# Blokování sledování

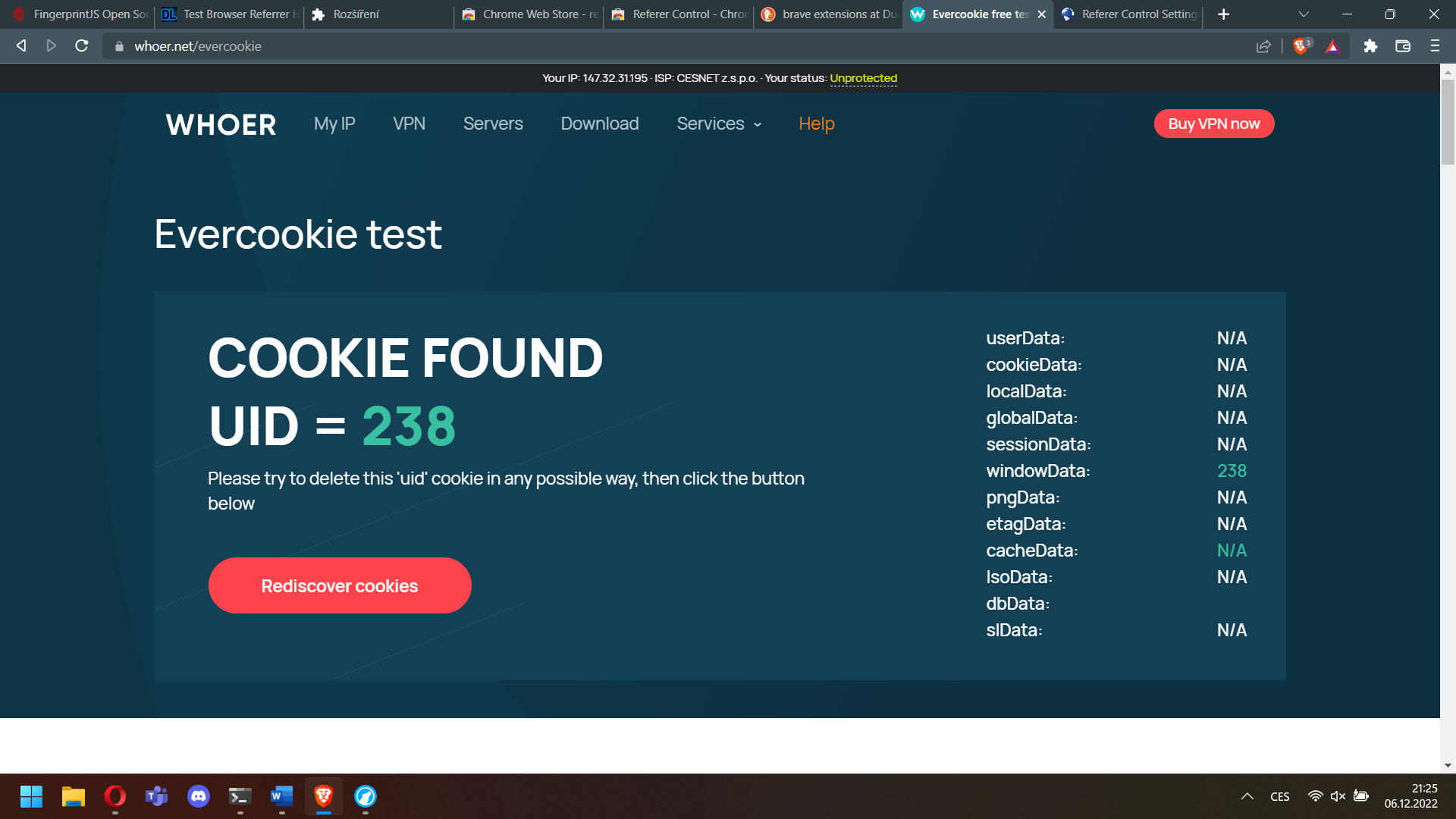
# 1. Evercookies

Pracuji v prohlížeči Opera.

Použití anonymního režimu zabraňuje znovu použití evercookies – musí se načíst nová. Obsah obrázku text, snímek obrazovky, monitor, obrazovka

Popis byl vytvořen automaticky

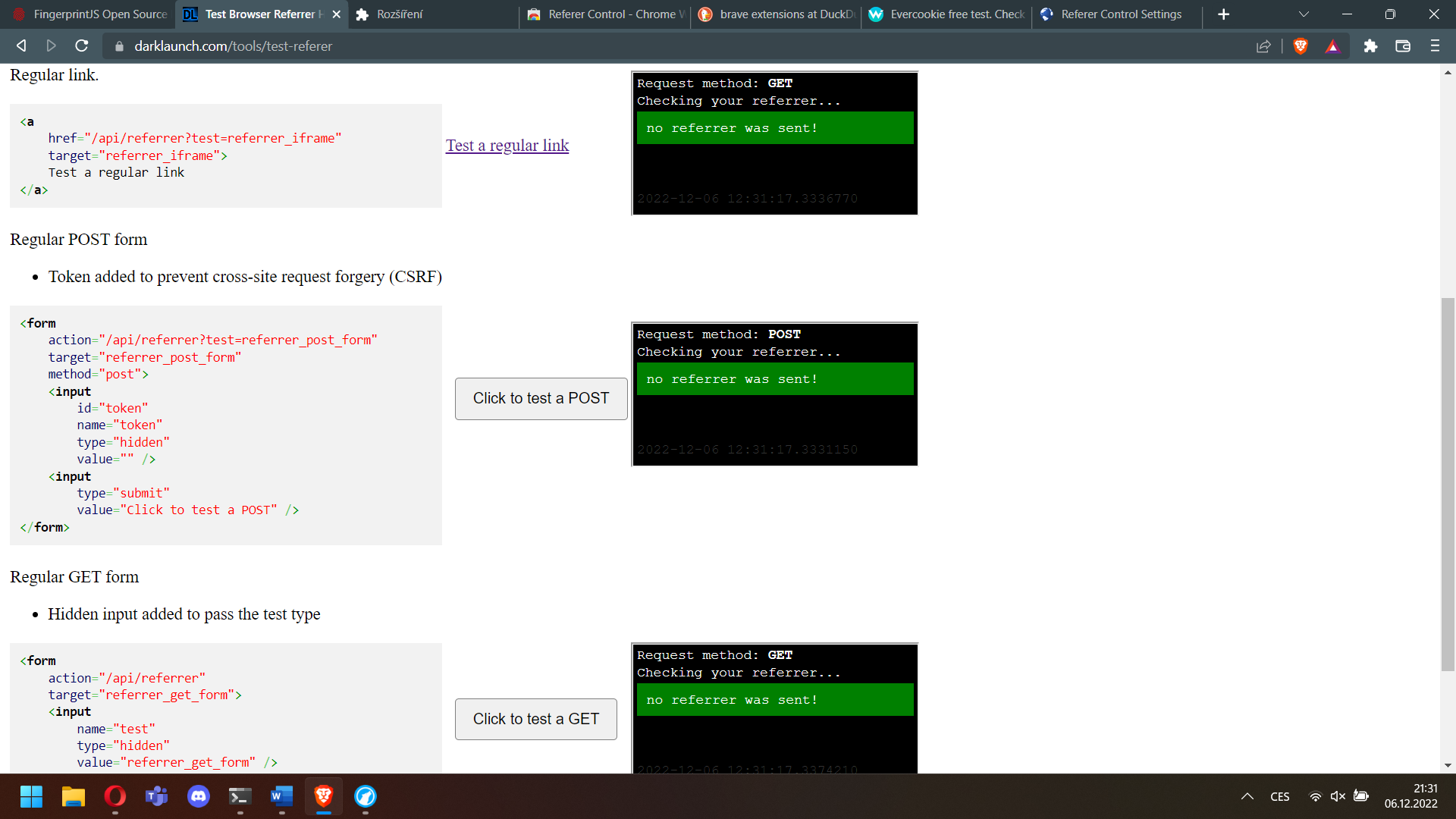
Další obranu proti evercookies ale Opera nenabízí (aspoň jsem nenašel), a tak jsem přešel k jinému prohlížeči. Nabízí se například LibreWolf, Brave, a další. Vybral jsem si Brave browser. V Brave prohlížeči zapneme předpřipravený „štít“ (Brave Shield). Ten se o Evercookies postará – neuloží/ po ukončení session smaže. Stačí výchozí nastavení, nebo je možné v nastavení nastavit striktnější politiku:



# 2. Referer

Brave Shield by měl za uživatele také řešit referer policy, nicméně náš testovací nástroj to vidí jinak, a hlásí, že se referer headers odesílají. To vyřeší add-on. Například „Referer Control“ (k nalezení na chrome web store: <https://chrome.google.com/webstore/detail/referer-control/hnkcfpcejkafcihlgbojoidoihckciin> )

Nastavíme blokování referera třetím stranám (totální blokování by mohlo narušit chod některých legitimních stránek) a zapneme blokování javascript referera – to přesvědčí i náš testovací nástroj.



# 3. Fingerprint

Brave Shield řeší i fingerprint. Konkrétně, mírně ho randomizuje. V nastavení prohlížeče existuje volba „block fingerprints“. Pokud bychom chtěli fingerprint ještě více zamlžit, pomůžou nám různé extensions. (Koneckonců takto bych to řešil třeba v Opeře) Na druhou stranu, může se stát, že přílišná změna fingerprintu z něj udělá naopak výjimečně nestandardní, a tedy naprosto unikátní fingerprint.

Obsah obrázku text, snímek obrazovky, monitor

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky