Timur Bairamukov

Email: job_bairamukov@mail.ru   **GitHub**: github.com/inagen   **HTB**: inagen#93334   **Phone**: +7(928) 923-2216

Education		
	ITMO University	St. Petersburg, Russia
	Applied mathematics and computer science	2019 − 2023
	SPbCTF reverse engineering course	2021
	SPbCTF pwn course	2021 - 2022

Work experience

C++ researcher and developer in EPAM   February 2022 - Current day
- Wrote a benchmark library and used it for optimizing some projects.
- Wrote a tool for debugging multiprocessor systems.
Technologies used: C++, intrinsics .

Java backend developer in Yandex   April - July 2021
- Added synchronisation of the state of several databases with user info so that data is the same in all of them.
- Optimized query processing by merging same methods and database queries into one.
Technologies used: Java 11, Spring, PostgreSQL, Docker.

Gamedev intern in Saber Interactive   January - April 2021
- Developed tools and methods for graphics engine, fixed bugs in legacy code.
- Developed multi-threaded graph of jobs and used it for rendering pipeline.
Technologies used: C++, OpenGL

Educational Projects

Bidirectional map   2020
A bimap is a data structure that stores a set of pairs and efficiently searches for a key by value. Unlike map, bimap searches can be performed both on the left elements of pairs, and on the right.

Variant   2021
The class template variant represents a type-safe union

Mandelbrot set   2021
Simple interactive visualization of the mandelbrot set.

Dll-injector   2020
Simple DLL-injector written on C++ using WinAPI.

Simple obfuscator   2020
Obfuscator, that creates the new executable containing obfuscated content of input file. During startup, the new executable creates a separate process containing the contents of the old executable. This solution helped bypass most of the antiviruses on the virustotal website.

HackTheBox machines   2022

Over the past week I have solved the following machines:

- Paper (easy)
- Timelapse (easy)
- Late (easy)
- OpenSource (easy)
- Noter (medium)
- Talkative (hard)

Skills   **Information security**

Confident Linux and Windows user.

Familiar with various pentesting utilities: nmap, metasploit framework, gobuster, burp suit, sqlmap, john the ripper, etc.

Experienced IDA Pro, CheatEngine and EDB user. Practiced reversing of Java and Python bytcode.

Programming

C/C++, x86-64 assembly language, Java, Python.

Also: Good knowledge of algorithms and data structures.

Languages

Russian (fluent), English (intermediate), Turkish (beginner)

About me   I am currently gaining experience in Software Development and I am very interested in gaining hands-on experience in Pentest/RedTeam. I've been programming for a long time, but my interest in practical hacking appeared even earlier.

So, as a child, I got tired of just playing games and wondered how I could get an advantage over other players using various technical methods - process memory patching, interacting with binary files, etc. Such an interest in the low-level details of how software works brought me to ITMO University, where I systematized my knowledge, took several courses on RE and binary exploitation, and also strengthened my skills in Computer Science. So, I dealt with many topics, for example, used by malware to hide activity from AVs.

Even now while working as a programmer, I periodically study various topics from computer security, in particular reverse engineering and pwn. Topic of computer security seems to me the most interesting, I recently started studying pentest, which I also really like, solving htb machines in my free time.

When solving any problem, I try to look for a non-standard approach, which helps me in solving information security problems, and my experience in solving algorithmic programming problems also helps me in this.

Interests   Pentesting, binary exploitation, protection bypass, low-level programming, OSINT