

# Marko Mladenovic

marko@bugdigger.com | bugdigger.com | [github.com/realbugdigger](https://github.com/realbugdigger) |  
linkedin.com/in/marko-mladenovic-9764721b7

## Education

---

**Bora Stankovic Gymnasium, Nis, Serbia** – Special class for Computer Science

**Metropolitan University in Nis, Serbia** - Software Engineering (On hold)

## Certifications & Achievements

---

**Malware development course by Maldev Academy** - maldevacademy.com

March 2024

- Developed a malware that bypasses Windows Defender Antivirus on x64 Windows, using my obfuscated shellcode that was run in a hijacked thread

**Ret2 Systems Binary Exploitation Course** - wargames.ret2.systems/course

February 2024

- Reverse engineered an algorithm that generates a software license
- Found race condition vulnerability in concurrent garbage collector. Challenge was inspired by the JavaScriptCore vulnerability presented at Pwn2Own 2018 competition

**ZDE VR Course** - [zerodayengineering.com/training/universal-vulnerability-research.html](https://zerodayengineering.com/training/universal-vulnerability-research.html)

February 2024

- Got essential knowledge and skills required to conduct modern low-level security research, vulnerability exploit development, secure software engineering and hardening

## Experience

---

**Advanced Security Technologies, Nis, Serbia (Internship)**

05/2024 - 08/2024

- Reverse engineering and finding vulnerabilities on a IP camera's firmware
- Developing firmware for ARM64 in microC
- Reversing and finding vulnerabilities in microC libraries

**FI3xx GmbH, Vienna, Austria (remote)**

06/2022 - 07/2023

- Backend developer (Tech stack: Java, Spring, Hibernate, JPA, Elasticsearch, Postgres, Redis)
- Maintained and expanded existing code base with occasional new feature development

## Projects

---

**Valve Anti-Cheat Bypass**

August 2024

- For educational purposes reverse engineered VAC and wrote a kernel driver for bypass

**KarolaScript on LLVM** - <https://github.com/realbugdigger/KarolaScriptLLVM>

(In progress)

- Transitioning my programming language to LLVM and MLIR infrastructure

**Rust ARM64 kernel for Raspberry Pi 3** - <https://github.com/realbugdigger/armRustOS>

(In progress)

- Wrote my ARM64 kernel in rust for Raspberry Pi 3 and kernel heap memory allocator

**Call of Duty Zombie Mod Hack** - <https://github.com/realbugdigger/Call-of-Duty-WaW-Hack>  
[https://www.bugdigger.com/projects/codwaw\\_hack](https://www.bugdigger.com/projects/codwaw_hack)

December 2023

- Reversed engineered a game and used dll injection to insert a hack into the game process.

- Hack uses function hooking on the D3D9 library graphics function

**KarolaScript** - <https://github.com/realbugdigger/KarolaScript>

*December 2023*

- Wrote my own interpreted programming language that is inspired by fusion of C and Python

**DirDigger** - <https://github.com/realbugdigger/DirDigger>

*July 2023*

- Directory busting extension for Burp Suite offering more features than alternatives

## **Skills**

---

- Programming languages (Java, C/C++, Rust, JavaScript, Python, x86-64 and ARM64 assembly)
- Reverse engineering, static analysis (ghidra, llvm), and dynamic analysis (gdb, WinDbg)
- Web exploitation (XSS, SQL injections, SSRF, Directory traversal, ...)
- Understanding of modern exploit mitigations (Sandboxing, PAC, Memory tagging)
- Ability to bypass common exploitation techniques (ASLR, DEP, PIE, Stack cookies)
- Exploit dev, writing n-day exploits for userland and kernel (Windows, Linux)
- Ability to quickly tackle and get familiar with unfamiliar large codebases
- CVE analysis, binary diffing and root cause analysis
- Malware development on x86-64 Windows (Obfuscation, Sandbox detection, Anti-debug, Anti-virtualization)
- Got my feet wet into LLVM and MLIR core ecosystem and libraries
- Embedded VR, extracting firmware from flash, emulation