Keyword of the day

TechmandanCZ

Tady jsem si říkal co bude za špeky - 4 bodová úloha a stačí najít web server který vrací vlajku? To zní nějak jednoduše.
Máme najít port, tak jsem začal samozřejmě oskenováním serveru (rustscan -> nmap). Následně jsem vzal pár portů a podíval se na ně. Vidím, HTML a obfuskovaný javascript, a krom různých emoji jsou téměř stejné. Napadá mě, zda-li mám stáhnout všechny stránky a filtrovat v nich, či jak nejrychleji najít řešení. Vezmu proto seznam portů, a koukám, však jich je jen 234, a všechny stránky mají jen jednu stránku.

Tak jsem si řekl, RAMky dost, co kdybych je načetl všechny naráz do prohlížeče?
A o jeden krátký fish script (`cat ports | string replace --regex "^" "http://keyword-of-the-day.cns-jv.tcc:" | xargs chromium`) později mám chromium s 230 záložkama které se pomalu načítají. Já jen postupně záložky zavírám (musím přes ctrl+w, chromium UI neumí zobrazit záložky které se nevejdou do seznamu), a po chvilce mám vlajku :)

Pro lehce delší popisek scriptu, přečte soubor ports (kde jsou pouze číselně porty, každý na vlastním řádku. Seznam jsem dostal z nmap výstupu, a ve VS code jsem na všech řádcích zároveň odebral zbytek krom portu samotného), před každý řádek přidá doménu a protokol k otevření, a pomocí xargs každý řádek samostatně spustí chromium.

To kdyby byly všechny 4 a 5 bodové úlohy takovéhle…