O lozinkama

written by js | 2023-02-04

Zašto je dobro, a i neophodno, imati posebnu lozinku za svaki drek

Uvod

Kada bi autori, vlasnici i/ili administratori web stranica zaista bili primorani brinuti o sigurnosti podataka i kada bi bili kažnjeni s npr. 10% prošlogodišnjeg prihoda svaki puta kad neka nepismena budala pokrade osobne podatke njihovih korisnika, svi bismo mogli imati isti username i istu lozinku za svaki sajt i nitko ne bi nikada saznao ni naš username ni password.

Kako?

Korištenjem tehnika zvane “hashing” i “salting”.
“Hashing” je pretvaranje teksta u neku vrstu šifre, a “salting” je jednostavno dodavanje jednog teksta na drugi.

Primjer

U idealnom svijetu server će i naš username “A” i password “B” pretvoriti u “hash” i tako ih spremiti u datoteku s lozinkama.
Hash slova “A” je “`559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd`“.
Hash slova “B” je “`df7e70e5021544f4834bbee64a9e3789febc4be81470df629cad6ddb03320a5c`“.
Dakle, totalno različiti su, a razlika je samo jedno slovo.

U još idealnijem svijetu server će na naš username “A” i password “B” dodati

“salt” (neki tekst) i sve zajedno pretvoriti u “hash” i tako ih spremiti u datoteku s lozinkama.
Na slovo “A” će dodati “123“, pa će hash biti “44b6e7cc9a53c0a1cd5cfb7e99eb9c5ec6750f5081918177ee0bf6e0b9c4456b“.
Na slovo “B” će dodati “234“, pa će hash biti “e6cfbddedf71cf1781351ee793eb20fddca48984613c5ce020fd0e55fd8b18c5“.

Trik je u tome da nitko tko čak i zna navedene hash-vrijednosti ne može znati jesu li nastale od slova “A” ili “hashiranjem” datoteke od 100 MB.

Razvalina1

Zamislimo situaciju da je napadač (M, 7g, Zg) razvalio server A1 ili HT i pokupio im datoteke s lozinkama. O načinu na koji su lozinke bile spremljene ovisi daljnja budućnost našeg accounta:

* Ako serveri spremaju našu lozinku u datoteku kao tekst “B” – svaka budala koja dođe do datoteke s lozinkama može doznati koja nam je lozinka. Tako npr. vrtićka djeca razvaljuju A1, HT i slične majstore informatike.
* Ako serveri spremaju lozinku kao hashirani “B” (dakle kao “df7e70e5021544f4834bbee64a9e3789febc4be81470df629cad6ddb03320a5c“), e, onda je napadačima stvoren problem. Možda nepremostiv, ovisi o duljini lozinke.
* Ako serveri spremaju i username “A” i lozinku “B” kao hashirane vrijednosti – napadači imaju vrlo veliki problem. Možda nepremostiv, ovisi o duljini lozinke.
* A ako serveri uvijek dodaju i “salt”, pa onda sve zajedno hashiraju – napadači imaju visoko vjerojatno nepremostiv problem, a posebno djecad od 7 godina koja razvaljuju hrvatske telekome, neovisno o duljini lozinke.

Važno

Naglašavam da će hash (*iste kvalitete*) slova “B” biti uvijek isti. Ali hash slova “B” + salt – neće. Ako koristiš istu lozinku na 10 servera, a svih 10 servera sprema samo hash vrijednosti – napadač koji pokrade datoteke sa tih 10 servera će znati da ti je password na svih 10 isti. Doduše, još ne zna koji je password, zna samo njegov hash, ali zna da treba “pogađati” samo jednom i da će mu se automatski otvoriti pristup na svih 10 servera. Sa “saltanjem” ne zna je li password svugdje

isti ili različit.

Zašto se uvijek naglašava da se ne koriste najčešće lozinke (“admin123”, “p4ssw0rd”, itd)? Jer se znaju hash vrijednosti za te lozinke. Npr. pokradu datoteke s lozinkama (“hashevima”), vide hash “`240be518fabd2724ddb6f04eeb1da5967448d7e831c08c8fa822809f74c720a9`” i provjere na internetu (bing) – odmah znaju da je password=admin123. Tvoj account na svih 10 servera je sada njihov. Ako serveri koriste hash+salt – u datotekama će biti drugi hash, a ne “`240b*`“, pa neće moći ni pretpostaviti da je “admin123”. Ok, pretpostavit će sigurno, ali pravimo se da neće. Ako koristiš na jednom serveru “admin123”, a na drugom “admin123admin123” – onda će napadač znati samo jedan tvoj password, ali ne i drugi, jer hasha za “dupli admin password” Bing ne nalazi na internetu (bing).

Sad ovdje uletavaju rainbow-tablice i nekakve matematike i šta ja znam, to je prepametno za mene, pa ću stati.

Uglavnom – hash vrijednosti za česte i/ili kratke lozinke se znaju. Postoji popis riječi i fraza i njihove hash vrijednosti. Ali ne postoji nigdje nijedan popis sa frazom
“`Ovim rijecima zapocinje moja lozinka koju cu zavrsiti dvostrukim usklicnikom!!`” i njenim hashom. Ako odaberes takvu kobasicu za lozinku i ako server sprema lozinke u hash obliku – možeš mirno spavati čak i da napadač dođe do datoteke.

“Lozinku je provjeriti lako. Pitaj me ‘Kako?'”

Lako, rekoh. Nakon što npr. u browseru, u polje “Password” upišeš lozinku, ona bude pretvorena u hash i server usporedi je li taj hash isti s hashem u datoteci hashova. Ako jest – lozinka ti je ista kao zadnja aktivna i server te pušta dalje. Ako ti dva hasha nisu ista – imaš problem. Isto je i sa hash+salt. Salt (v.gore “`123`” i “`234`“) je isti, može biti čak i javan, ako se ne varam? Bitno je da se promijeni hash lozinke i nešto totalno neprepoznatljivo (v.gore – slova A i B imaju različite hasheve). Ne može se “dehashati” (“unhashati?”) čak i ako znaš salt, da bi se recimo dobio barem originalan hash.

Stanje

Autori, vlasnici i/ili administratori web stranica / servera **nisu** primorani brinuti o sigurnosti podataka, jer su članovi vlade mutavi kao i telekomi i nit znaju da je to potrebno nit znaju kako to organizirati, pa stoga moramo mi, vlasnici svojih podataka, paziti na njih i raditi nečiji posao. Jedni ih spremaju ovako, drugi onako, neki namjerno, najčešće nemaju pojma, …

Dobro, okej, šta da radim, šta?!

I zato moramo na svakom sajtu koristiti drugu lozinku. Dovoljno je da imaš lozinku "admin123admin123admin123" i onda dodaš barem tri slova specifična za sajt – npr. za outlook.com dodaj "olk" ili "out", pa ti je password "Bolk" ili "Bout". Za bing.com koristi "bng" ili "bin", pa ti je password "Bbng" ili "Bbin". Naravno, lozinka ne smije biti kratka! Kratke lozinke sigurno postoje u gotovim tablicama s popisom riječi i njihovih pripadnih hasheva.

Ostalo

Dobro je ne koristiti čžš – nikad ne znaš kad ćeš sjesti za tastaturu koja nema ta slova.

Bilo bi lijepo kada bi se i username spremao kao hash. No, onda se ne bi mogli prodavati naši osobni podaci za $100 na 10.000 podataka, pa ću prestati maštati.

Zato je dobro koristiti i različita korisnička imena na različitim sajtovima.

Ovo nije sve. Ima mnogo pametnih stvari još oko toga, ali meni je dovoljno.

Kvantna računala će razjebat ovu priču o passwordima kao Pandrija Lenković ljudski integritet. Ne razumijem ni trunčicu kako ta računala rade, pa ne znam ni kako će razjebat ovo, ali pametni ljudi kažu da će razjebat. Ne znam kada. Mislim da ne tako skoro?

NSA, FBI, CIA, KGB i ostali imaju vjerojatno procesorsku i/ili softversku moć za razjebat hash kratkih passworda. Možda čak i ne "grubom silom" (pogađanjem je li "A"? Je li "B"? Bingo!) nego razvaljivanjem algoritama ili nekim "backdoorom" za razbijanje. Ne znam. Ono što znam jest – ako radiš online i pokušavaš se

sakriti, neće ti uspjeti. Nitko te neće naganjati ako gledaš pornić Milana Zoranovića s konjima, ali ako uputiš ozbiljne prijetnje ozbiljnim ljudima ili organiziraš ozbiljnu kriminalnu udrugu, a ne plaćaš ili ne trošiš državni proračun – najebat ćeš. "*They will seek for you, they will find you, and they will fuck you*".

Tekst su sponzorirali hrvatski, a i šire, telekonji.

password xpassword pwd xpwd lozinke xlozinke hash xhash salt xsalt