Ime in priimek: **Datum:**

HTTPS MITM iz znanih aplikacij

Namen vaje je:

- Izvesti HTTPS MITM napad in spoznati tehniko, ki to preprečuje.
- Namen vaje je kako s preprostimo orodji in tehnikami izvedemo brute force napad.
- Spoznati nekaj tehnik shranjevanja gesel in navesti njihove prednosti in slabosti.

1. HTTPS MITM

Nadgradnja na protokol HTTPS.
Infrastruktura javnih ključev se aktivira z namestitvijo SSL certifikata, ki vsebuje dva elementa: protokol SSL in samo potrdilo. Protokol SSL zagotavlja prehod na HTTPS, ki varuje vsako spletno in elektronsko komunikacijo. Zasebni ključ je edini, ki lahko vzpostavi veljavno povezavo v povezavi z ustreznim potrdilom.
Certifikat potrjuje identiteto in zanesljivost lastnika na podlagi infrastrukture overitelja potrdil (CA).
Ko je certifikat SSL nameščen na strežniku, so izključeni vsi posegi tretjih oseb, kot so napadi MitM. Čeprav ima morda možnost prestrezanja podatkov, jih heker ne more dešifrirati, ker nima zasebnega ključa. Zasebni ključ pripada izključno strežniku.

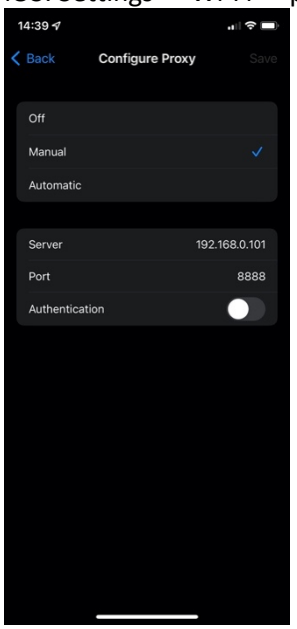
* In 2013, Nokia's Xpress Browser was revealed to be decrypting HTTPS traffic on Nokia's proxy servers, giving the company clear text access to its customers' encrypted browser traffic. Nokia responded by saying that the content was not stored permanently and that the company had organizational and technical measures to prevent access to private information.

Nalogo bomo izpeljali na vaših osebnih telefonih, tako so navolila ločena za android in ios naprave:
Navodila in vprašanja:

a) Prenesite program Charles in ga namestite na vaše računalnike.

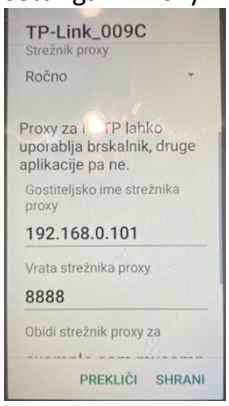
b) Na telefonu nastavite proxy:

[1] iOS: Settings -> Wi-Fi -> podrobnosti -> Configure Proxy

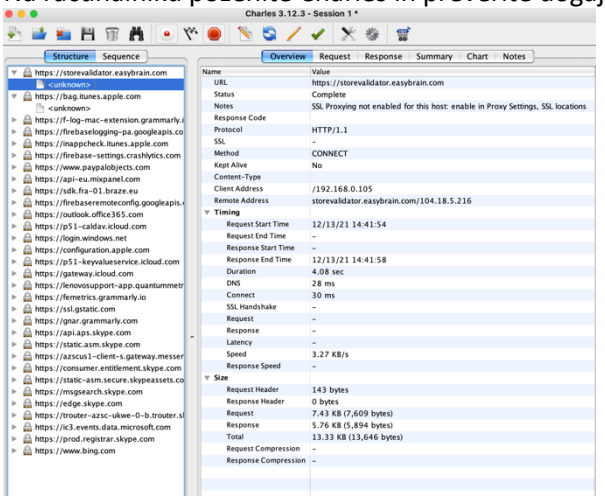


*server naj bo IP vašega računalnika

[2] Android: Settings -> Network & internet -> Wi-Fi -> Settings icon -> Edit -> Additional settings -> Proxy



c) Na računalniku poženite Charles in preverite dogajanje:

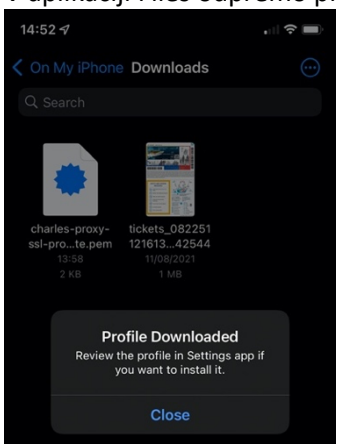


d) Na telefon namestimo SSL root certifikat:

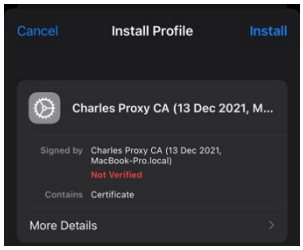
[1] iOS: prenesemo certifikat: https://chls.pro/ssl

[2] Datoteko shranimo v Files

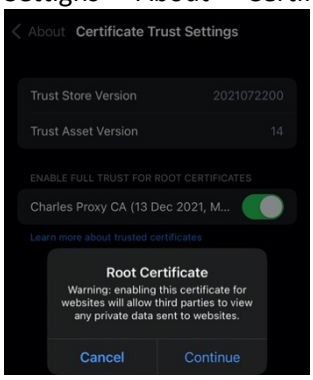
[3] V aplikaciji Files odpremo prenešeno datoteko



[4] Settings -> General -> VPN & Device Management izberete prenešen certifikat in ga namestite



[5] Settigns -> About -> Certificate Trust Settings

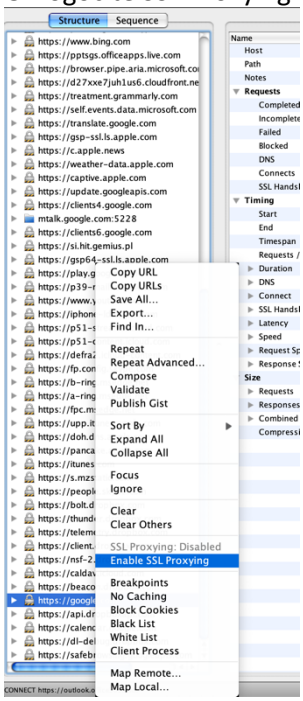


[1] Android: prenesemo certifikat: https://chls.pro/ssl

[2] Namestitev certifikata: Settings -> Security -> Encryption & credentials -> Install credentials -> Izberete prenešen certifikat in kliknete Install

e) Na računalniku poženite Charles in preverite dogajanje:

[1] Omogočite SSL Proxying: desni klik -> enable SSL Proxying



[2] Osvežite stran na telefonu in opazujte dogajanje

f) Razložite primer iz uvoda: Nokia's Xpress Browser in skicirajte dogajanje:

g) Odprite eno aplikacijo npr. Facebook. A aplikacija deluje? Ali ima povezavo s spletom?

h) Kaj je Certificate pinning?

i) Ponastavitev
   - Odstranite certifikat
   - Onemogočite proxy

2. Brute force ugibanja gesel za spletne strani

Brute force napad oz. napad z grobo silo je tehnika razbijanja gesel oz. pridobivanja podatkov o pravicah uporabnikov z namenom njihove zlorabe. Napadalec sistematično preveri veliko število gesel in šifrirnih fraz, dokler ne najde prave kombinacije.
Hydra je vgrajeno Kali orodje namenjeno brute force napadom. Pomoč: `man hydra`

Navodila in vprašanja:

a) Odpremo spletno stran https://cybersec.ltfe.org/login in se vpišemo z napačnim user/pass. Oglejmo si kaj se v ozadju doagaja s spletno stranjo. (desni klik –> Inspect -> Network, Headers)

b) KALI LINUX: Odpremo terminalno okno ter zaženemo Hydra program z ukazom, ki ga sestavimo. Manjkajoče podakte najdete na spletni strani, pomagajte si tudi s hydra pomočjo (KALI LINUX).

```
hydra -l [USER] -P Desktop/pass.txt [DOMENA] http-post-form
"/[DATOTEKA.php]:[USERNAME]=^USER^&[PASSWORD]=^PASS^:F=[IZPIS_NEP
RAVILNO_GESLO] -v -V
```

c) Izpišite končni ukaz Hydra orodja.

d) Ali najde pravo geslo?

e) Brute force način ugibanja ponovimo še s Python skripto (https://cybersec.ltfe.org/login/crack.py, https://cybersec.ltfe.org/login/user.txt in https://cybersec.ltfe.org/login/pass.txt). Komentirajte dogajanje!
Ukaz: `python3 crack.py`

3. Kako (ne) shranjujemo gesel(a)

Večina spletnih aplikacij zahteva, da se njihovi uporabniki prijavijo z uporabniškim imenom in geslom. Podatki, ki jih je predložil uporabnik se nato primerjajo s podatki, shranjenimi v podatkovni baze, in če se ujemajo, se uporabniku odobri dostop. Zveni dobro! Toda kaj se zgodi, ko takšna podatkovna baza postane kompromitirana. V tej vaji bomo obravnavali nekaj tehnik shranjevanja gesel in navedli njihove prednosti in slabosti.

Navodila in vprašanja:

a) Golo besedilo: primer (https://cybersec.ltfe.org/passwords/plainpass.txt)
   I. Prednosti
   II. Slabosti
   III. Uporabnost

b) Dvosmerno enkriptirana gesla: primer(https://cybersec.ltfe.org/passwords/encypted.txt)
   I. Prednosti
   II. Slabosti
   III. Uporabnost

c) Hashirana gesla (MD5, SHA1): primer(https://cybersec.ltfe.org/passwords/hash.txt)
   I. Prednosti
   II. Slabosti
   III. Uporabnost

d) Predlagajte rešitev in komentirajte prednosti, slabosti in uporabnost!

Komentar, zapiski vaje: