VÍT CHRAMOSTA

linkedin↗ :: portfolio↗ :: github↗

chramiq@proton.me
773 098 405
Brno

PROFIL

Student kyberbezpečnosti na **FI MU** se zaměřením na **nízkoúrovňové programování a ofenzivní bezpečnost**. Mimo studium se aktivně věnuji nezávislému bezpečnostnímu výzkumu (Bug Bounty), v rámci kterého jsem reportoval zranitelnosti **globálním společnostem** i **vládním institucím** (Expedia, vláda Nizozemska). Ve volném čase vyvíjím open-source nástroje pro **analýzu malwaru** a **reverzní inženýrství**.

PRAXE

Nezávislý bezpečnostní výzkumník / Bug Bounty Hunter *2024 – současnost*

- **NCSC-NL (Vláda Nizozemska):** Objevení **kritických zranitelností** (potenciální **RCE** přes **SQL Injection**) napříč 3 doménami Ministerstva zdravotnictví. Oceněno **oficiálním poděkováním** (Letter of Appreciation) a odměnou. (článek↗)
- **Expedia Group:** Identifikace kritického **úniku produkčních API klíčů** platební brány TokenEx, umožňujícího **obcházení platební logiky**. Reportovány další bezpečnostní chyby (**Stored XSS**, **Enumerace kupónů, Admin Panel Takeover**). (hackerone↗)
- **Supply Chain Security Research**: Demonstrace plošného **Stored XSS** skrze převzetí opuštěné analytické domény. Analýzou provozu identifikováno okolo **10 000 zasažených uživatelů měsíčně**. Publikována detailní případová studie. (case study↗)
- **Další cíle**:
  - ➔ **Livesport:** Nalezení **Ad-domain Takeover** (plošné **Stored XSS**) (síň slávy↗)
  - ➔ **Zurich Insurance: IDOR** vedoucí k neautorizovanému přístupu a modifikaci **PII dat.**
  - ➔ **BrnoID: IDOR** v aplikaci města Brna vedoucí k úniku **platebních dat.**

PROJEKTY

de4vmp – .NET VMProtect Devirtualizer **C#, Reverse Engineering**

- Samostatně vyvinul statický analytický nástroj pro **automatickou devirtualizaci aplikací** chráněných obfuskátorem **VMProtect** kvůli častému zneužívání tvůrci malwaru.

nadlabem – Custom Intel 8086 Compiler **Python, Assembly (x86)**

- Navrhl a **naprogramoval kompilátor** překládající vlastní syntaxi (inspirovanou jazykem C) do 16bitového strojového kódu pro architekturu Intel 8086.

workaround – WAF Evasion Proxy **Go, Web Security**

- Vytvořil ofenzivní nástroj pro **bypass WAF** ochran využívající masivní IP pool Cloudflare k anonymizaci zdrojového provozu.

VZDĚLÁNÍ

Masarykova univerzita, Fakulta Informatiky *2024 – 2027*

- Bakalářské studium – program **Kyberbezpečnost**

ZNALOSTI

Programovací jazyky: C#, Python, Go, Shell, C, Assembly
Nástroje: Linux, Docker, Git, Vim, Wireshark, Burp Suite
Ostatní: OWASP, MITRE ATT&CK, CI/CD, Angličina C1