Vaja 2 – Spletni sledilniki

2. november 2024

Pri tej vaji sem implementirala spletno aplikacijo za persistentno sledenje odjemalcev. Preizkusila sem persistentnost fingerprintov za dva brskalnika, Brave in Chrome. Tako v brskalniku Brave kot v Chrome je bil fingerprint veljaven tudi po zaprtju in ponovnem odprtju aplikacije, tako v navadnem načinu kot v načinu incognito.

Po namestitvi vtičnika za zaščito pred canvas fingerprinting sem ugotovila, da vtičnik učinkovito opravlja svoje delo, saj je bil ob vsakem vklopu ustvarjen nov fingerprint.

Zanimivo je, da vtičnik za zaščito pred font fingerprinting ni bil tako uspešen: v približno polovici poskusov je bil ustvarjen popolnoma enak fingerprint in skripta je identificirala istega uporabnika. Nato sem spremenila funkcijo font fingerprintinga, da bi videla, kaj bi povečalo uspešnost zaščite vtičnika. Ugotovila sem, da je eden od dejavnikov število pisav, ki sem jih preverjala. Izbrala sem 10 najpogostejših pisav, ki so podprte v skoraj vseh brskalnikih, in z vsako pisavo dodala nekaj besedila v element span. Širino in višino elementa span sem dodala v polje rezultatov. To polje se pozneje uporabi za ustvarjanje edinstvenega hasha vsakega uporabnika. Ko sem število pisav, ki sem jih preverjala, zmanjšala z 10 na 1, se je močno povečala zmožnost vtičnika, da uspešno zakrije uporabnikov fingerprint.

Pri gostovanju odjemalca na strežniku nginx in pošiljanju zahteve strežniku node.js je bila zahteva CORS blokirana. CORS je mehanizem, ki strežniku omogoča, da navede tudi druge izvore, iz katerih lahko brskalnik naloži vire. Da bi to odpravila, sem v aplikacijo server.js s funkcijo setHeader() dodala glavo 'Access-Control-Allow-Origin' in zahteva je šla skozi. Drug način za to je uporaba Expressov paket CORS.

Po dodajanju glave CSP v konfiguracijo strežnika nginx sem v konzoli opazila sporočilo o napaki, ker sem z ukazom 'self' brskalnik nastavila le na nalaganje virov, ki so istega izvora. Po nastavitvi direktive connect-src na naslov strežnika nodejs sem odpravila napako, saj zdaj dostop do virov, naloženih iz strežnika nodejs, ni bil več omejen.