through WebSign and the critical need for it in the crypto/web3 space to enable user-friendly self-custody solutions
- TechCrunch Disrupt** *Off-the-record Privacy & Security panel* [tcdisrupt.ryanlester.io](https://tcdisrupt.ryanlester.io) 2017  
Spoke on various privacy and security topics, including predictions on future industry and regulatory developments
- Black Hat & DEF CON** *"Abusing Bleeding Edge Web Standards for AppSec Glory"* [bhdc.ryanlester.io](https://bhdc.ryanlester.io) 2016  
Demoed novel web security techniques, supercookie, and "RansomPKP" attack concept, which ultimately led to the deprecation of HPKP
- Georgetown University** *"Crypto In Security"* 2016  
Guest lecture on applied cryptography to Professor Hans Engler's undergraduate Intro to Cryptography course

## Patents

- Cyph Portfolio** *Principal Inventor* [patents.ryanlester.io](https://patents.ryanlester.io) 2015 – Present  
Led the creation of a highly valuable portfolio of 15 issued patents which advanced the state of the art in secure usability of cryptography

## Projects

### 🔑 Security

- pqcrypto.js** *Author (open source)* [pqcrypto.ryanlester.io](https://pqcrypto.ryanlester.io) 2022 – Present  
Suite of NIST PQC quantum-resistant cryptographic algorithms for WebAssembly, built with JavaScript, C, Bash, and emscripten
- libsodium.js** *Co-Author (open source)* [sodium.ryanlester.io](https://sodium.ryanlester.io) 2017 – Present  
Official WebAssembly version of the extremely popular cryptographic library libsodium, built with JavaScript, C, Bash, and emscripten
- Bug Bounties** *Hacker* 2016  
Discovered Google Chrome vulnerabilities CVE-2016-1636 (SRI bypass, high severity) and CVE-2016-1694 (HPKP eviction, low severity)
- Stripe: Capture the Flag** *Winner (one of 250, out of 12k participants)* [stripectf.ryanlester.io](https://stripectf.ryanlester.io) 2012  
CTF competition to root a server; involved buffer overflows (C / assembly), validation failures (C / Bash, PHP, Python), and a timing attack (C)

### 🌐 Web

- emscripten** *Contributor (open source)* [emscripten.ryanlester.io](https://emscripten.ryanlester.io) 2017 – Present  
Developed the SINGLE\_FILE flag, which has made WebAssembly viable for many use cases; built with Python and JavaScript
- Repl.co** *Author* 2013 – 2016  
Collaborative C# code editor with in-browser execution, built with Firebase and JSIL; gifted the domain to Amjad Masad for Replit
- Napster.fm** *Author (open source)* [techcrunch\\_napsterfm.ryanlester.io](https://techcrunch_napsterfm.ryanlester.io) • [napsterfm.ryanlester.io](https://napsterfm.ryanlester.io) 2013 – 2014  
Social music streaming service with real-time sync, internationalization, and over 100k users; built with AngularJS, Bootstrap, and Firebase
- html-resume** *Author (open source)* [htmlresume.ryanlester.io](https://htmlresume.ryanlester.io) 2012 – Present  
HTML framework used to create this document, built with CSS, Node.js, Puppeteer, and pdf-lib (originally Bash, wkhtmltopdf, and pdftk)

### 💰 Finance

- simplebtc** *Author (open source)* [simplebtc.ryanlester.io](https://simplebtc.ryanlester.io) 2014 – Present  
High-level Bitcoin wallet API for browsers and Node.js, initially spun out of Token and currently used in Cyph
- YC Hacks: Token** *Team Member* [yhacks.ryanlester.io](https://yhacks.ryanlester.io) 2014  
Bitcoin debit card created for Y Combinator hackathon, built with Selenium, Coinbase, Blockchain.info, Node.js, and the iOS SDK
- Algorithmic Trading** *Author* 2013 – 2014  
Experimentation with various machine learning approaches for trading stocks and forex, built with C#, Node.js, and the TradeStation API
- Hackswipe** *Author* 2010  
Mobile point of sale system with SMS support, built using Python, Perl, and jQuery UI; awarded "best mobile app" at Yahoo! Hack Day

### 🌍 Misc

- cordova-plugin-chooser** *Author (open source)* [chooser.ryanlester.io](https://chooser.ryanlester.io) 2020 – Present  
Android- and iOS-compatible Cordova plugin for importing files, adopted by Ionic Native; built with Java and Swift
- @cyph/prettier** *Author (open source)* [prettier.ryanlester.io](https://prettier.ryanlester.io) 2019 – Present  
A custom fork of the prettier code formatter which improves ternary readability and aligns with pre-existing Cyph style conventions
- Sundown.go** *Author (open source)* [sundown.ryanlester.io](https://sundown.ryanlester.io) 2011  
Markdown parser library for Go, built using Go, C, and Cgo to bind to a C implementation
- Relationship Advice** *Founder* [relationshipadvice.ryanlester.io](https://relationshipadvice.ryanlester.io) 2009 – Present  
Started an online community on reddit and helped grow it to over 10 million users