5. zadatak:

5. Educational Purposes Only
    a. Flag format : UNS{}
    b. Together with your friends, you browsed the web archive of the Faculty of Technical Sciences and came across some very old archive. You downloaded it to see what was inside, but it was locked. Along with it, you also found a file that you think can help you unlock the archive.

Da biste “provalili” lozinku, odgovorite na sledeća pitanja i spojite odgovore zajedno. Srećno!
https://www.md5hashgenerator.com/

1. Datum kada je Fakultet tehničkih nauka zvanično otvoren. (Format datuma: DD/MM/YYYY) MD5: 02c3890bb0b03a24b99c3e4a39f18c44
2. Ime osobe koja je obavljala funkciju dekana fakulteta od 01.10.1975. do 30.09.1977. MD5: 06904f68128802c069e782b772e85eda
3. Datum kada je pokrenut sajt FTN-a. (Format datuma: DD/MM/YYYY) MD5: f4d7caf81e33bc156cc3e98cf8095d2e
4. Godina kada su uvedene studije u oblasti "Poštanski saobraćaj i telekomunikacije". MD5: 5ec829debe54b19a5f78d9a65b900a39

Zadatak 5 - Educational Purposes Only Dekodiranjem md5 hash-eva odgovora na pitanja u fajlu : forgotten_password.txt i njihovim spajanjem dobija se password za otključavanje zip-a. Korišćen je sajt : https://www.md5hashgenerator.com/

• Pitanje 1 : 18/05/1960 - 02c3890bb0b03a24b99c3e4a39f18c44

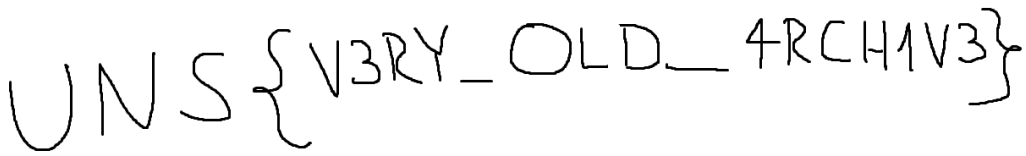
• Pitanje 2 : Dragutin - 06904f68128802c069e782b772e85eda

• Pitanje 3 : 18/05/2005 - f4d7caf81e33bc156cc3e98cf8095d2e

• Pitanje 4: 1999 - 5ec829debe54b19a5f78d9a65b900a39 Kombinovanjem ovih podataka, otključali smo zip fajl u kojem se nalazila slika

. Password : 18/05/1960Dragutin18/05/20051999

Na slici je bio prikazan sledeći tekst: UNS{V3RY_OLD_4RCH1V3}



3d236fbff6970ebbc320ec4a04c7641b

3. Zadatak:

3. COMMITMENT

- Flag format : csictf{}

- hoshimaseok is up to no good. Track him down.

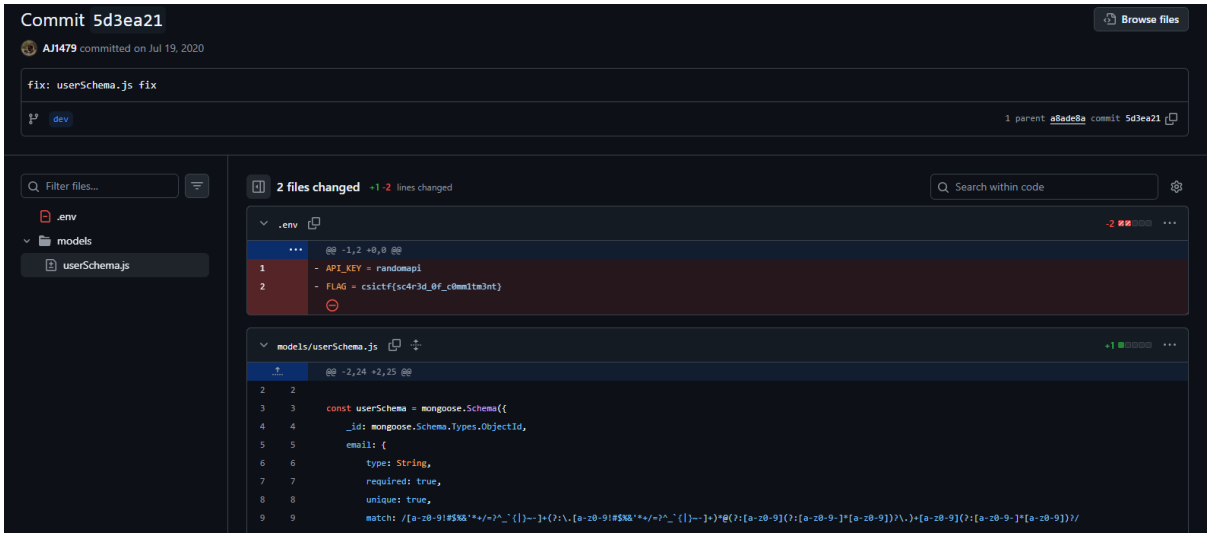
Prvo vidim GitHub nalog: https://github.com/hoshimaseok

Zatim vidim repozitorijum nazvan **SomethingFishy** i gledam u istoriju commit-ova. Proveravam ih jedan po jedan i vidim commit poruku: **feat: Looking for flag?**. Pogledavši to, vidim mnogo hebrejskog teksta koji, nažalost, nije bio koristan i predstavljao je distrakciju.

Pregledom ostalih commit-ova vidimo commit **fix: userSchema.js fix** koji sadrži obrisan `.env` fajl sa flag-om.

Flag:

`csictf{sc4r3d_0f_c0mm1tm3nt}`



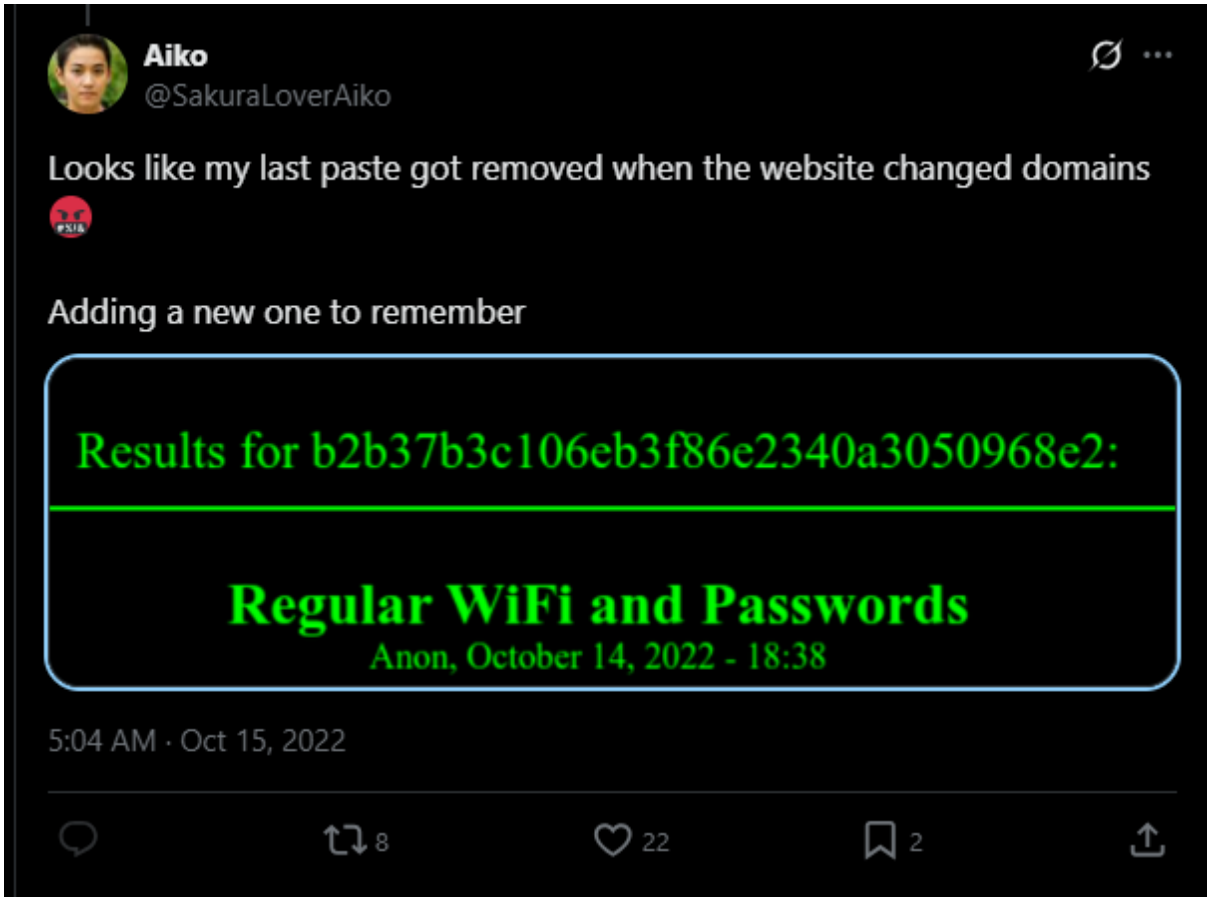
Sakura

Zadatak 5

Pitanje 9: Koji je trenutno Twitter nalog napadača?

Imamo stari Twitter nalog mete koji dobijamo iz slike **@AikoAbe3**. Pretragom tog imena na Google-u možemo pronaći novi nalog. To takođe možemo potvrditi posmatranjem tvitova mete.

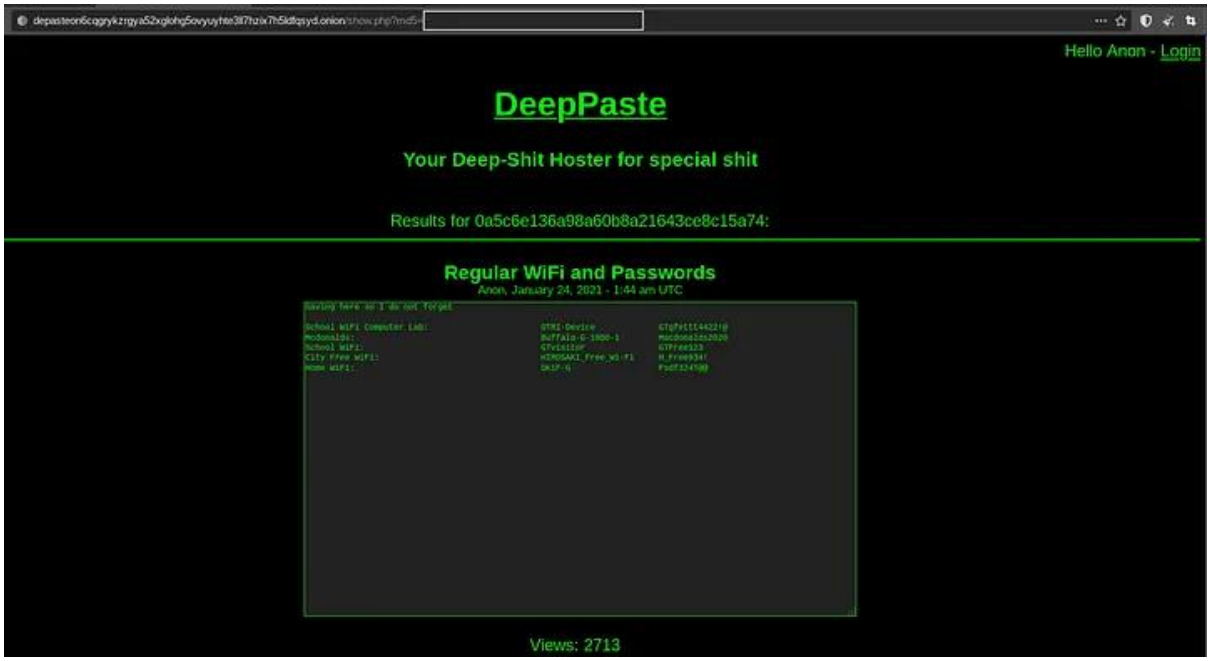
@SakuraLoverAiko



Pitanje 10: Koji je URL lokacije na kojoj je napadač sačuvao svoje WiFi SSID-ove i lozinke?

Na priloženoj slici vidimo MD5 heš i listu pristupnih tačaka (AP) sa SSID-ovima i lozinkama.

URL:



http[:]//depasteon6cqgrykzrgya52xglohg5ovyuyhte3ll7hzix7h5ldfqsyd.onion/show.php?md5=0a5c6e136a98a60b8a21643ce8c15a74

Pitanje 11: Koji je BSSID napadačevog kućnog WiFi-ja?

Koristeći samo ponuđeni SSID "Home Wifi", možemo dobiti dodatne informacije preko WiGLE baze dovoljno je uneti SSID u polje za pretragu.

84:af:ec:34:fc:f8

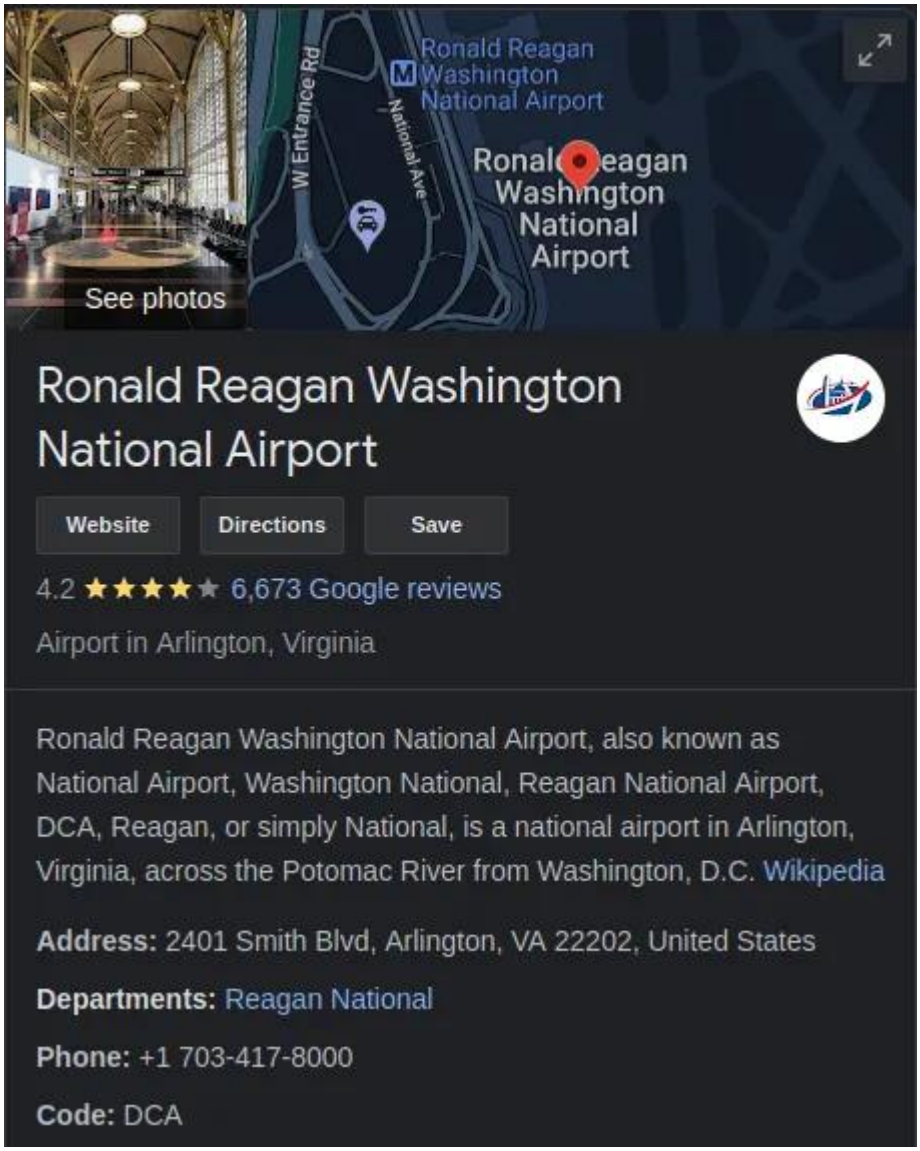
Zadatak 6

Pitanje 12: Koji je aerodrom najbliži lokaciji sa koje je napadač podelio fotografiju pre nego što je ušao u avion?

Na Twitter nalogu mete ostavljeni su tragovi o ruti kojom ide pre nego što se vrati kući. Prvi trag je fotografija trešnjinog cveta.

Na slici se vidi jedinstven veliki beli obelisk u centru. Kada isečemo taj deo i uradimo *reverse image search*, otkrivamo da je u pitanju **Washington Monument**, koji se nalazi u **National Mall-u u Vašingtonu, SAD**.

U Vašingtonu postoje tri glavna aerodroma: **Ronald Reagan Washington National Airport**, **Washington Dulles International Airport** i **Baltimore/Washington International Thurgood Marshall Airport**. Najbliži **National Mall-u** je **Ronald Reagan Washington National Airport**.



Pitanje 13: Na kom aerodromu je napadač imao poslednje presedanje?

Sledeća slika na njihovom Twitter nalogu uslikana je u salonu, verovatno aerodromskom lounge-u.

Ako pokrenemo *reverse image search* na fotografiji, dobićemo više različitih sajtova. Prvi sajt je na japanskom jeziku i sadrži identičnu sliku sa naloga mete. Kada prevedemo stranicu na engleski, dobijamo naziv aerodroma. Potom pronalazimo **troslovni kod aerodroma**.

Top Latest People Media Lists

Aiko @SakuraLoverAiko · Jan 25, 2021

My **final** layover, time to relax!

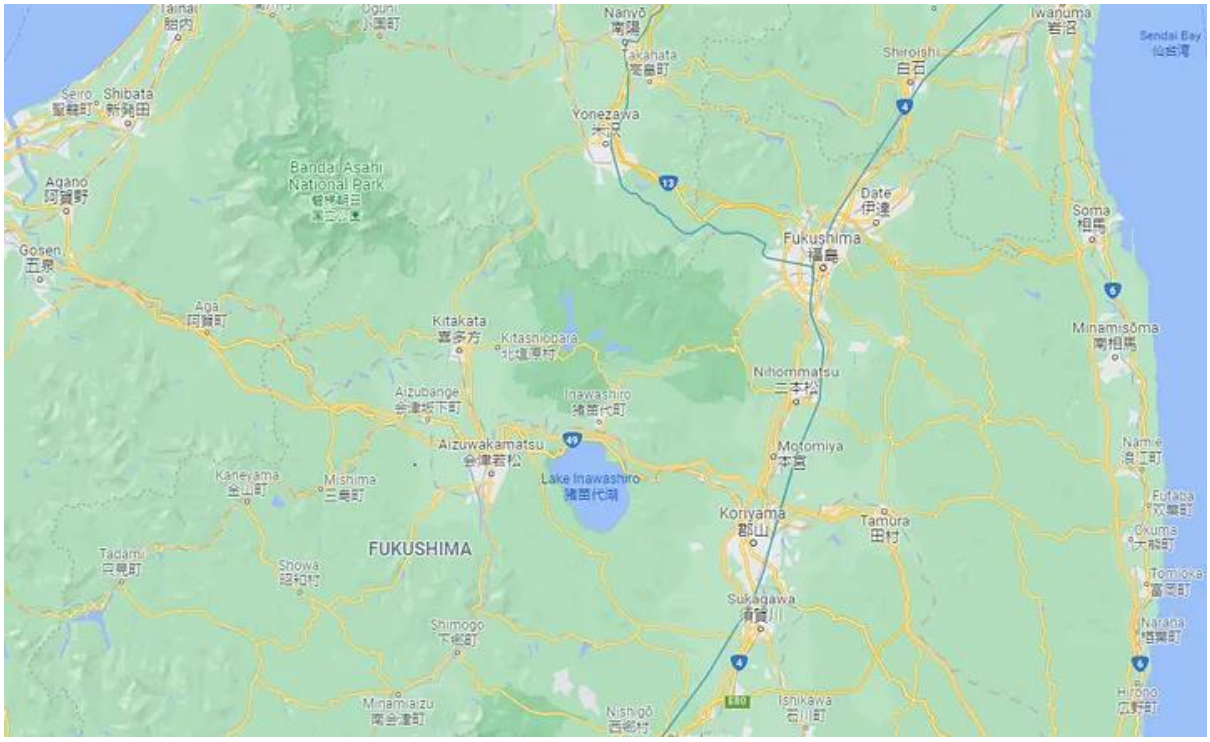
14

HND (Tokyo Haneda Airport)

Pitanje 14: Koje jezero se vidi na mapi koju je napadač podelio dok je bio na poslednjem letu ka kući?

Meta je tvitovala sliku koja izgleda kao satelitski prikaz leta. Na slici je deo japanskog poluostrva. Pomoću **Google Maps-a** možemo identifikovati naziv jezera.

Lake Inawashiro



Pitanje 15: Koji grad napadač verovatno smatra “domom”?

Na osnovu pitanja 13 i 14, znamo da meta leti na sever. Imamo pravac, ali ne i tačan grad. Međutim, u **pitanju 10** pominju se neki drugi SSID-ovi, uključujući “Home Wifi”. Pomoću **Wigle** baze možemo proveriti lokaciju ovog SSID-a. Ostali SSID-ovi takođe se nalaze u istom gradu, koji je u skladu sa očekivanim pravcem leta.

Hirosaki

Network Location

Click for interactive map


Aiko @SakuraLoverAiko · Jan 24, 2021
Checking out some last minute cherry blossoms before heading home!
5
49