Persondata sikret

Baggrund

I denne uge blev der udgivet en trussel om, at folks persondata ville blive lækket inden for en uge. Vi fandt imidlertid ud af, at dette kunne afværges, hvis det var muligt at bryde hackernes hjemmeside op. Jeg henvender mig, som en del af den gruppe, der blev nedsat til at håndtere dette problem, i dette notat for at underrette jer om, at krisen er blevet afværget. Der blev udformet en løsning, som har sikret, at folks persondata ikke vil blive lækket til offentligheden.

Løsning

Hackerne havde gudskelov været så inkompetente omkring opbevaringen af nøgler, at man næsten skulle tro, at de ønskede, at vi ville finde dem. Jeg vil spare jer for de allermest tekniske detaljer, men opgaven kan brydes op i to dele.

Identifikation af nøgler

De omdiskuterede nøgler skulle naturligvis findes for at låse op for hackernes hjemmeside. Lokationen for nøglerne kunne findes ved at inspicere hjemmesidens kilde og dernæst ved at inspicere siderne, der indeholder nøglerne. Et mønster dannede sig hurtigt for, hvilke nøgler der var gyldige for at låse siden op. Det viste sig at være tallene imellem 1 og 1000, begge inkluderet, som ved division med 10 ville efterlade en rest på 1. Det vil sige tallene i sekvensen,

1, 11, 21, .., 101, 111, .., 201, 211, .., 981, 991

Indtastning af nøgler

På hjemmesiden, der skulle låses op for, kan man finde tusind tjekbokse, man kan vinge af. Vi har identificeret de kasser, der skal vinges af, ud fra de gyldige nøgler, og siden der er tale om et hundrede gyldige nøgler og et tusind kasser, var det nødvendigt at få programmet til at kommunikere med browseren for at udfylde dem, siden indtastning skulle ske på under tredive sekunder.

Til fremtiden

Skulle vi ende med at stå i en lignende situation, er løsningen heldigvis udbygget på en sådan måde, at den kan håndtere.

1. **Flere sider med koder:** Hackernes kode befandt sig spredt ud på 10 websider. Koden er skrevet i en form, så det nemt er at udvide antallet af sider.
2. **Tilpasser sig talrækken:** Som forklaret ovenfor kunne nøglerne findes ud fra et mønster (rest på 1 efter division med tallet 10). Koden er skrevet således, at programmet kan identificere et nyt mønster med visse begrænsninger.
   Men hvis f.eks. det skulle forholde sig sådan, at den nye rest ved division skulle være 2, så kan koden stadig anvendes.

Nedenunder vil jeg formulere et par forhold, der måske kunne være værd at tage hensyn til, selvom det naturligvis er yderst usandsynligt, at hackerne anvender nøjagtig samme metode til at opbevare nøglerne og lække folks persondata.

- **Valg af browser:** Lige nu er browservalget statisk og skal ændres i selve koden. Dette kan hurtigt udvides til, at man selv vælger ved anvendelse af programmet.
- **Rapportering:** Som diskuteret, befandt nøglerne sig på sider af 2 forskellige kategorier. Skulle mønsteret ændre sig, ville det være en god idé at have en rapportering, der kan tilbagemelde om sider, der ikke følger de nuværende mønstre.
- **Fejlhåndtering:** Koden tager ikke hensyn til fejl i anvendelse. Det ville betragteligt forbedre brugeroplevelsen og fejlfinding, hvis fejl var prædefineret til at blive håndteret på en bestemt måde.

På vegne af,

Simon Echers