# Jay Patel

jpatelapple1@gmail.com
609-510-6558
Berea, OH

## Summary

Passionate Reverse Engineering and Cybersecurity enthusiast with hands on experience analyzing client-side security systems, deobfuscating JavaScript, and researching bot detection techniques. Skilled in tools such as Ghidra, Babel AST, Burp suite and Frida, with a strong foundation in computer systems, networking, and software development. Driven by curiosity to understand how technology works under the hood and committed to building secure, efficient systems.

---

## Experience

### Software Engineer

Metrosmoke • Brookpark, OH
06/2024 - Present
Created and deployed a POS system that integrates with Shopify to manage and update products in real time, pricing, quantity, mutation of the product. Developed a warehouse order-picking application, customer management tools, and email marketing automation. Experienced in handling multiple roles, focusing on front-end development and team collaboration. Implemented automated CI/CD structures using Git and Docker.

### Network Engineer

Oxheberg LLC • Remote
01/2023 - 06/2024
My first ever experience into my computer science journery, with the incredible team and support I learned how to manage KVM virtualization, and managed iptables configurations to mitigate DDoS and unauthorized cryptocurrency mining attempts on production servers.

---

## Skills

Reverse Engineering, AST Manipulation with Babel to deobfuscate code, With frida - Experience pentesting apks

---

## Education

### B.S. in Computer Science (Cybersecurity Focus)

Ohio State University • Columbus, OH
06/2027
Undergraduate in Computer science with major focus on cyber security, protecting against bot traffic. Currently taking remote classes for Software I & II and Linear Algebra.

---

## Projects

My skills have been honed through hobby projects and small professional engagements that deepened my passion for bot detection.

Imperva's Incapsula: A pure JS based challenge from imperva's team, they focused a bit more on obfuscating their client sided js code, which I was able to deobfuscate with Babel AST.  After doing this I was able to understand how their payload was constructed and able to sandbox this into JSDOM, TLS Fingerprinting, Proxy rotation, and multiple different canvas, and webgl fingerprinting collected from real devices being shuffled I was able to penetrate and able to create successful reese84 clearance cookies.

Human Security's Perimeter X: I have been working on this for few weeks and learned a lot more new skills and techniques they employ. Their implementation is much more advanced and harder than any other I have tried to solve, they focus more on the behavior aspect of detection, which includes mouse movements, webgl, font fingerprinting, audio fingerprinting, your timing

also has to be perfect and a lot more. In the end you are given a px3 token which can be used to check if you are blocked or passed. Which then released additional interrogation of client their famous, Hold Captcha which is much more aggressive and harder involving WASM based puzzle, and more mouse movements recording.

Both of these projects have been open sourced or show casing my skill set, for PX only the deobfuscator opened sourced the generator is private as its not finished - though imperva could be outdated as the cat and mouse game advances. I have done more projects related to RE, but under NDA I cannot show but can briefly talk.

Links :

https://github.com/00Prime/perimeterx-deobfuscator

https://github.com/00Prime/incapsula-solver