

RYAN LESTER

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

Highly experienced full-stack engineer and startup veteran
Perfect score on CodeSignal Industry Coding Framework — codesignal.ryanlester.io

P.O. Box 3402
McLEAN, VA 22103

Employment History

WebSign	<i>Cofounder & CTO (lead developer)</i>	2022 – Present
WebSign is a patented static website host with end-to-end client-side security (code signing) — websign.app		
HackerOne / PullRequest	<i>Security Auditor / Code Reviewer</i>	2022 – Present
I review code in various languages and frameworks, including web/mobile apps, smart contracts, and shell/container scripts; I've received many positive ratings, with my findings often including security flaws and significant optimization opportunities		
PlusMinus	<i>Full-Stack Developer</i>	2019
Added features to an Angular/React/.NET application for a Fortune 100 client, focusing on pixel perfection with Figma design specs		
Cyph	<i>Cofounder & CEO (lead developer)</i>	2014 – Present
Cyph is a patented user-friendly quantum-resistant end-to-end encrypted messenger — cyph.com		
<ul style="list-style-type: none">Responsibilities include: architecture, DevOps, engineering, project planning, QA, support, general company operations/managementTech stack includes: Angular, AWS, Bash, Bitcore, C, CircleCI, Cordova, Docker, Electron, Firebase, Go, Google Cloud, IndexedDB, IPFS, Java, msgpack, Node.js, prettier, protobuf, Python, rxjs, SCSS, Swift, TypeScript, UDP, Web Crypto, webpack, WebRTC, Workers		
SpaceX	<i>Software Design Engineer in Test</i>	2012 – 2013
Built web UI testing stack for internal ERP software Warp Drive: rapidly scaled up test coverage with integrated test recorder UI and clean C# code generation, optimized CI using Selenium Grid and Redis, and increased utility with PowerShell/WPF test runner GUI		
Robin Hood Camp	<i>Counselor & Reports Director</i>	2008 – 2010
Taught chess and Rubik's Cube (my record was 26 seconds); developed simple administrative software in FileMaker Pro		

Talks

HackerOne Security@	<i>"Lessons Learned in the Race to Secure Open Source"</i>	2022
Discussed open source software security topics, the role of organizations, and potential future ecosystem developments		
W3BX	<i>"Building a Secure Bridge from Web2 to Web3 is a Fundamental Infrastructure Investment for the Ecosystem"</i>	2022
Walked through WebSign and the critical need for it in the crypto/web3 space to enable user-friendly self-custody solutions		
TechCrunch Disrupt	<i>Off-the-record Privacy & Security panel</i>	2017
Spoke on various privacy and security topics, including predictions on future industry and regulatory developments		
Black Hat & DEF CON	<i>"Abusing Bleeding Edge Web Standards for AppSec Glory"</i>	2016
Demoed novel web security techniques and the "RansomPKP" attack concept, which ultimately led to the deprecation of HPKP		

Projects

libsodium.js	<i>Co-Author (open source)</i>	2017 – Present
Official JavaScript/WebAssembly version of the widely used libsodium cryptographic library		
pqcrypto.js	<i>Author (open source)</i>	2015 – Present
Suite of quantum-resistant cryptographic algorithms for JavaScript/WebAssembly (primarily NIST PQC selections)		
Napster.fm	<i>Author (open source)</i>	2013 – 2014
Social music streaming service with real-time synchronization and around 100k users that was featured on TechCrunch		
Stripe: Capture the Flag	<i>Winner (one of 250, out of 12k participants)</i>	2012
CTF competition to root a Linux server; vulnerabilities I exploited include buffer overflows, validation failures, and a timing attack		

Patents

9,794,070	Method of ephemeral encrypted communications
9,906,369	System and method of cryptographically signing web applications
9,948,625	Encrypted group communication method
9,954,837	Method of multi-factor authentication during encrypted communications
9,961,056	Method of deniable encrypted communications
10,003,465	System and method of encrypting authentication information
10,020,946	Multi-key encryption method
10,103,891	Method of generating deniable encrypted communications via password
10,419,223	Method of using symmetric cryptography for sign-on authentication
10,491,399	Cryptographic method for secure communications

Education

MACH37 Cyber Accelerator	2014
Three-month MBA-style curriculum	
Carnegie Mellon University	2010 – 2012
Intended Computer Science major (incomplete)	
Certifications	2009
Microsoft Certified Systems Administrator, et al.	

CVEs

CVE-2016-1636	<i>Severity: High</i>	2016
Subresource Integrity bypass in Chrome		
CVE-2016-1694	<i>Severity: Low</i>	2016
HTTP Public Key Pinning eviction in Chrome		