Rodný list soutěžní úlohy

*Rodný list slouží pro sběr a evidenci úloh, neobsahuje vše pro nasazení úlohy v soutěžní platformě (CTFd). Kompletní definici úlohy obsahuje repozitář, který obsahuje tyto soubory:*

* *zadání pro řešitele vč. uvedení formátu vlajky a související soubory – např. PCAP, logy, šifrové texty, binárky, …*
* *autorské řešení*
* *rodný list – tento dokument*

**Kategorie úlohy:** Mobile

**Název úlohy**: Instrumentace mobilní aplikace

**Typ úlohy**: Individuální

**Autor úlohy**: Matěj Sychra, Corpus Solutions a.s.

**Kontakt na autora**: [matej.sychra@corpus.cz](mailto:matej.sychra@corpus.cz), +420603861240

**Datum vytvoření úloh: 1. listopadu 2022**

**Stav úlohy**: POŽADAVEK NA KOOPERACI

**Cíl úlohy** *(pozn. její smysl, přínos, co se naučí účastník):*

Instrumentace vzorové mobilní aplikace – pro čtení paměti a objektů v běžící aplikaci na Androidu.

**Kapacitně - technická náročnost úlohy** *(pozn. popište objem datového podkladu – B, kB, MB, GB, TB, technické podklady – autor provozuje úlohu / je požadavek na zajištění platformy pro provoz)*:

Aby nebylo nutné řešit právní důsledky pře-podepisování cizí aplikace, úloha se provádí nad vzorovou aplikací. Ta zároveň obsahuje vlajku. K realizaci je třeba nástroj Objection a Frida, celkem bude tedy pro VM potřeba cca 15GB místa. **Ne**vyžaduje „rootnutý“ telefon Android, ale je snazší použít telefon ve vývojářském režimu, než simulátor.

**Hodnocení** *(pozn. uveďte rozpis bodového hodnocení; celkový počet bodů, popřípadě rozdělení na dílčí části úlohy, časová náročnost)*:

10 bodů, časová náročnost až 3h

**Nápovědy pro řešitele** *(pozn. vyplňte rozpis nápověd, přiřazení bodových ztrát)*:

Frida.re

Objection (Sensepost)

Apktool nesmí být `-dirty`, doporučujeme ručně nainstalovat stable verzi

**Další požadavky – technické prerekvizity** *(pozn. uveďte požadavky na organizátora/na řešitele)*:

Notebook s libovolným OS, VirtualBox s nainstalovaným posledním Ubuntu nebo Kali, Virtual Box Extensions, telefon Android.

**Licence** (Licenční ujednání)

Souhlasíte se zveřejněním úlohy a jejím řešením? ANO

Souhlasíte s modifikací úlohy pro využití v dalších letech? ANO

Souhlasíte s uvedením Vašeho jména/jmen, organizace, příp. kontaktů na Vás?

ANO. Souhlasím s výše uvedeným.

Souhlasíte s použitím Vaší úlohy pro výzkumné účely (např. analýza zadání) členy soutěžního výboru? *(pozn. v případě částečného souhlasu, rozepište rozsah omezení)*

ANO