Refleksija - Varnostna analiza spletne aplikacije Lanuma.eu

Pri izvedbi varnostne analize spletne aplikacije lanuma.eu sem ugotovil, da ima aplikacija več tipičnih ranljivosti, ki se pogosto pojavljajo v spletnih aplikacijah, še posebej v manjših ali srednje velikih projektih. Čeprav nobena izmed zaznanih ranljivosti sama po sebi ni ocenjena kot kritična, njihova kombinacija predstavlja resno varnostno tveganje, saj omogoča napadalcu več različnih vstopnih točk.

Večina zaznanih ranljivosti spada v kategorijo Security Misconfiguration in Identification and Authentication Failures iz seznama OWASP Top 10. Manjkajoče varnostne glave, kot sta Content Security Policy (CSP) in pravilno nastavljeni atributi piškotkov, kažejo na to, da varnost ni bila v celoti upoštevana že v fazi zasnove aplikacije. Takšne napake pogosto nastanejo zaradi osredotočenosti razvijalcev na funkcionalnost in uporabniško izkušnjo, medtem ko je varnost obravnavana kot sekundarni vidik.

Posebej problematična se mi zdi kombinacija manjkajočih CSRF tokenov in piškotkov brez atributov HttpOnly, Secure in SameSite. To pomeni, da bi napadalec lahko z relativno preprostimi metodami izvedel CSRF napad, pri katerem bi uporabnik nehote izvajal dejanja v svojem imenu. V primeru dodatne XSS ranljivosti pa bi napadalec lahko dostopal do sejnih piškotkov in prevzel uporabniško sejo, kar je za e-poslovanje izjemno nevarno.

Rezultati analize so pokazali tudi pomanjkljivo implementacijo Content Security Policy, kjer so uporabljene direktive unsafe-inline in *. Takšna konfiguracija bistveno zmanjša učinkovitost CSP in omogoča izvajanje zlonamerne kode v primeru XSS napada. To se navezuje na OWASP kategorijo Injection in Insecure Design, saj aplikacija ne omejuje dovolj strogo virov, iz katerih se lahko nalaga koda.

Odprti porti 8080 in 8443 so me nekoliko presenetili, saj so ti porti pogosto namenjeni testnim ali administrativnim okoljem. V produkcijskem okolju takšna konfiguracija predstavlja dodatno tveganje, saj lahko napadalec poskuša izkoristiti

slabše zaščitene storitve ali zastarele komponente. To neposredno sodi v kategorijo Security Misconfiguration in Vulnerable and Outdated Components.

Pozitivno pa je, da je večino zaznanih ranljivosti mogoče relativno hitro odpraviti. Dodajanje ustreznih varnostnih glav, pravilna nastavitev piškotkov in zaprtje nepotrebnih portov ne zahtevajo večjih arhitekturnih sprememb, temveč predvsem boljšo konfiguracijo in upoštevanje varnostnih smernic. To kaže, da bi se z osnovnim poznavanjem OWASP priporočil in rednimi varnostnimi pregledi lahko bistveno izboljšala varnost aplikacije.

Ta vaja mi je pokazala, kako pomembno je, da se varnost spletnih aplikacij obravnava že od začetka razvoja in ne šele po tem, ko pride do težav. Prav tako sem spoznal, da tudi na videz manjše ranljivosti lahko v kombinaciji vodijo do resnih posledic, kar je še posebej pomembno v kontekstu elektronskega poslovanja, kjer se obdelujejo občutljivi osebni in finančni podatki.