TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Informaatikainstituut

Rasmus Rugam, 166056IAIB

Krüpto Äpp

Raport

Lektor: Sten Mäses

Tallinn 2019

Tudengi nimi: Rasmus Rugam
Tudengi häkkerinimi: YouGotPwned
Tudengi kood: 166056IAIB

Raport: Krüpto äpp

Rakendus asub järgneval veebilehel: https://rrugam.github.io/index.html

Rakendus toimib koos kujundusega kõige paremini, kui veebileht avatakse arvutist. Kujundus läheb veits paigast ära, kui see avatakse nutitelefonis või tahvelarvutis.

OTP Encrypt ja Decrypt toimivad mõlemad ühe ja sama algoritmi järgi, decrypti käigus on muudetud ainult tingimusi natukene.Töötamiseks on tarvis, et oleks Sisend(sõnum) ja Võti(salasõna, mida kasutatakse krüpteerimisel). Mõlemad väljad on vaja tarvis ära täita ja kusjuures veel peavad mõlemad väljad olema sama pikad. Juhul kui ei ole, teavitatakse sellest kasutajat. Alert boxiga, mis ilmub ekraanil. Antud rakendusel ei ole kahjuks võimalik kasutada tühikut, et moodustada korrektsed ja loetavad laused. On tarvis kirjutada kogu tekst ühe reana. Kood on kommenteeritud eraldi “backend.js” failis, kus on iga rida hästi ära seletatud, mis mida teeb ja miks ta nii teeb.

Sha 512 koodijupp on sellel leheküljel mida sai ka kasutatud enda projekti raames. See kood teeb sisendi SHA-512 stiilile --) https://coursesweb.net/javascript/sha512-encrypt-hash_cs

SHA-512 to base64 jaoks on kasutatud internetist olevat koodijuppi mis asub järgneval veebilehel -> https://developer.mozilla.org/en-US/docs/Web/API/WindowOrWorkerGlobalScope/atob

Antud kood teeb sisestatud teksti SHA512 stiilile, ning kasutame seda koodi meie eraldi funktsioonis SHA-2 var encodedData = window.btoa(SHA512(sisend));

Kus muudame Sha512 funktsiooni sisendi BASE64 stiilile ning tagastame antud aknas. Kõige raskem minu jaoks oli arvatavasti välja mõelda Encrypt ja Decrypt süntaks, mis vajas natuke aega mõtlemist, et kuidas need tähed omavahel vahetuvad. Kui sellest sai aru, siis edasine läks juba veidi libedamalt.

MD5 ei õnnestunud teha, kuna igalpool, kus seda uuritud sai oli common answer, et see on loodud selleks, et seda ei olekski võimalik decryptida, et see olevat NSA poolt valmis töötatud. Lahti muukimiseks läheks vaja väga väga suurt andmebaasi ning brute forceiga hakata lihtsalt hash/räsi lahti muukima läbi antud andmebaaside. Kuna sellega ma väga hakkama ei saanud, siis jätsin selle lihtsalt tegemata. Küll aga uurisin kuidas ta töötab, aga see vajab liiga palju aega ja teadmisi mida mul ilmselt praegu veel ei eksisteeri. Ning ülesanne käis üle jõu.

Kommenteeritud kood on ainult “backend.js”. Kuna seal toimus peamine töö ja aeg ning keerulisus, ei näinud väga mõtet kommenteerida HTML koodi, mis on lihtne ning arusaadav.