Në fillim të viteve 90-ta filluan të paraqiten edhe uebfaqet e para në internet, që përmbanin tekst dhe aty këtu ndonjë imazh me rezolucionit shumë të vogël. Me kalimin e kohës dhe me paraqitjen e uebfaqeve dinamike filluan të ndryshojnë gjërat për të mirë. Filluan të hapen mundësi të reja siç janë: mundësia për vendosje të zërit në ueb, video incizime, krijimi i hartave mbi imazhe, puna me baza të të dhënave etj. Sa më shumë që ngarkoheshin gjëra të rëndësishme në rrjet proporcionalisht rriteshin edhe gjasat për sulme kibernetike.

Vrimat e sigurisë u mundësonin keqpërdoruesve kyçje direket në të dhënat e ndjeshme, andaj u shfaq nevoja për gjetjen e një zgjidhjeje. Si masë e parë sigurie që në fillet e këtij problemi ishte përdorimi i fjalëkalimeve.

Ç’ janë fjalëkalimet ?

Fjalëkalimi është një fjalë sekrete që përdoret nga shfrytëzuesi me qëllim që sistemi ta vërtetojë faktin që shfrytëzuesi ka apo nuk ka privilegje për tu kyçur në resurse.

Fjalëkalimet edhe pse ishin preventivë e shumë sulmeve me kalimin e kohës filluan ta humbasin efektin e tyre, arsyeja, sepse fjalëkalimet në baza të të dhënave ruheshin ashtu siç edhe shkruheshin. Për shembull fjala “ylber12345” e përdorur si fjalëkalim ruhej e njëjtë “ylber12345”.

Ishte ky shkaku i paraqitjes së algoritmeve për kriptim (kriptografisë) me qëllim që fjalën e përdorur si fjalëkalim ta paraqesin në formë të pakuptueshme me qëllim të parandalimit të sulmeve të mundshme.

Problemet e fjalëkalimeve të pakriptuar!

Le të supozojmë që kemi një aplikacion ku për të pasur qasje në zona të caktuara, përdoruesit duhet të regjistrohen në uebfaqe me një e-mail dhe fjalëkalim. Pra unë jam përdorues dhe regjistrohem me fjalëkalimin “ylber12345” duke menduar se të dhënat janë të sigurta. Ndërkohë një sulmues tenton të gjejë vrima sigurie në sistem dhe arrin t’i gjejë duke përdorur një teknikë shumë të përhapur (fatkeqësisht) si SQL Injections. Në dorën e sulmuesit është e

gjithë tabela e përdoruesve me e-mailet e tyre dhe fjalëkalimet, duke i dhënë mundësi të identifikohet në sistem si kushdo përdorues. Imagjinoni që sistemi në fjalë të jetë për të blerë produkte! E gjithë kjo mund të parandalohej nëse kriptohej fjalëkalimi, pa harruar gjithashtu edhe vrimat ndaj SQL Injections.

Çfarë është kriptimi?

Kriptografia është shkenca e fshehjes së informacionit, në mënyrë që të lexohet vetëm nga personat apo sistemet që dinë ta dekriptojnë mesazhin.

Për shembull nëse fjalën “ylber12345” e kriptojmë me ndihmën e algoritmit SHA1 do të fitojmë “289ac24822b6c6d84c1e6de4efee3cf8db73e90e”.

Nga shembulli I lartshënuar kuptohet përparësia e përdorimit të algoritmeve të tilla. Andaj ne pamë të arsyeshme që në këtë artikull të flasim shkurtimisht për disa prej tyre.

- MD5 –

MD5 (Message-Digest Algorithm 5) është një funksion HASH shumë i përdorur në ueb dhe zgjedhja për kriptim në shumë aplikacione të njohura. Fjala e gjeneruar është 128 bit e gjatë me 32 karaktere heksadecimale. Në shumë përdorime sensitive, MD5 është abandonuar sepse është provuar dobësia e tij.

- SHA1 –

Ashtu si MD5, edhe SHA1 (SHA – Secure HASH Standart) gjeneron një fjalë të pa dekriptueshme, por gjatësia e të cilës është 160 bit dhe 40 karaktere heksadecimale. SHA1 konsiderohet më i sigurt se MD5 në përgjithësi, edhe pse dobësi sigurie janë gjetur në të.

Shpresoj ta keni kuptuar se sa e rëndësishme është për ju ti enkriptoni fjalëkalimet e klientëve tuaj, ueb aplikacioneve tuaja do tu shtohet një masë sigurie e një niveli më të lartë dhe njëkohësisht do ta fitoni edhe besimin e klientëve tuaj.

Përgatiti Ylber Veliu - *Student në Universitetin Shën “Qirili dhe Metodi” – Fakulteti i elektroteknikës*