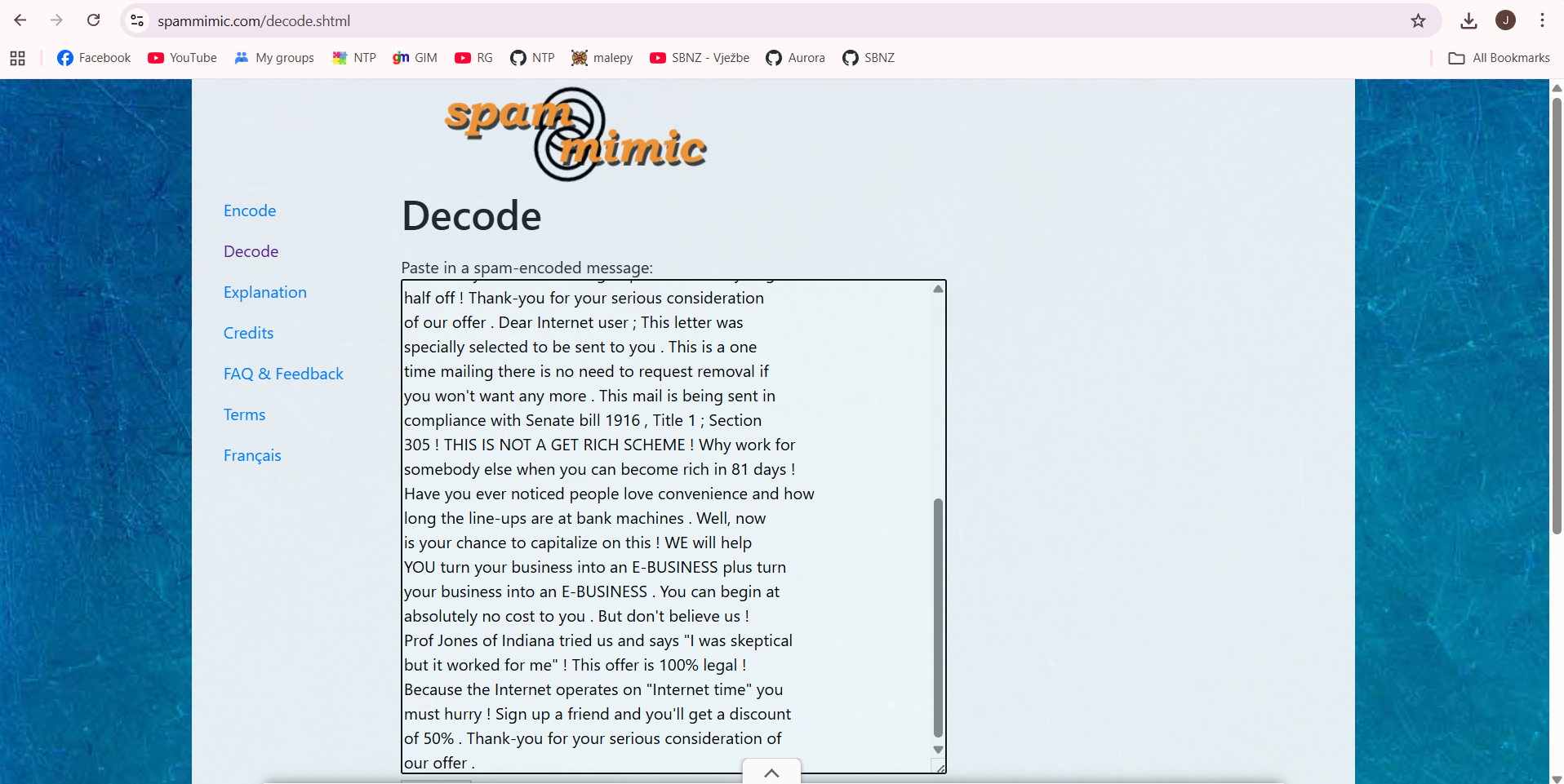
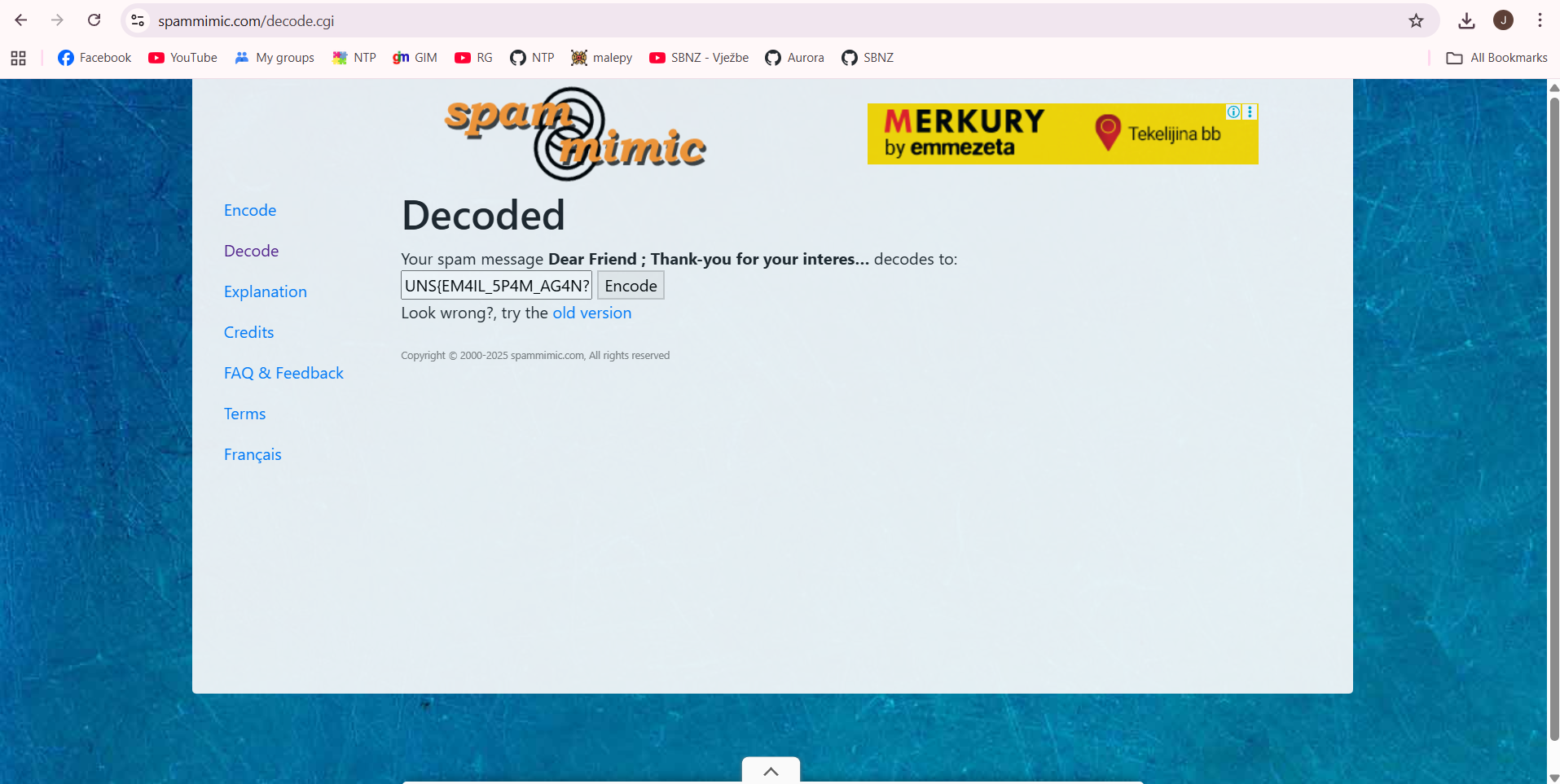
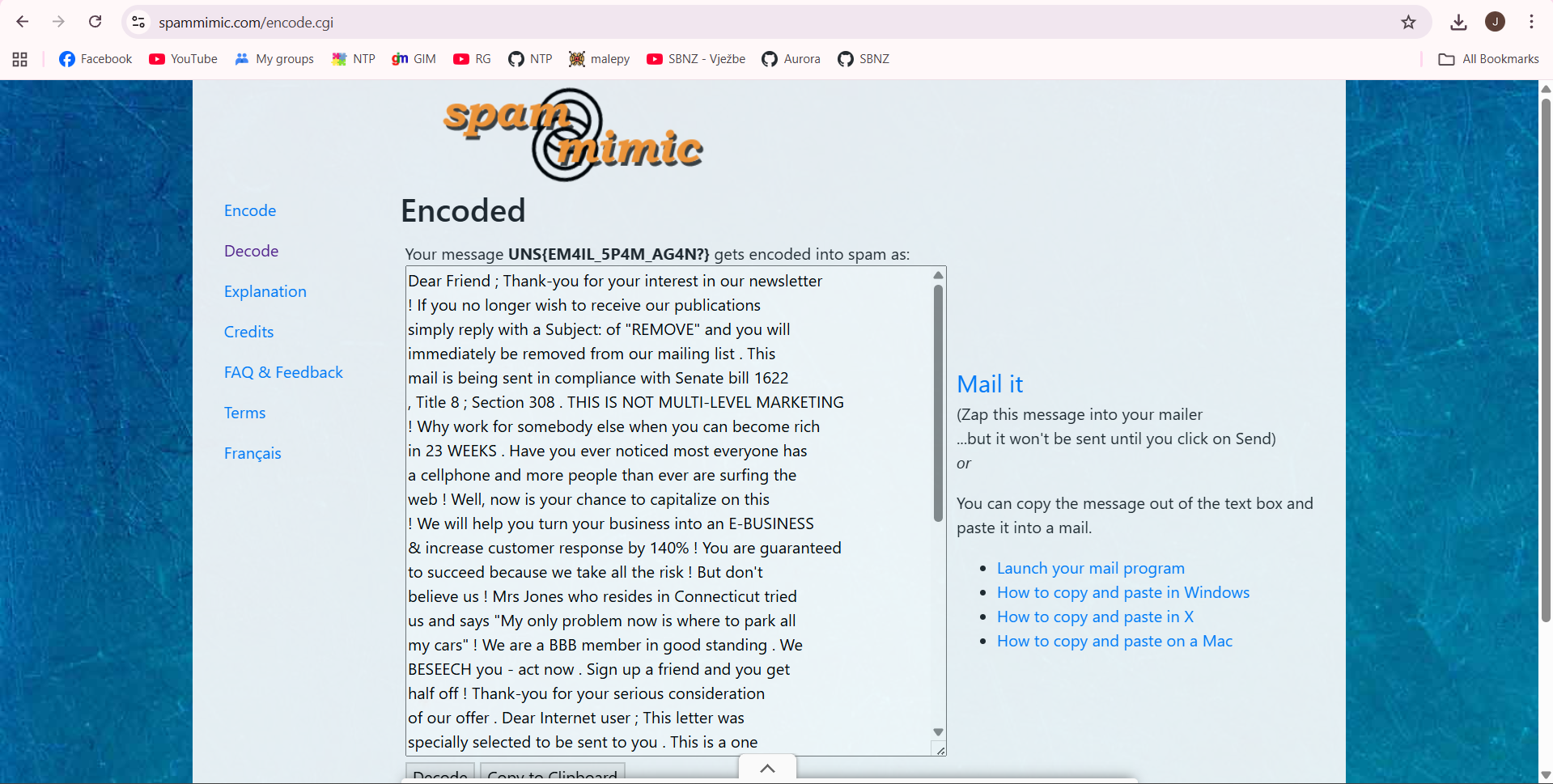
# Zadatak 4 - Nigerian Prince

Prvo što radimo jeste dekodiranje mejla pomoću alata [spammimic](https://www.spammimic.com/decode.cgi). Ovaj alat ima mogućnost dekoridanja sumnjivih imejl poruka i otkirivanja skrivenih poruka u njima.

Nakon izvršenog dekodiranja teksta imejl poruke, dobili smo sledeći flag: **UNS{EM4IL\_5P4M\_AG4N?}**



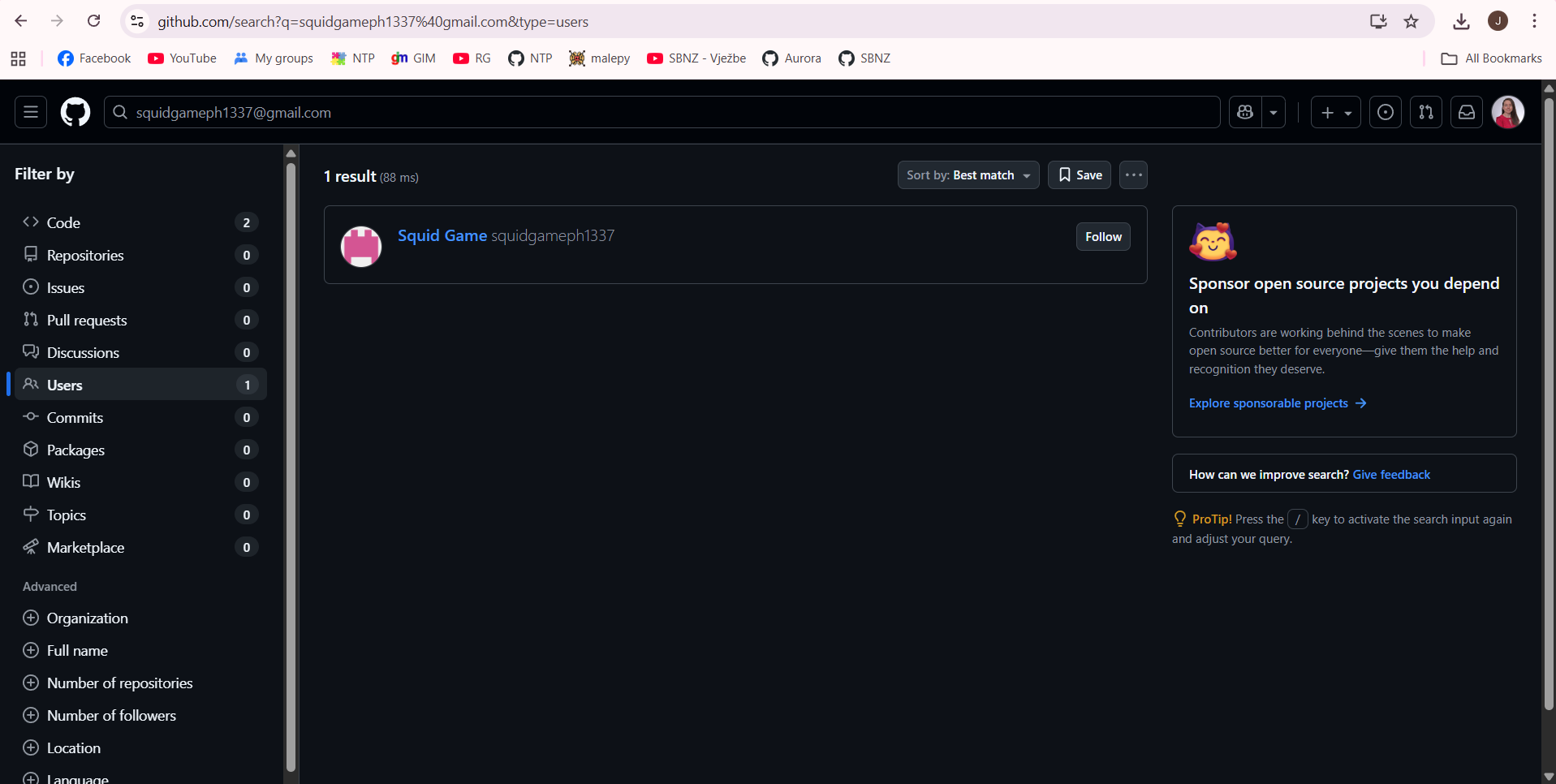


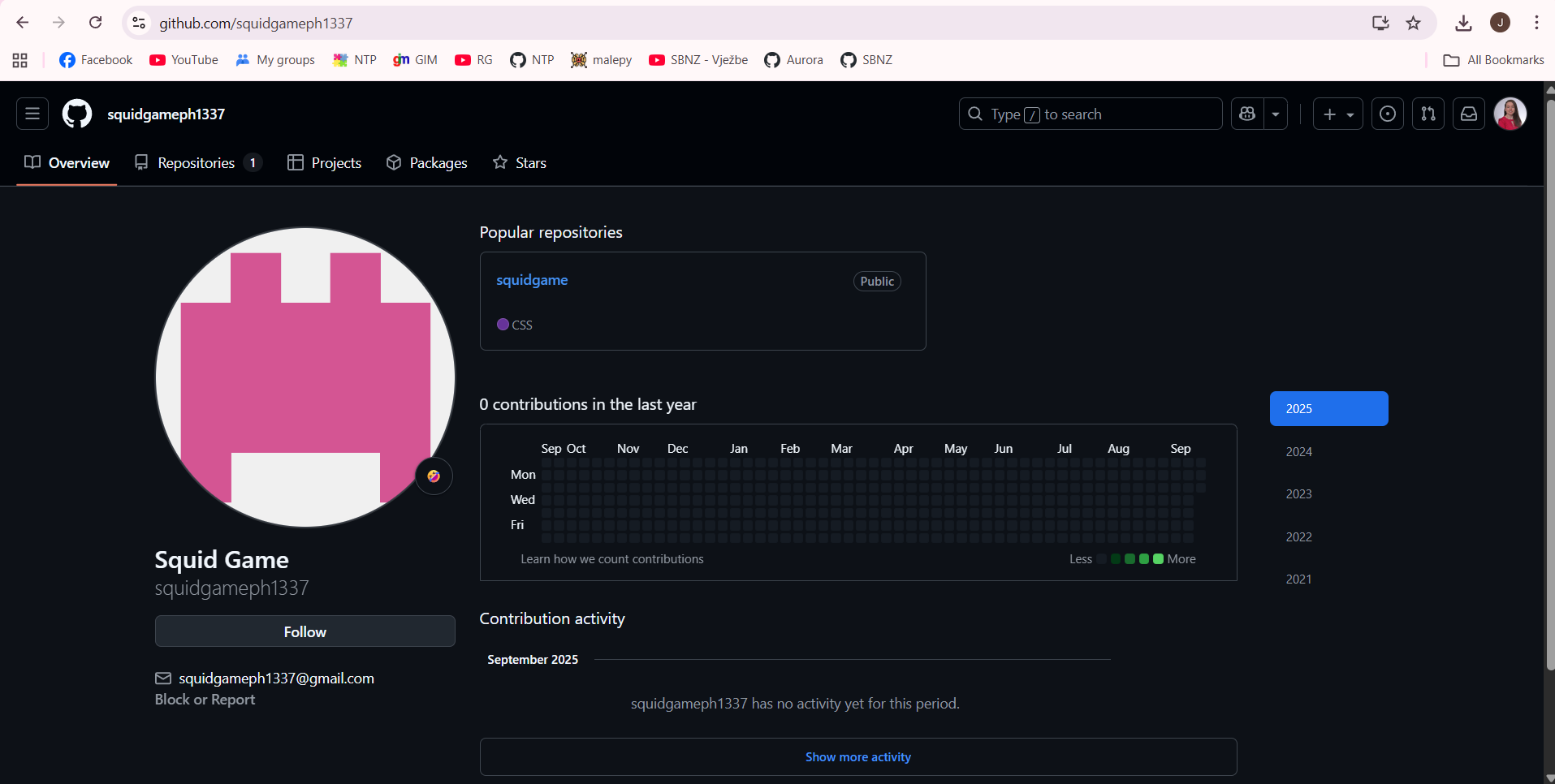


*Prikaz rezultata dekodiranja*

# Zadatak 8 - Squid Game Invitation

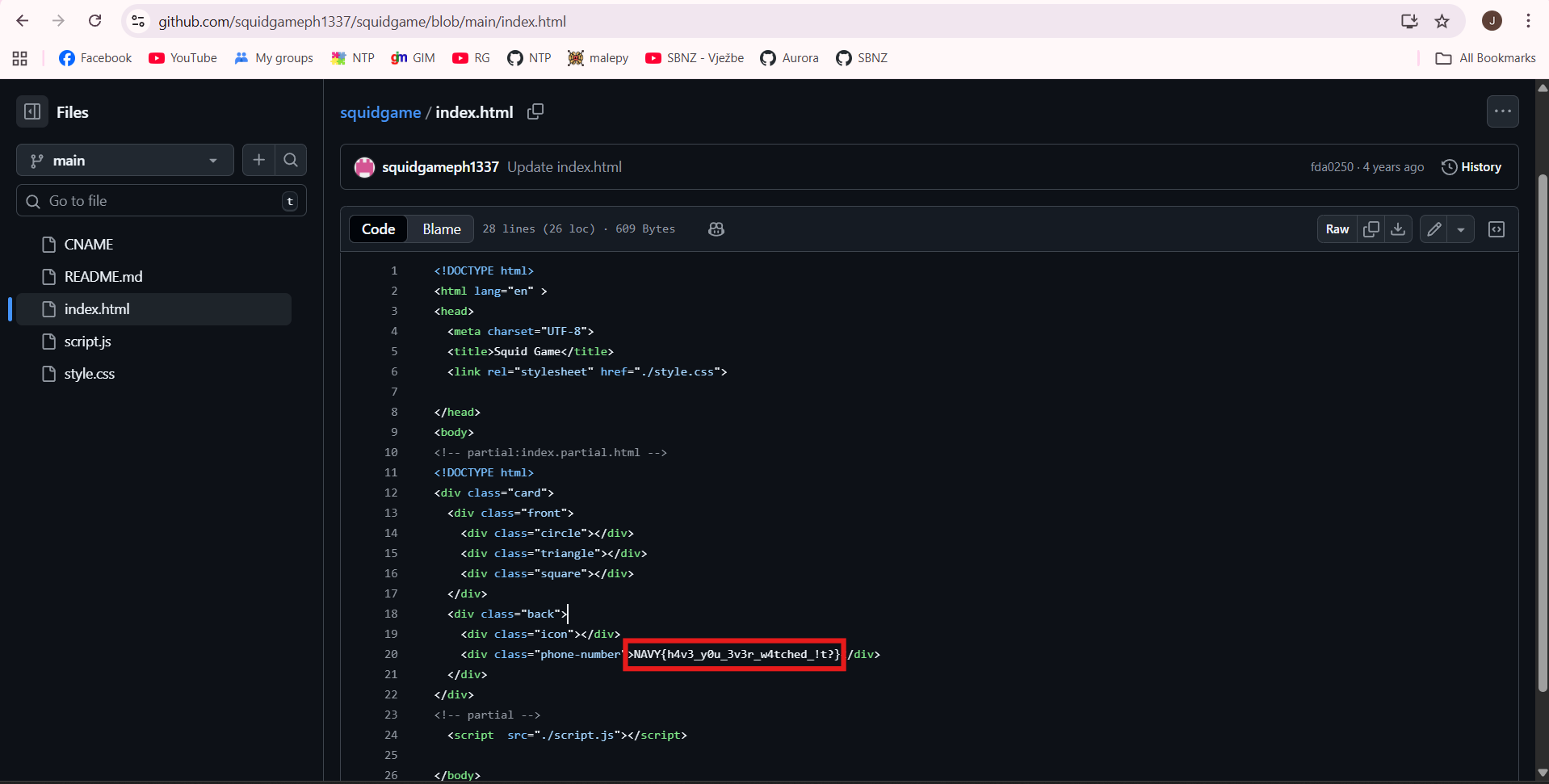
Na slici koju smo dobili uz zadatak uočili smo gmail adresu [squidgameph1337@gmail.com](mailto:squidgameph1337@gmail.com). Pretpostavili smo da se prvi deo gmail adrese mogao iskoristiti kao korisničko ime za registraciju na nekim onlajn servisima. Nakon provere nekoliko različitih onlajn servisa, pronašli smo nalog sa istim korisničkim imenom i imejl adresom na GitHub-u.





Na GitHub profilu korisnika *squidgameph1337* uočavamo jedan repozitorijum i ulazimo u njega kako bismo videli šta se tu nalazi.

Prošli smo kroz sve fajlove i u fajlu index.html smo uočili vrednost čiji format odgovara formatu flag-a koji se traži:



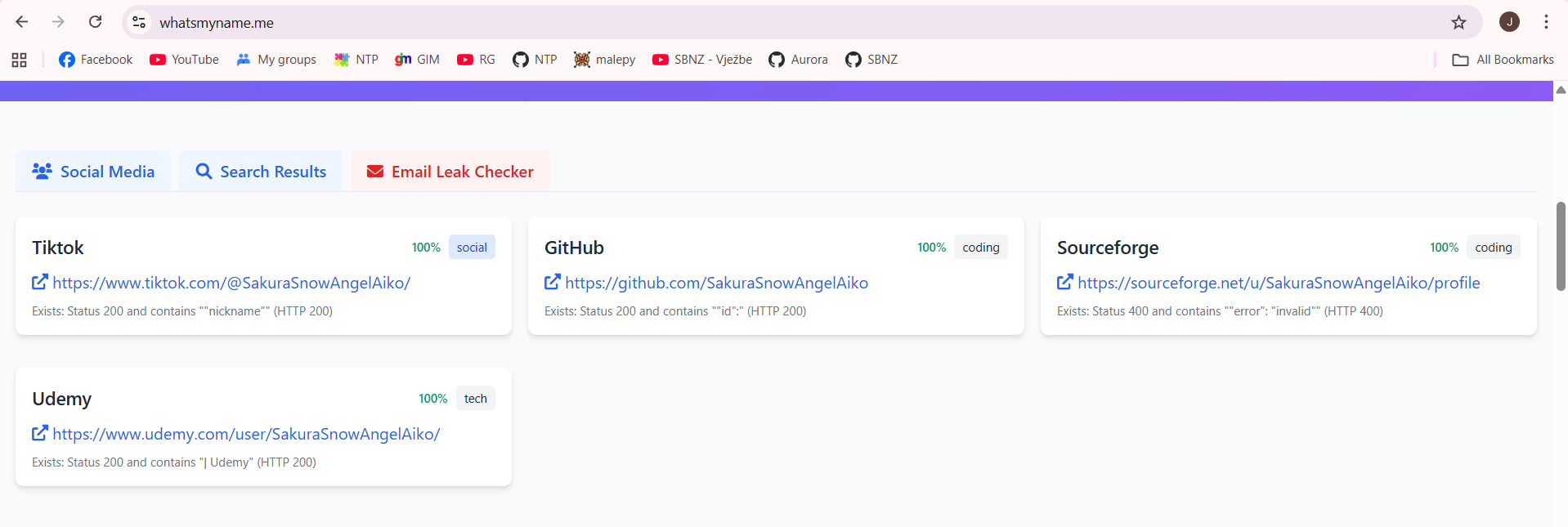
Vrednost traženog flag-a je: **NAVY{h4v3\_y0u\_3v3r\_w4tched\_!t?}**

# Sakura Challenge

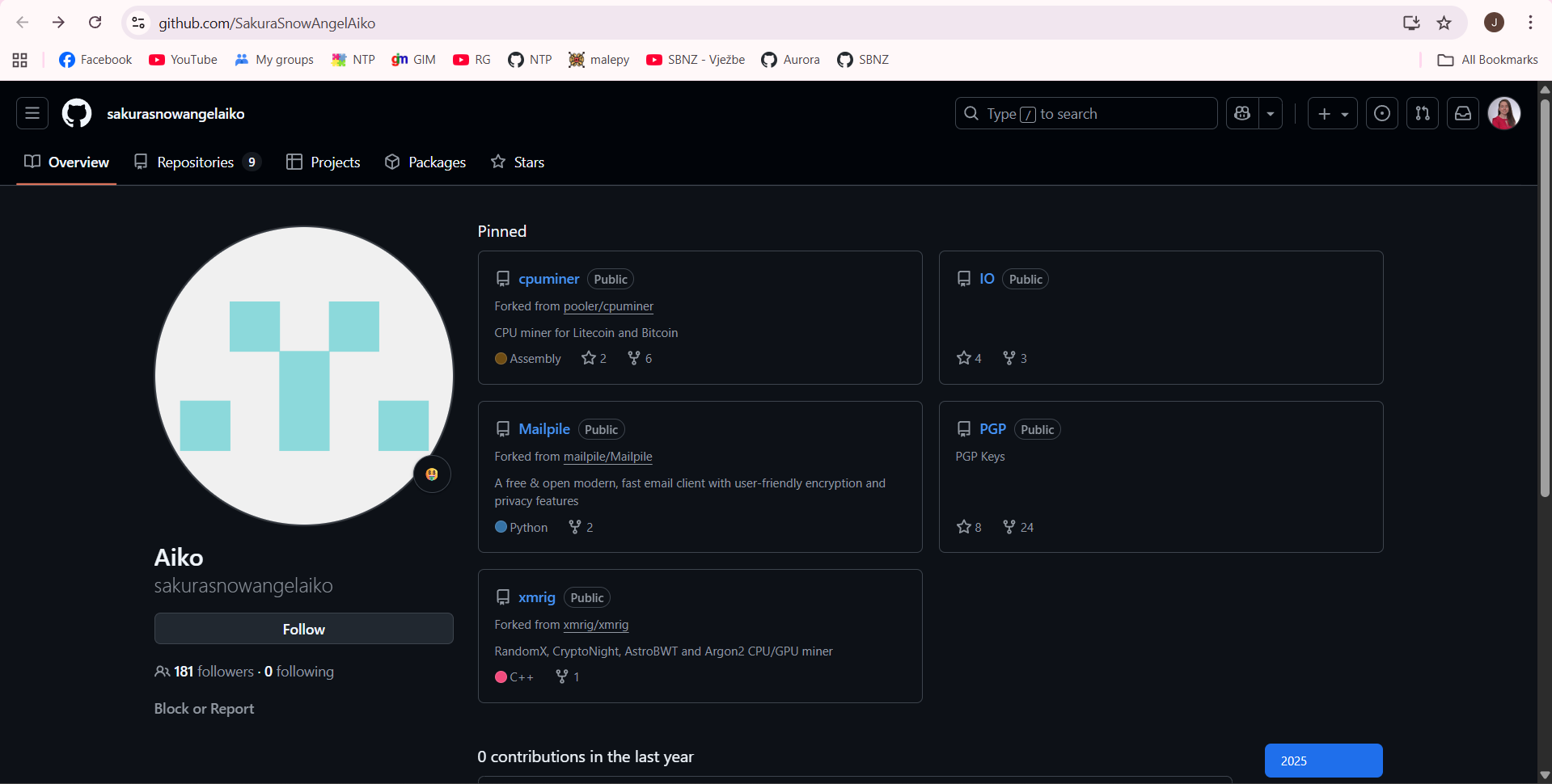
## Zadatak 3: RECONNAISSANCE

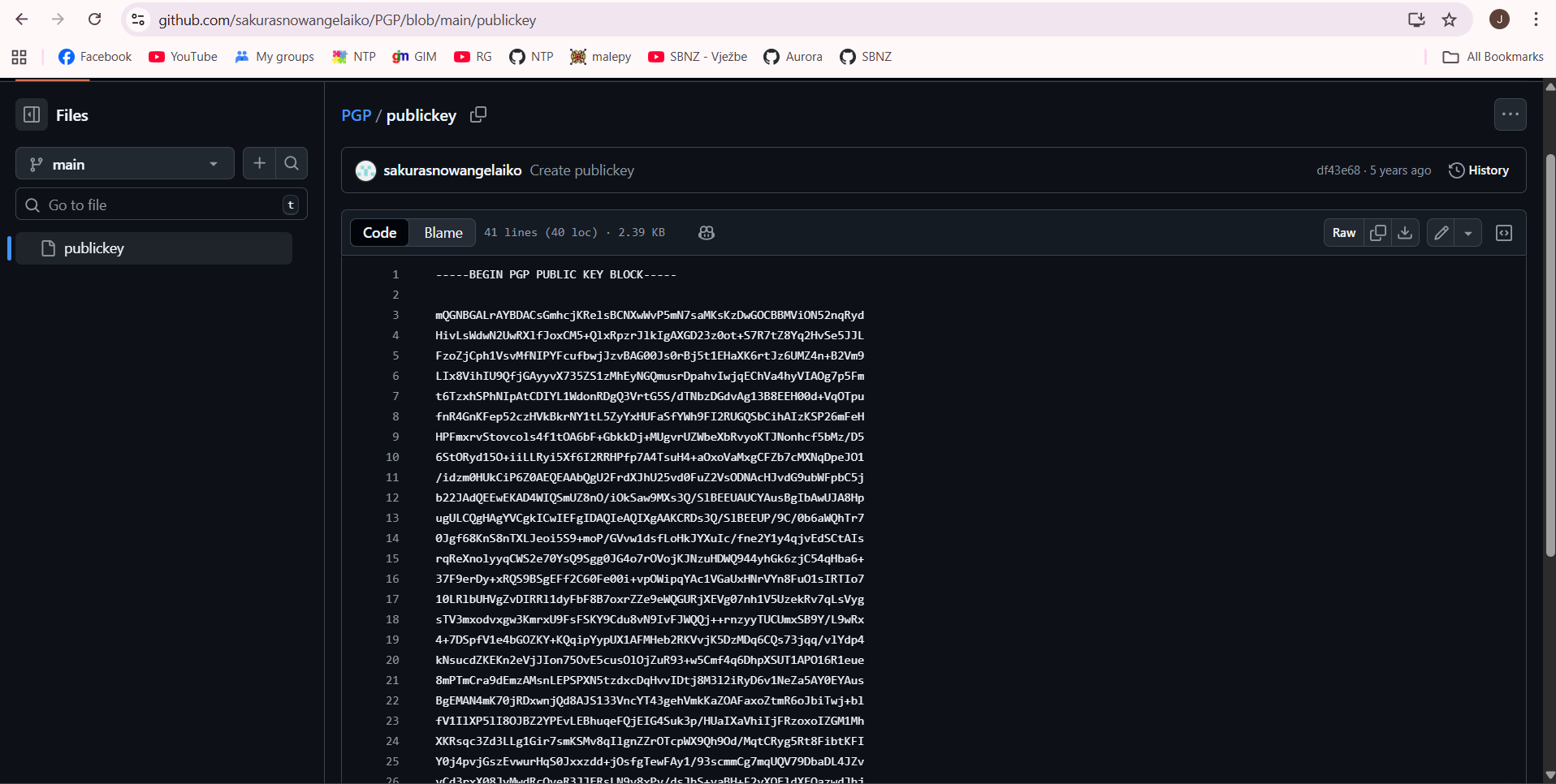
Cilj ovog zadatka je pronaći imejl adresu i puno ime napadača na osnovu njegovog korisničkog imena koje smo pronašli u Zadatku 2 (SakuraSnowAngelAiko).

Prvi korak je da pronađemo na kojim onlajn servisima postoji nalog sa takvim korisničkim imenom. Za tu namenu korišćen je alat [whatsmyname](https://whatsmyname.me/).



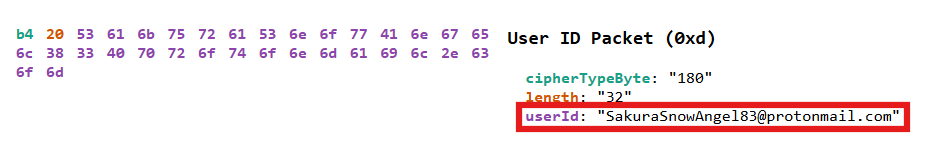
Nakon izvršene pretrage, vidimo da nalog sa istim korisničkim imenom postoji na nekoliko sajtova (TikTok, GitHub, SourceForge i Udemy). Posećujemo svaki od ponuđenih linkova i tražimo potrebne informacije. Na GitHub nalogu pronalazimo više repozitorijuma i proveravamo svaki od njih. U repozitorijumu GPG pronalazimo javni ključ napadača.





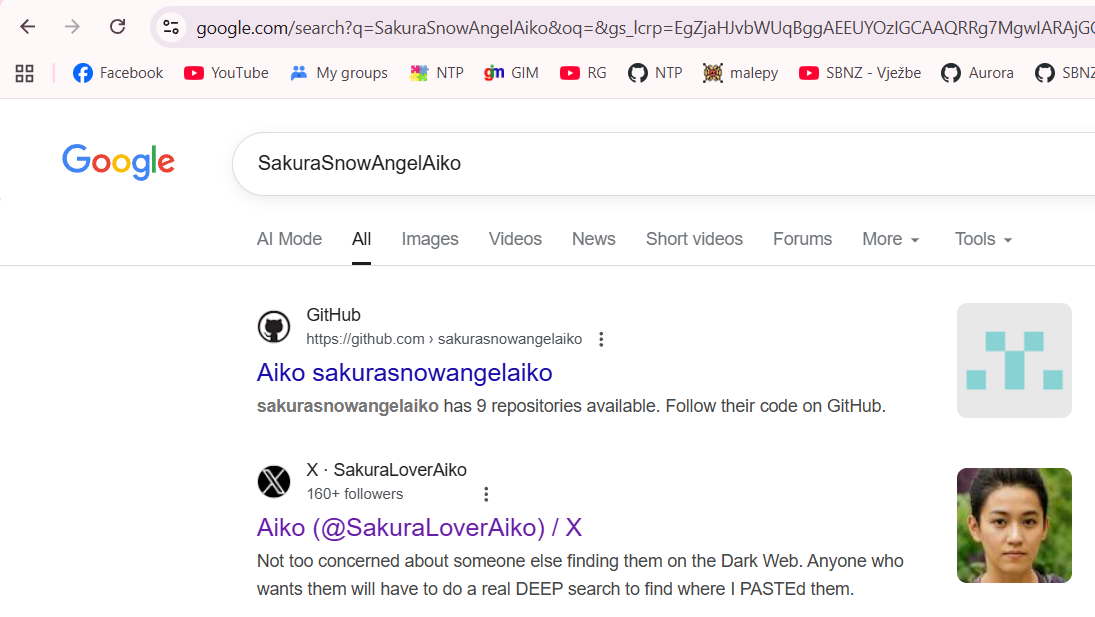
Kopirala sam ključ iz publickey fajla u repozitorijumu GPG i nalepila ga u onlajn alat za dekodiranje GPG ključeva [cirw](https://cirw.in/gpg-decoder/).

U jednom delu ključa je pronašao sledeću imejl adresu:

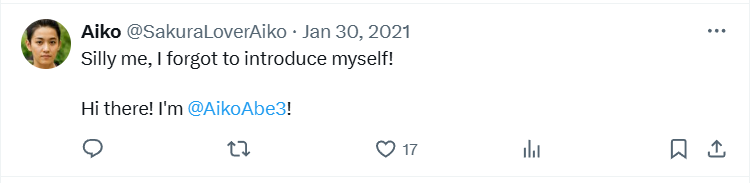


Uzimam tu imejl adresu i kopiram je u Sakuru.

Odgovor je tačan i time je ovaj deo zadatka rešen. Zatim prelazim na pronalazak punog imena napadača. Pošto nam pretraga korisničkog imena specijalizovanim alatom nije dala zadovoljavajuće rezultate za rešavanje ovog problema, odlučila sam da izvršim ručnu pretragu tako što ću izvršiti Gugl pretragu korisničkog imena.



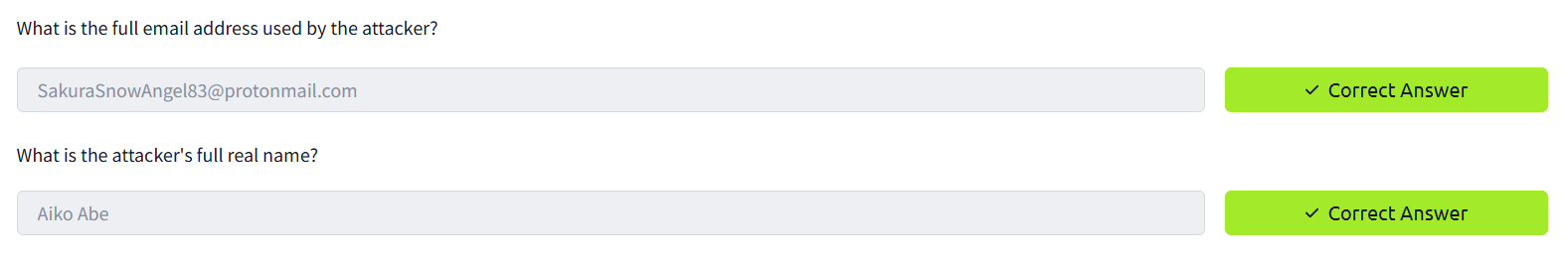
Postoji i X nalog sa istim korisničkim imenom, pa ulazim da proverim šta tu ima.



Napadač se u jednom postu predstavio kao AikoAbe3, pa ulazimo u taj nalog.



Pošto tu nema nikakvih novih informacija, pretpostavljam da je ime napadača Aiko Abe i to unosim u polje za odgovor u Sakura Room-u.



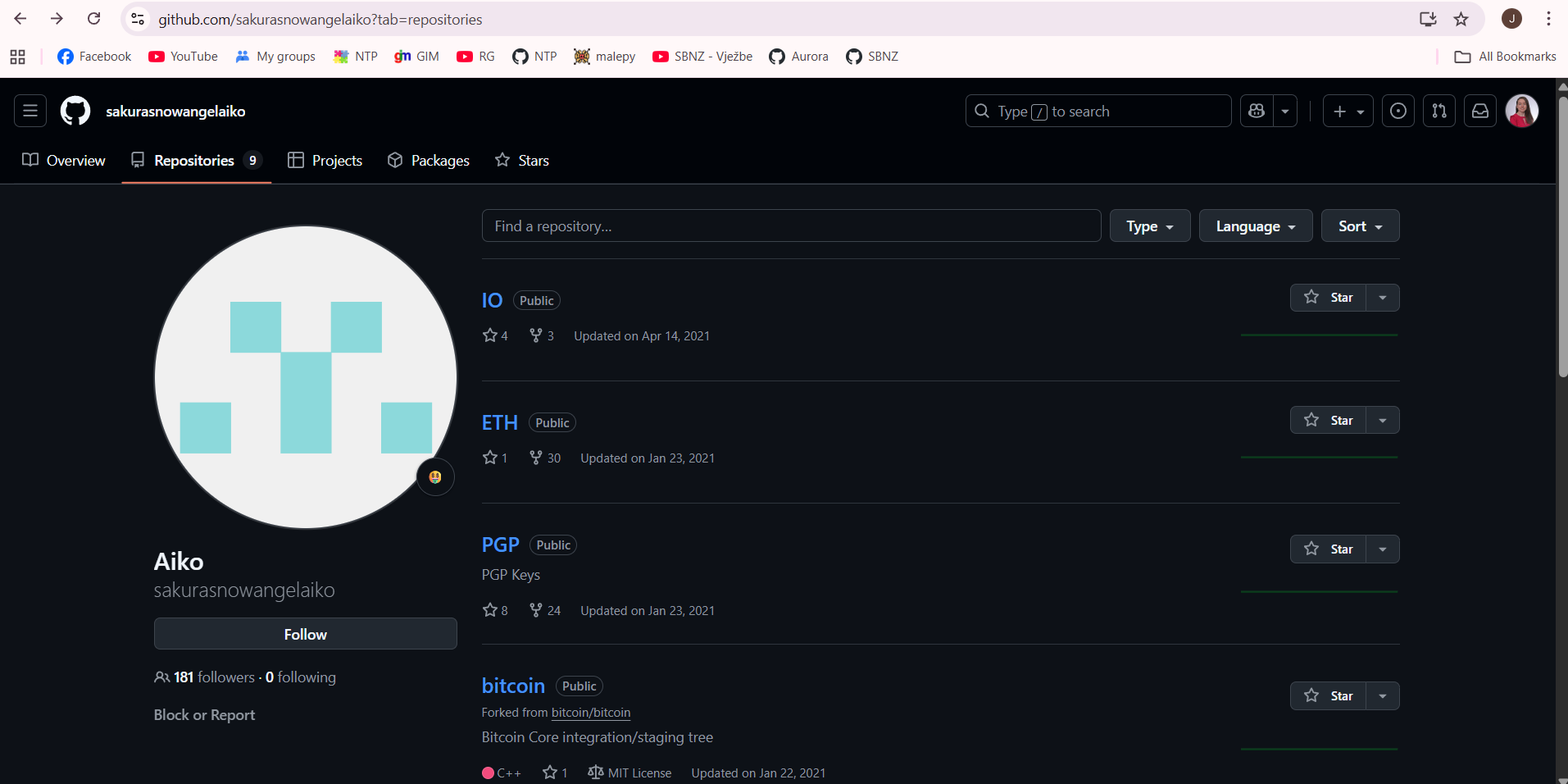
Odgovor je tačan i time je ovaj zadatak u potpunosti rešen.

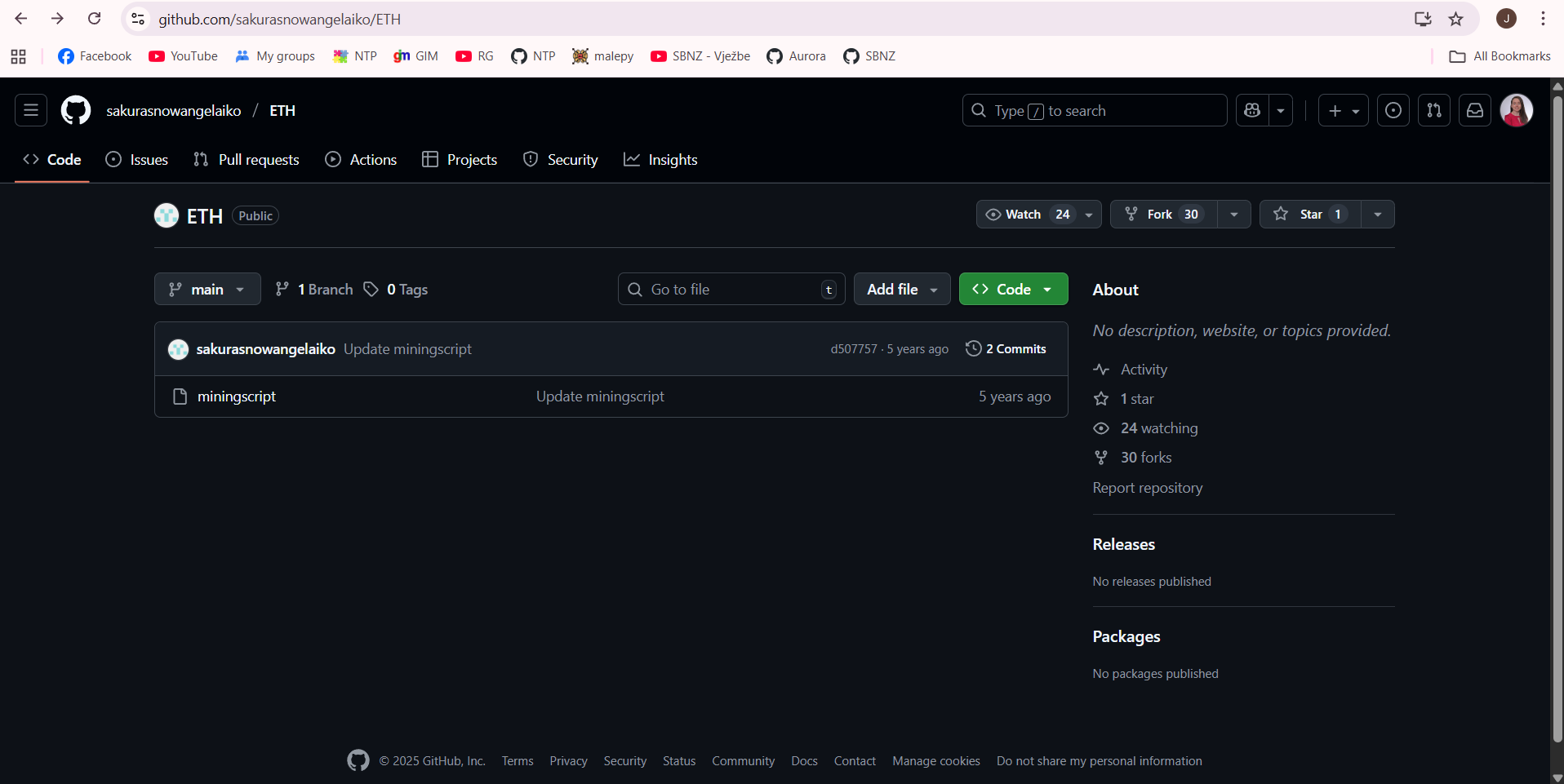
## Zadatak 4: UNVEIL

Cilj ovog zadatka je pronaći sledeće informacije o napadaču:

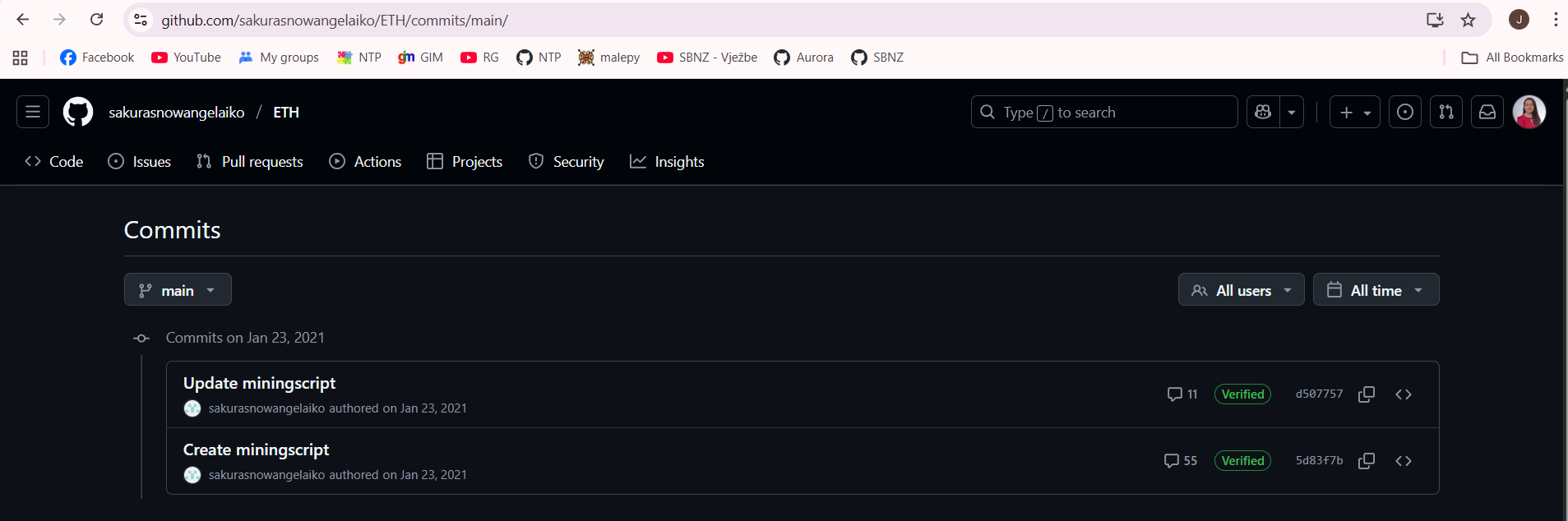
1. Za koju kriptovalutu napadač poseduje kripto-novčanik?
2. Koja je adresa kripto-novčanika napadača?
3. Od kog *mining pool*-a je napadač primio uplate 23. januara 2021. UTC?
4. Kojom drugom kriptovalutom je napadač trgovao (ili razmenjivao) koristeći svoj kripto-novčanik?

Pregledom GitHub naloga napadača, dolazimo do repozitorijuma ETH u kome se nalazi samo jedan fajl pod imenom miningscript.

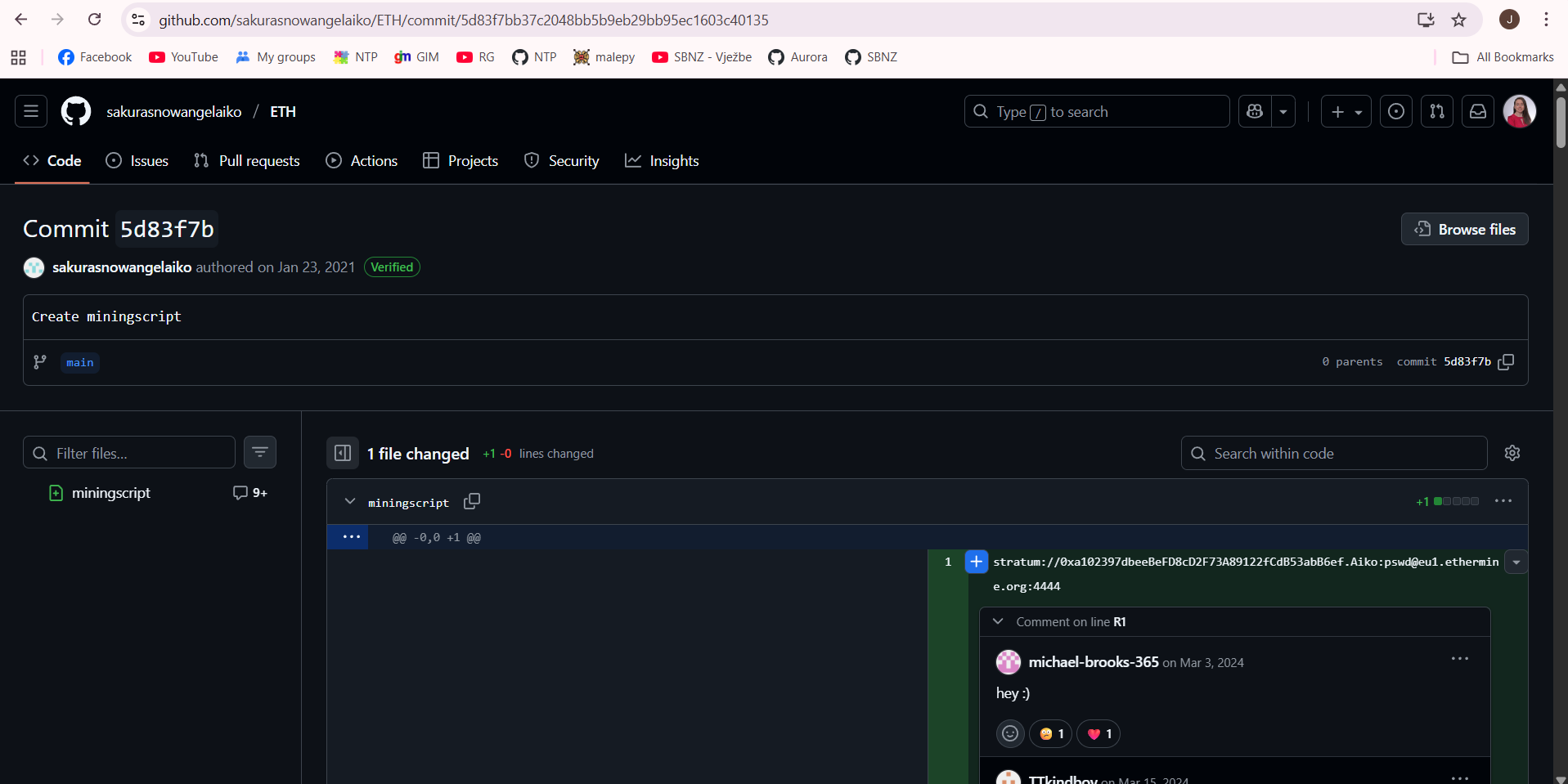




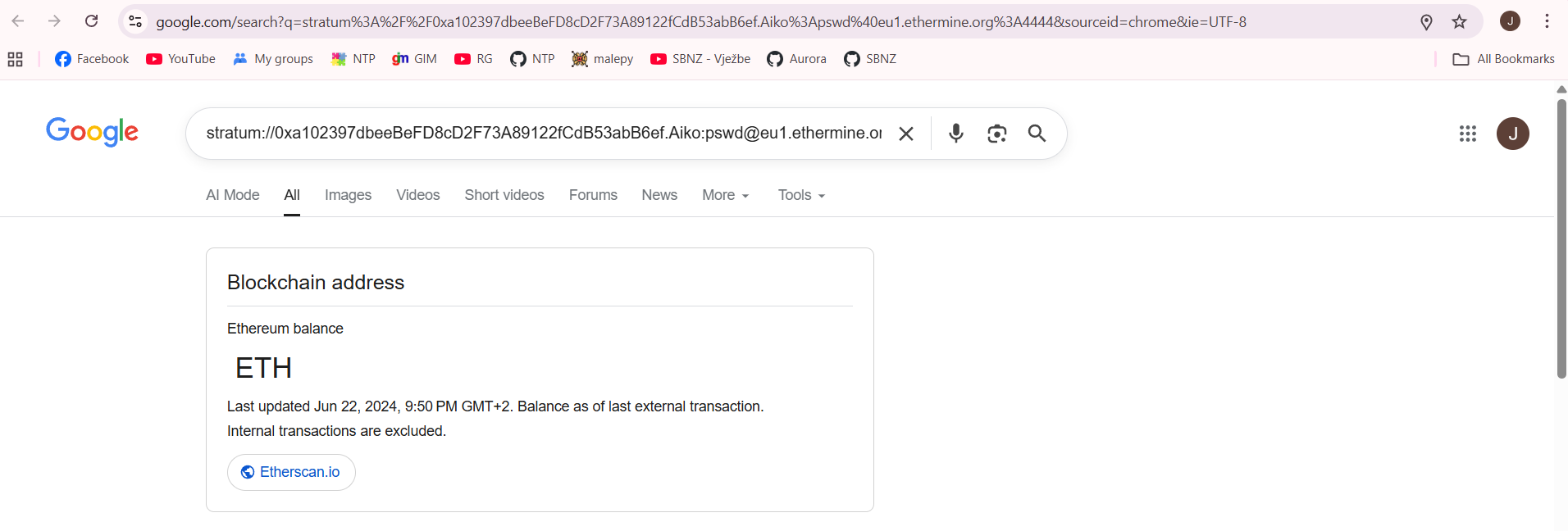
Vidimo da je bilo više od jednog *commit*-a u ovom repozitorijumu, pa ulazimo u istoriju *commit*-ova kako bismo videli da li u ranijim izmenama ima nečega što bi moglo da nam bude od koristi.



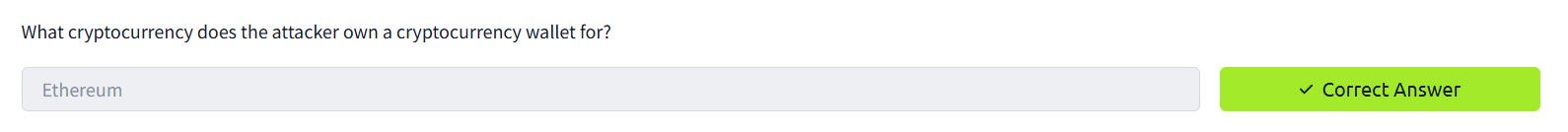
Ulazimo u prvi od ovih *commit*-ova kako bismo videli kako je izgledala inicijalna verzija *miningscript* fajla.



Uočavamo neki link i odlučujemo da ga kopiramo u browser.



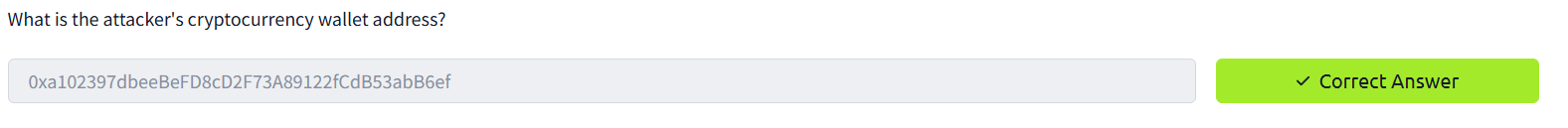
Prvi rezultat na Guglu nam kaže da je to *blockchain* adresa za *Ethereum* novčanik i to nam je odgovor na prvo pitanje. U Sakura Room-u kao odgovor na prvo pitanje unosimo “Ethereum” i proveravamo rezultat.



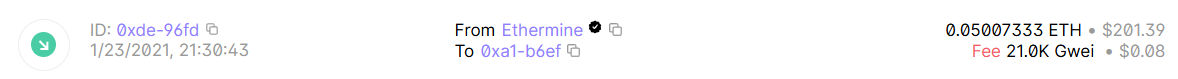
Ispostavilo se da je to tačan odgovor, pa prelazimo na sledeće pitanje.

Ulazimo na sajt [blockchain.com](https://www.blockchain.com/explorer/addresses/eth/0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef) otvara nam se kripto-novčanik napadača. U polju za URL imamo deo */adresses/0xa102397dbeebefd8cd2f73a89122fcdb53abb6ef* pa pretpostavljamo da je *0xa102397dbeebefd8cd2f73a89122fcdb53abb6ef* adresa kripto-novčanika napadača i to unosimo kao odgovor na drugo pitanje iz *Sakura Room*-a. Ispostavlja se da je to tačan odgovor.

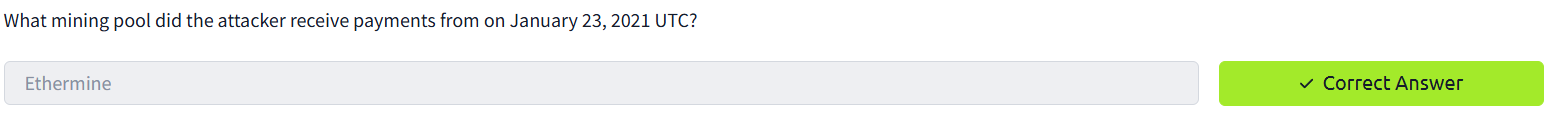




Kako bismo pronašli odgovor za treće pitanje, neophodno je da pregledamo istoriju transakcija na sajtu [blockchain.com](https://www.blockchain.com/explorer/addresses/eth/0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef) i pronađemo dolaznu transakciju sa datumom 23. Januar 2021. Godine.

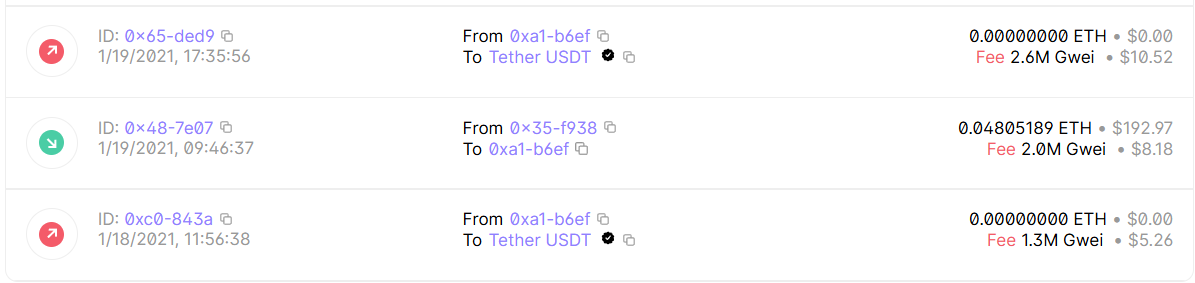


Pronalazimo dolaznu transakciju sa tim datumom i uočavamo da je pristigla od *mining pool*-a pod nazivom *Ethermine*, te to unosimo kao odgovor na treće pitanje u *Sakura Room*-u. To se ispostavlja kao tačan odgovor.



Kako bismo odgovorili na poslednje pitanje, neophodno je da još jednom prođemo kroz istoriju transakcija.

Uočavamo da je napadač više puta izvršio konverzije iz ETH u Tether USDT, te odlučujemo da isprobamo Tether kao odgovor u Sakura Room-u.



To se ispostavilo kao tačan odgovor i time je ovaj zadatak u potpunosti rešen.

