Charlotte Som

Systems programmer, videogame cheat developer, reverse engineer, multispecialist.

✉ charlotte@som.codes 🜋 @char 🔗 char.lt 🔗 hackery.site

Competitions

Google Hash Code 2020   *Google*

📅 *February 2020*

Worldwide intractable problem optimization competition. Competed as part of a globally-distributed team of three.

- **UK**: 6th place out of 406 teams.
- **USA**: 13th place out of 619 teams.
- **Canada**: 3rd place out of 135 teams.
- **Worldwide**: 252nd place out of 10724 teams.

Deloitte UK CTF   *Deloitte*

📅 *December 2020* 📍 London

UK-wide infosec competition, organised by Deloitte. Participated as a university team of six.

- **Qualifiers**: 10th place.
- **London finals**: 7th place.

BLÅHAJ CTF Team

📅 *2021 – Present*

Casual infosec competition team:

- **Hack-A-Sat 2 CTF**: Organised by the *US Air Force & US Space Force*. Placed 15th out of 697 teams.
- **corCTF 2021**: Placed 11th out of 904 teams.

Writing

"Circumventing the JVM Classfile Verifier"

🔗 *som.codes/jvm-force-no-verify*
📅 *2019*

"Reverse Engineering GTA V's Stunt Jumps"

🔗 *hackery.site/writing/gta-v-stunt-jumps*
📅 *2021*

"Circumventing Cisco Duo's Authenticator App"

🔗 *som.codes/cisco-duo-bypass*
📅 *2021*

"Extracting API Keys from a Minecraft Launcher"

🔗 *som.codes/mmc-msaclientid*
📅 *2022*

Experience

Multiplayer game technology   *WorldQL Corporation*

📅 *April 2022 – Present*

I currently work at WorldQL, building technology to reduce the barrier between singleplayer and multiplayer game development techniques.

The work is varied and has involved machine learning models, image processing pipelines, high-performance networking software, and 3D programming.

I mainly work with **Rust**, **TypeScript**, **Python**, **PyTorch**, **CUDA**, and **ONNX**.

Game modding / game-hacking   *Self-employed*

📅 *2016 – Present*

- *GTA Online*: **C++**, Rust
- *Minecraft*: **Java**, Kotlin, Scala, JVM Bytecode
- *Counter-Strike: Global Offensive*: **C++**, Rust
- *Various Unity3D*: **C#**, .NET MSIL, C++ (for il2cpp games)

Professionally, I used to sell a custom client for Minecraft (5-figure USD revenue from 2016 – 2019), and a subscription trainer menu for GTA Online (4-figure annually recurring USD revenue until 2020).

Commercial obfuscator for JVM programs

paramorphism.dev (Self-employed)

📅 *2017 – 2022*

Java bytecode is one of my specialist areas.

Involved writing the product itself and internal tooling around JVM bytecode to aid debugging. Working primarily with **Kotlin** and **Java**.

- *Paramorphism*: Bytecode obfuscator for JVM programs written in **Kotlin**.
- *libparamorphism*: Optional native runtime opaque library for programs obfuscated by Paramorphism written in **Zig** and **Rust**.
- *Koffee*: Domain-specific language for **Kotlin** for Java classfile generation.
- *Aksara* (internal): Bytecode assembly language and assembly/disassembly toolchain written in **Kotlin**.
- *Katon* (internal): Bytecode viewer and editor with a GUI written in **Rust** and interfacing via **Java Native Interface** to **Kotlin** (*Aksara*) and **Java** (*Fernflower*).

"Splashforce"   *Force Software LLC*

📅 *November 2020 – October 2021*

At Force Software, I was a "Software developer and strategy coordinator". The flagship "Splashforce" product is an end-user e-commerce automation suite for various sneaker sites. My duties included:

- cronet: Custom patches for & isolation of Chromium's HTTP stack. (To evade TLS fingerprinting.)
- Pairing an Electron (node.js / web **JavaScript**) frontend to a **Go** backend.
- Anti-piracy, reverse-engineer-deterrent releases for the **Go** backend. (Code virtualization, cgo FFI bindings, etc.).
- Reverse engineering bot protection measures on websites.
- Reverse engineering & circumventing bot prevention measures on Android apps. (**Java**, **Smali**, etc).