SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

**Antonio Valentić**

**Josipa Vresk**

**Hrvoje Vujasinović**

**Bruno Žitković**

**CTF-ovi u kontekstu edukacije o sigurnosti; implementacija vlastitog edukativnog ctf-a**

projektni rad

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Antonio Valentić - 0016133923

Josipa Vresk - 0016130227

Hrvoje Vujasinović - 0231042668

Bruno Žitković - 0016130386

Studij: Informacijsko i programsko inženjerstvo, Baze podataka i baze znanja

NASLOV ZAVRŠNOG/DIPLOMSKOG RADA

ZAVRŠNI/DIPLOMSKI RAD

Mentor/Mentorica:

Doc. dr. sc. Igor Tomičić

Varaždin, siječanj 2021.

*Antonio Valentić*

*Josipa Vresk*

*Hrvoje Vujasinović*

*Bruno Žitković*

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

*Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sadržaj

[Sadržaj iv](#_Toc61301851)

[1. Uvod 1](#_Toc61301852)

[2. CTF natjecanja 2](#_Toc61301853)

[2.1. Napad-obrana natjecanje 3](#_Toc61301854)

[2.2. „Jeopardy-style“ natjecanje 3](#_Toc61301855)

[3. Tipovi zadataka 4](#_Toc61301856)

[3.1. Kriptografija 4](#_Toc61301857)

[3.2. Steganografija 4](#_Toc61301858)

[3.3. Binarno manipuliranje 5](#_Toc61301859)

[3.4. Digitalna forenzika 6](#_Toc61301860)

[3.5. Eksploatacija web-a 6](#_Toc61301861)

[3.6. Obrnuto inženjerstvo 7](#_Toc61301862)

[4. Alati 8](#_Toc61301863)

[5. Primjer CTF-a 10](#_Toc61301864)

[5.1. Zar i ti, sine Brute? 10](#_Toc61301865)

[5.2. Dođoh, vidjeh, pobjedih 12](#_Toc61301866)

[5.3. Pazi se morskog psa 14](#_Toc61301867)

[5.4. Ime je znamen 17](#_Toc61301868)

[5.5. Kakav život, takva smrt 19](#_Toc61301869)

[6. Zaključak 22](#_Toc61301870)

[Popis literature 23](#_Toc61301871)

[Popis slika 24](#_Toc61301872)

1. Uvod

Tema ovog projektnog rada je CTF-ovi u kontekstu edukacije o sigurnosti te implementacija vlastitog edukativnog ctf-a. Puni naziv je „Capture the flag“ što u prijevodu znači „Zauzmi zastavu“. CTF je vrsta natjecanja iz područja informacijske sigurnosti kojoj se može pristupiti samostalno ili u timu, a je cilj rješavanje različitih problemskih zadataka i pronalaženje određenog teksta koji se naziva „zastavica“.

Tipovi zadataka koji se mogu pronaći na CTF natjecanjima, a vezani su za područje informacijske sigurnosti su kriptografija, steganografija, te ostali zadaci vezani uz pronalaženje puta do nečijih podataka. Zadaci težinski mogu varirati, od najjednostavnijih do onih najtežih za koje je potrebna vještina profesionalaca.

U početnom dijelu projekta će biti razrađen teorijski dio koji stoji iza CTF-a, a u drugom dijelu rada prikazat ćemo vlastitu implementaciju teorijskog dijela u području CTF-a korištenog u edukativne svrhe.

1. CTF natjecanja

U posljednjih nekoliko godina broj cyber napada je u porastu, da bi se odgovorilo na te napade, informacijski profesionalci u području sigurnosti, ali i studenti prolaze kroz zahtjevne treninge kako bi shvatili način na koji hakeri upadaju u sustav i kako bi se naučili obraniti od takvih napada.

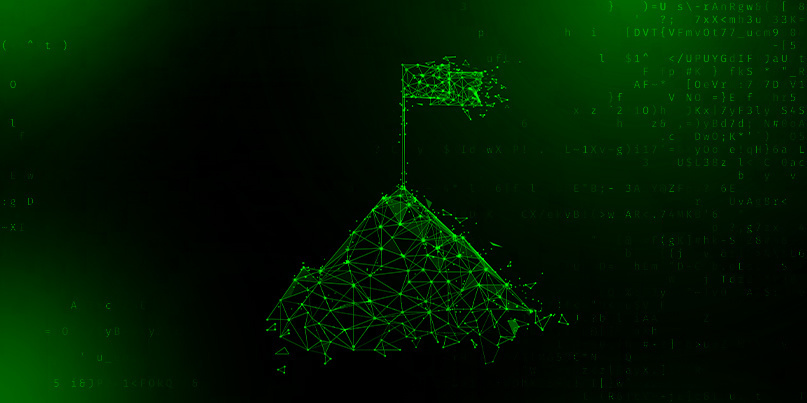
CTF natjecanja koriste se kao alat za učenje i omogućuje svim sudionicima proširivanje znanja iz područja informacijske sigurnosti. Prvo tako natjecanje održalo se u Las Vegasu na DEFCON konferenciji 1996. godine. DEFCON je postao platforma za unapređivanje znanja iz raznih područja, raznih informacijskih vještina. CTF natjecanja su postala popularna jer nisu ograničena mjestom. 3 najpoznatija CTF natjecanja su:

* Insomni'hack - koje se održava u Ženevi
* 0CTF/TCTF - organiziran on Shanghai Jiao Tong sveučilišta
* GoogleCTF- organiziran od Google-a

Postoje 2 tipa CTF natjecanja, napad-obrana, „Jeopardy-style“. [1]

Vještine poželjne za pristupanje CTF natjecanjima su [2]:

* Osnovna znanja o računalima
* Osnovne vještine programiranja
* Poznavanje osnova računalnih mreža
* Vještine kreativnog rješavanja problema
* Vještine istraživanja o problemu



Slika 1: CTF zastavica [1]

* 1. Napad-obrana natjecanje

Tip CTF natjecanja napad-obrana temelji se na tome da jedan tim napada sustav drugog tima i obrnuto, ali istovremeno i brane svoj sustav. Najčešće se natjecanje sastoji od 2 runde, gdje se u jednoj rundi jedan tim brani, a u drugoj rundi napada, i obrnuto. Postoje tzv. „zastavice“ koje mogu biti:

* Tekstualne datoteke
* Datoteke
* Slike

Zastavice su na sustavu kojeg se napada koje napadački tim pokušava pronaći prilikom napada na sustav i ugroziti sustav branitelja. Napadački tim ima različite alate na raspolaganju kako bi uspjeli ugroziti sustav obrambenog tima, ali isto tako postoje određena pravila kako bi se osigurala regularnost natjecanja. [1]

* 1. „Jeopardy-style“ natjecanje

„Jeopardy-style“ tip natjecanja je sličan „jeopardy“ igri, gdje postoji tablica u kojoj su pitanja iz različitih kategorija. U ovom tipu natjecanja može sudjelovati dva ili više timova zato što jedni ne napadaju druge. A kategorije koje se najčešće pojavljuju su:

* Kriptografija
* Steganografija
* Sigurnost fizičkog sloja i skeniranje

Neki od izazova odnose se na pobjeđivanje glavnog servera razvijenog za to natjecanje te se rješavanjem zadatka dobivaju bodovi koji su zatim uneseni u tablicu bodova. Na početku natjecanja pokreće se vremenski brojač koji kada dođe do kraja i samo natjecanje završava te tim koji u tom trenutku ima najviše bodova je pobjednik. [1]

1. Tipovi zadataka

Tipovi zadataka koji se mogu pojaviti na ranije spomenutim vrstama natjecanja su najčešće zagonetke ili pitanja vezana uz kriptografiju, steganografiju, binarno manipuliranje (eng. *Binary Exploitation*), digitalnu forenziku, eksploataciju web-a, obrnuto inženjerstvo i mnogi drugi.

* 1. Kriptografija

Zadaci kriptografskog tipa se sastoje od razbijanja nekog kriptografskog koda. Natjecatelju je zadan šifrirani tekst koji on zatim pokušava dešifrirati u originalnu poruku ili se dobije tekst koji je potrebno sažeti korištenjem algoritma za sažimanje. [3]

Neka od pitanja koja se mogu pojaviti su sljedeća:

* Koja je originalna poruka koja je šifrirana kao: „PREBAODRAGASWIBKNDSSI“?
* Koja je poruka: „--- ..- .-. -. . -..- - - .- .-. --. . - .. ... -... .- -. -.- --- ..-. .- -- . .-. .. -.-. .-“?

Kako bi našao zastavice, natjecatelj mora primijeniti određenu tehniku dekriptiranja. Npr. „Rail Fence“ šifru s ključem 4 na prvom pitanju. Dok drugo pitanje koje je ranije spomenuto predstavlja Morseov kod te natjecatelj mora pronaći pravi odgovor iz tog koda. [4]

* 1. Steganografija

Zadaci stenografskog tipa uče natjecatelje sakrivanju poruka unutar određenih objekata. Primjer jednog stenografskog zadatka je sljedeći:



Slika 2: Sakrivena riječ „root“ [2]

Na slici 2. možemo vidjeti kako je na šahovskoj ploči sakrivena riječ „root“ sastavljena od šahovskih figurica. Također, još jedan primjer steganografije je prikazan na slici 3. gdje je poruka napisana u zrcaljenom obliku.



Slika 3: Zrcaljeni tekst na slici [2]

* 1. Binarno manipuliranje

Binarno manipuliranje podrazumijeva pronalaženje ranjivosti unutar nekog određenog programa. Tipično se ta ranjivost nalazi unutar UNIX sustava te je cilj eksploatirati tu ranjivost kako bi se pronašla zastavica.

Takva eksploatacija obično podrazumijeva korištenje nekog programa kako bi se dobila mogućnost pristupa shell-u ili neko modificiranje istog za pristupanje sakrivenoj zastavici [3]

Neke od najčešćih tema koje se binarno manipuliranje dotiče su manipuliranje registrima, stogom, „bufferima“, hrpom itd. [5]

* 1. Digitalna forenzika

Zadaci digitalne forenzike mogu se podijeliti u nekoliko kategorija, a neke od najčešćih su sljedeće:

* Analiza formata
* Steganografija
* Analiza memorije
* Analiza mrežnih paketa

Svaki zadatak koji u sebi sadrži neki oblik istraživanja, tj. procesuiranje određenog oblika informacije može se smatrati zadatkom iz digitalne forenzike jer je forenzika dosta široko područje koje može imati više različitih tipova zadataka.

Neke od vještina koje su potrebne za rješavanje zadataka iz digitalne forenzike uključuju znanja iz:

* Poznavanje skriptnog jezika
* Poznavanje manipulacije podataka
* Prepoznavanje formata, protokola, struktura itd.

Poznavanje skriptnog jezika i poznavanje manipulacije podataka se najčešće uči izvan CTF-a, ali prepoznavanje formata, protoka itd. se najčešće steče sudjelovanjem na CTF natjecanjima i rješavanjem zadataka takvog tipa. [6]

* 1. Eksploatacija web-a

Zadaci koji se dotiči eksploatacije web mjesta uključuju dobivanje zastavice tako što se pretražuje web i rješavaju određeni problemi koji uključuju [3]:

* SQL injektiranje
* Pregledavanje HTML elemenata
* Navigacija direktorija
* XSS
* Injektiranje naredbi
  1. Obrnuto inženjerstvo

Zadaci iz obrnutog inženjerstva koji se nalaze u CTF natjecanjima najčešće se dotiču toga da se dobije kompajlirani program, a zatim je cilj iz tog programa dobiti izvorni kod koji je čitljiv čovjeku kako bi se došlo do zastavice. [7]

Kod koji se dobije je najčešće dobiven u sljedećim programskim jezicima:

* Assembly
* C
* Java

Isto tako u većini slučajeva natjecatelju koji sudjeluje u CTF natjecanju, i zadan mu je zadatak obrnutog inženjerstva, ne dobije izvorni kod nego samo izvršnu verziju tog koda. Kako bi se taj problem riješio koriste se tzv. „dekompajleri“ koji onda taj izvršni kod pretvaraju natrag u izvorni. [3]

1. Alati

Postoji velik broj alata koji mogu poslužiti u rješavanju ranije navedenih tipova zadataka na CTF natjecanjima. Neki od tih alata će biti navedeni u nastavku teksta i bit će kategorizirani po tipu zadatka za koji su namijenjeni.

**Kriptografija**

* CyberChef - web alat za analizu i dekodiranje podataka
* FeatherDuster - automatizirani, modularni alaz za kriptoanalizu
* Hash Extender - alat za izvođenje napada produljenjem hash dužine
* Padding-oracle-attacker - CLI alat za izvršavanje padding-oracle napada
* PkCrack - alat za razbijanje PkZip enkripcije
* QuipQuip - online alat za razbijanje zamjenskih šifri ili šifri bez ključa

**„Brute-force“**

* Hashcat - alat za razbijanje lozinki
* Hydra - paralelizirani alat za prijavu koji podržava brojne protokole za napad
* John the Jumbo - verzija John the Ripper alata s nadogradnjama zajednice
* John the Ripper - alat za razbijanje lozinki
* Nozzlr - "brute-force" okvir

**Eksploatacija**

* DLLInjector - injektiranje dll-ova u procese
* Libformatstr - biblioteka za eksploataciju formata stringova
* Metasploit - softver za penetracijsko testiranje
* V0lt - sigurnosni CTF alati

**Digitalna forenzika**

* Audacity - analizira zvukovne datoteke
* CFF Explorer - PE uređivač
* Fibratus - alat za istraživanje i praćenje Windows kernel
* Malzilla - alat za lov malwera
* Wireshark - analiza pcap i pcapng datoteka

**Mreže**

* Masscan - alat za masovno skeniranje IP portova i TCP portova
* Nipe - skripta za postavljanje Tor mreže kao zadanog mrežnog izlaza
* Monit - Linux alat za provjeru domaćina na mreži
* Nmap - alat otvorenog koda za istraživanje mreže
* Wireshark - alat za analizu mrežnog prometa

**Obrnuto inženjerstvo**

* Androguard - obrnuto inženjerstvo Android aplikacija
* Angr - platformski agnostično programsko okružje za analizu programskog koda
* ApkTool - Android dekompajler
* Barf - programsko okružje za analizu i obrnuto inženjerstvo programskog koda

**Steganografija**

* Convert - alat za konverziju slika između različitih formata
* Exif - alat za pregled EXIF informacija na JPEG datotekama
* Steganabara - alat za steganografsku analizu
* Stegsolve - alat za primjenu steganografskih tehnika na slike
* Zsteg - alat za PNG/BMP analizu

**Web**

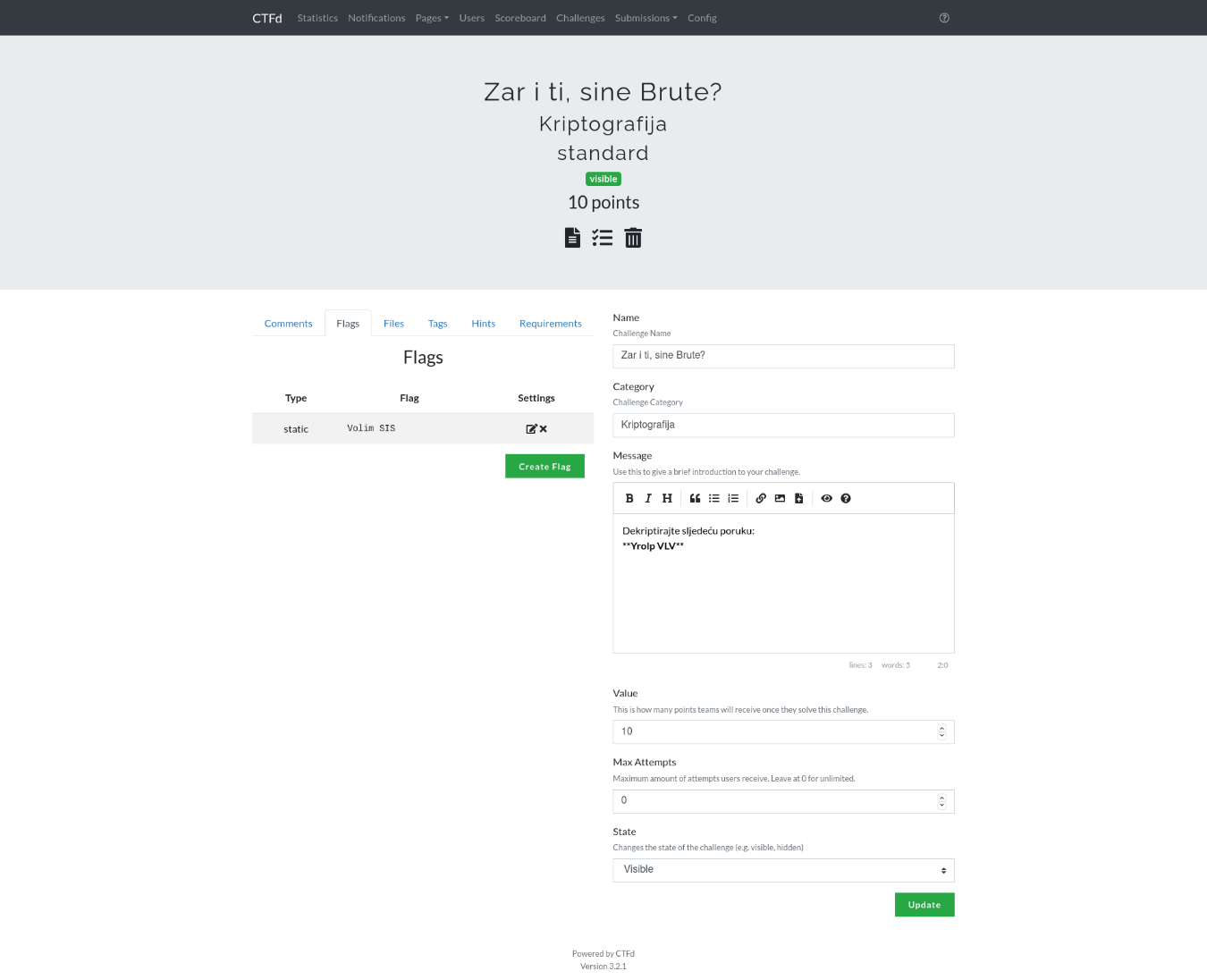
* BurpSuite - grafički alat za testiranje web sigurnosti
* Commix - automatizirani alat za injektiranje OS naredbi
* Hackbar - Firefox dodatak za jednostavnu web ekspoataciju
* SQLMap - automatizirani alaz za SQL injektiranje
* Postman - softver za debugiranje mrežnih poziva

1. Primjer CTF-a

U praktičnom dijelu rada prikazana je implementacije jednostavnog CTF-a koji se sastoji od 5 zadataka različitih tipova te može biti korišten u edukacijske svrhe s obzirom na to da kao pomoć sadrži linkove na stranice na kojima se može naučiti o temi vezanoj uz određeni zadatak.

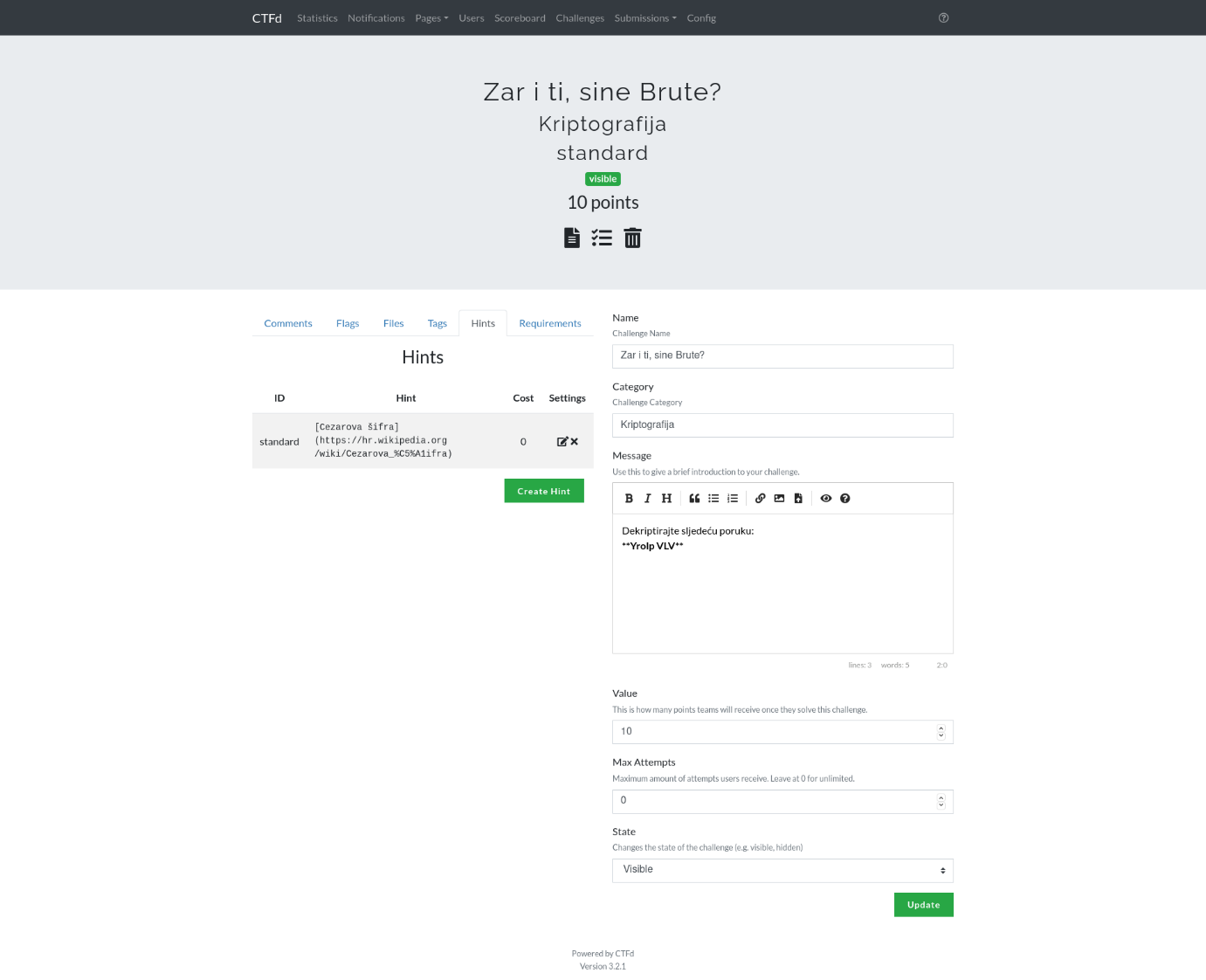
Edukativni CTF građen je na platformi otvorenog koda [8]. Korišteno je korisničko sučelje platforme zbog ljepšeg i jednostavnijeg prikaza postavljenih izazova koji su u potpunosti samostalno realizirani.

U nastavku ćemo prikazati implementaciju pojedinog zadatka izrađenog u ranije spomenutoj platformi te način rješavanja istog.

* 1. Zar i ti, sine Brute?

Slika 4: Prikaz zadatka kriptografije, prvi dio [3]

Prvi zadatak pripada kategoriji kriptografije i vrijedi 10 bodova, a kako izgleda postavljen u alatu CTFd možemo vidjeti na slici 4 i 5. U zadatku se traži da se dekriptira poruka koja glasi: Yrolp VLV te je kao zastavica, odnosno rješenje postavljena rečenica „Volim SIS“ što znači da dekriptiranjem zadane poruke moramo dobiti taj niz znakova.



Slika 5: Prikaz zadatka kriptografije, drugi dio [3]

Pomoć kod pronalaženja rješenja je u samom naslovu koji glasi: „Zar i ti, sine Brute?“. Naslov nas odmah upućuje na Julija Cezara i Cezarovo šifriranje. Otvorimo alat za Cezarovo šifriranje i unosimo zadani kod. Ovdje bi bilo dobro znati vrijednost premještanja (eng. *shift*) koji je po osnovnim postavkama 3 i s time ćemo dobiti rješenje, ali ukoliko nismo sigurno ili ne želimo isprobavati sve kombinacije tada možemo koristiti **Brute**-force napad kojim će se ispisati sve kombinacije i tada možemo izabrati onu koja nam se čini najsmislenija, a to je u našem slučaju „Volim SIS“. Izgled Caesar chiper alata i postizanje rješenja možemo vidjeti na slici 6. Ukoliko ne uspijemo sami doći do zaključka na koji način rješavati problem tada možemo iskoristiti pomoć koja nas vodi na wiki stranice Cezarove šifre.



Slika 6: Prikaz postizanja rješenja iz kriptografije [3]

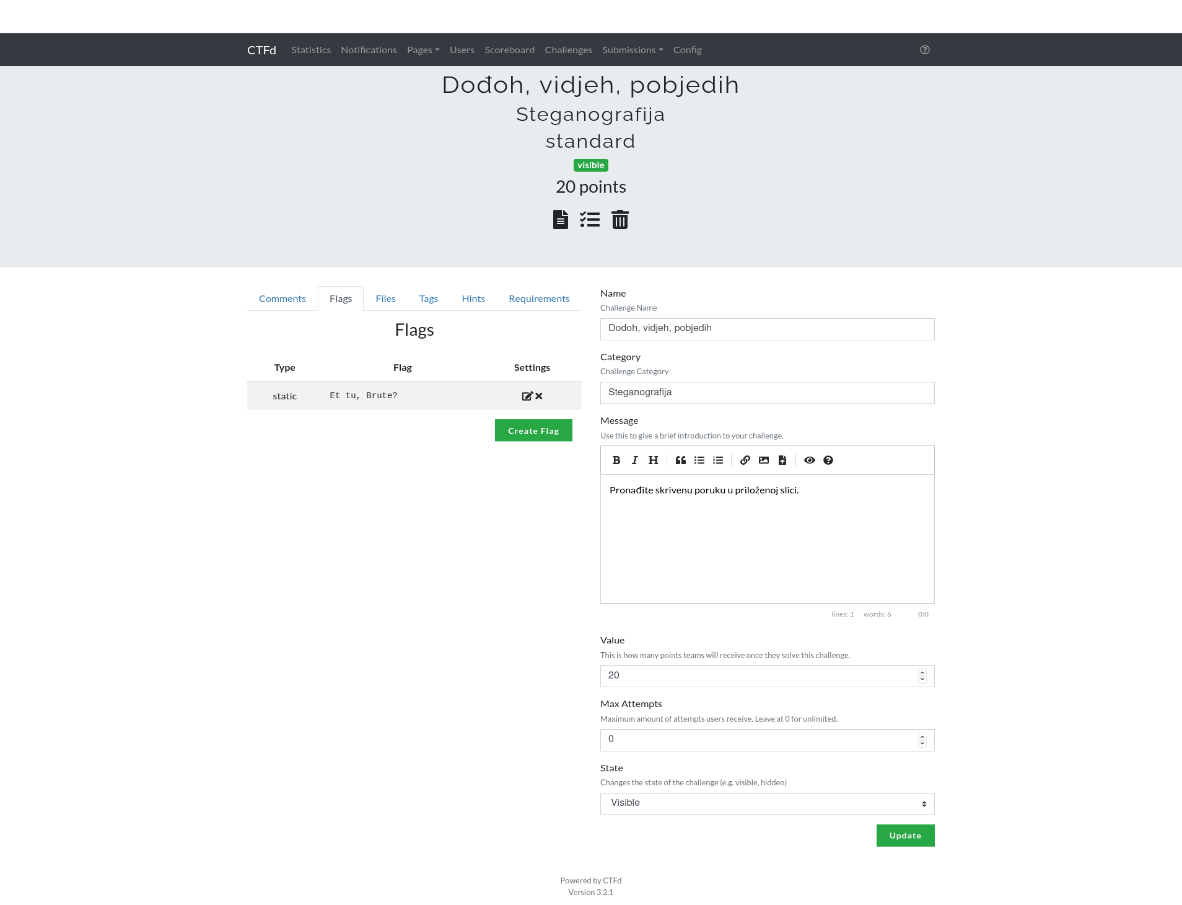
Na ovaj način zadatak je riješen te je potrebno još samo unijeti rješenje na to predviđeno mjesto i potvrditi ga. Potrebno je pripaziti na unos malih i velikih slova.

* 1. Dođoh, vidjeh, pobjedih

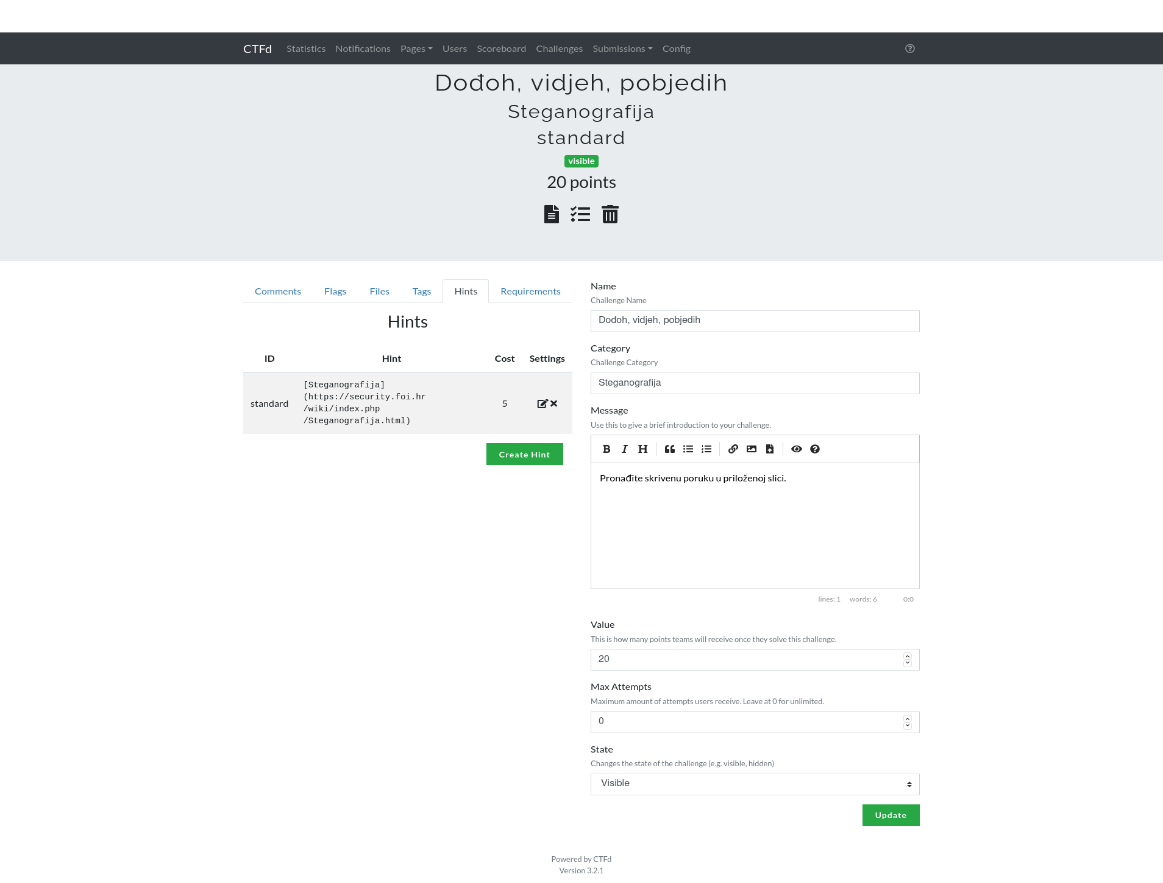
Zadatak koji se krije iza ovog naslova pripada tipu steganografije. Zadatak u prilogu sadrži fotografiju vidljivu na slici 7 na kojoj je potrebno pronaći skrivenu poruku. Vrijednost rješenja je 20 bodova, a zastavica je postavljena na poruku „Et tu, Brute?“. Pomoć nas vodi na wiki stranice steganografije.Postavljen zadatak u CTFd-u možemo vidjeti na slikama 8 i 9.



Slika 7: Slika koja sadrži skrivenu poruku [4]

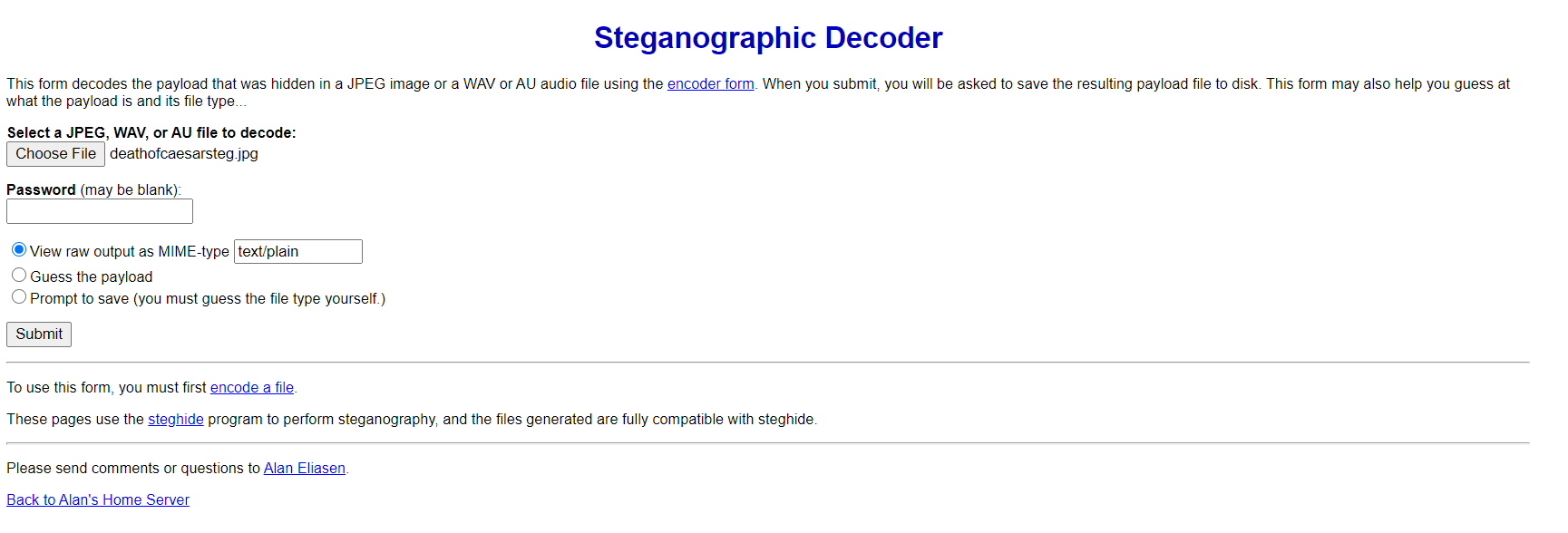


Slika 8: Prikaz zadatka steganografije, prvi dio [3]



Slika 9: Prikaz zadatka steganografije, drugi dio [3]

Do rješenja dolazimo na način da preuzmemo priloženu sliku te ju unosimo alat za detekciju skrivenih poruka na slici. U našem slučaju korišten je alat *Steganography decoder* te su parametri podešeni kao na slici 10, odnosno učitava se slika pomoću opcije *Browse* i poruka se vraća u formatu *text/plain* nakon čega se potvrđuje izbor.

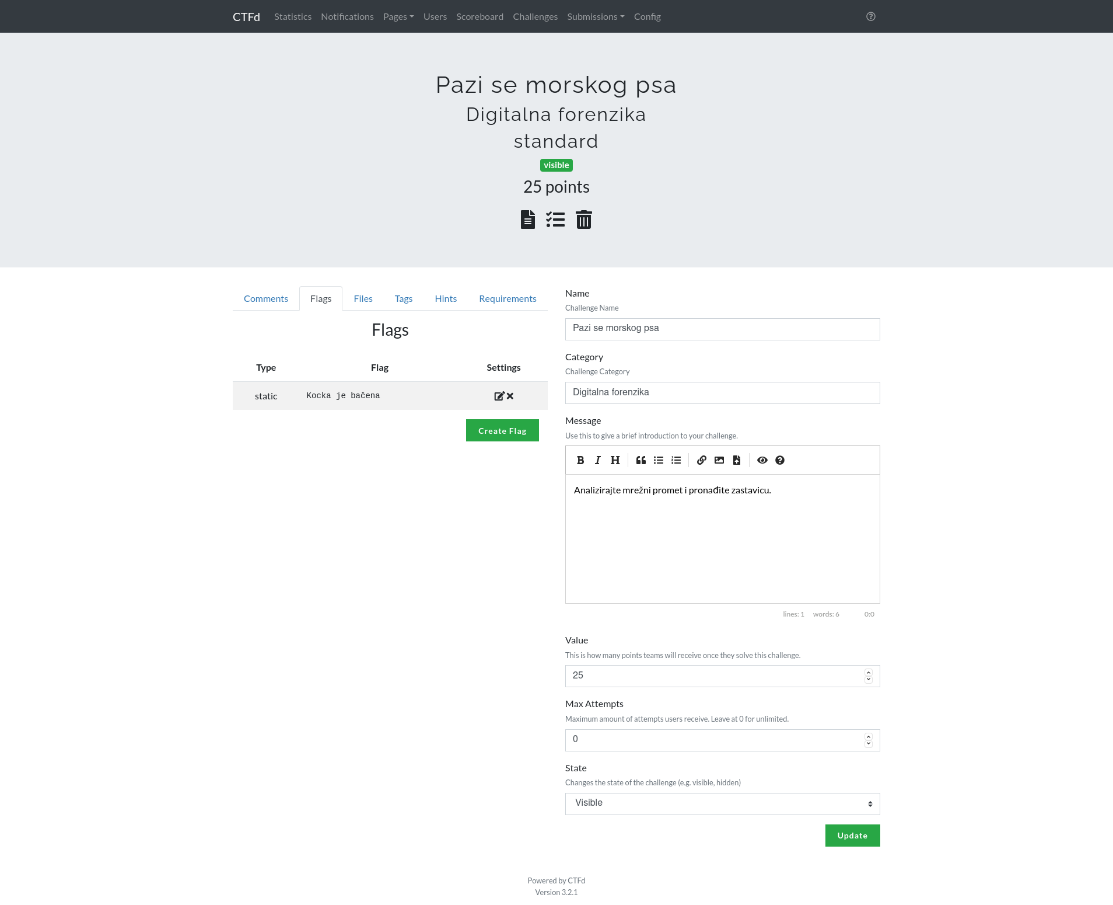


Slika 10: Prikaz postizanja rješenja zadatka steganografije [3]

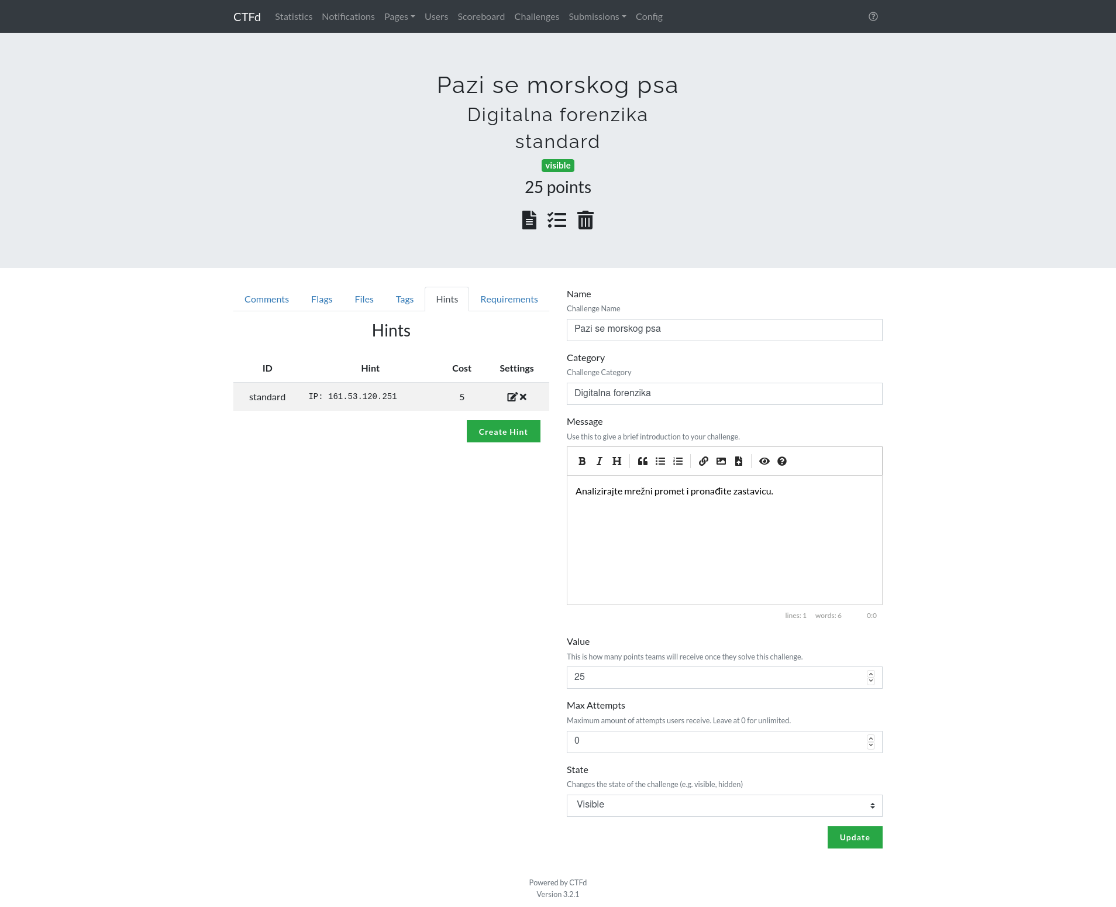
Kao rješenje vraća nam se rečenica „Et tu, Brute?“ koje je jednaka postavljenoj zastavici te ju unosimo u za to predviđeni prostor i uspješno rješavamo ovaj zadatak.

* 1. Pazi se morskog psa

Zadatak Pazi se morskog psa pripada kategoriji digitalne forenzike i vrijedi 25 bodova. U zadatku je priložena snimka mrežnog prometa te ga je potrebno analizirati. Ponovo, naslov nam služio kao pomoć, morski pas trebao bi asocirati na alat za analizu mrežnog prometa *Wireshark* koji će biti korišten za pronalazak rješenja. Zadatak je postavljen na način kako je prikazano na slikama 11 i 12.

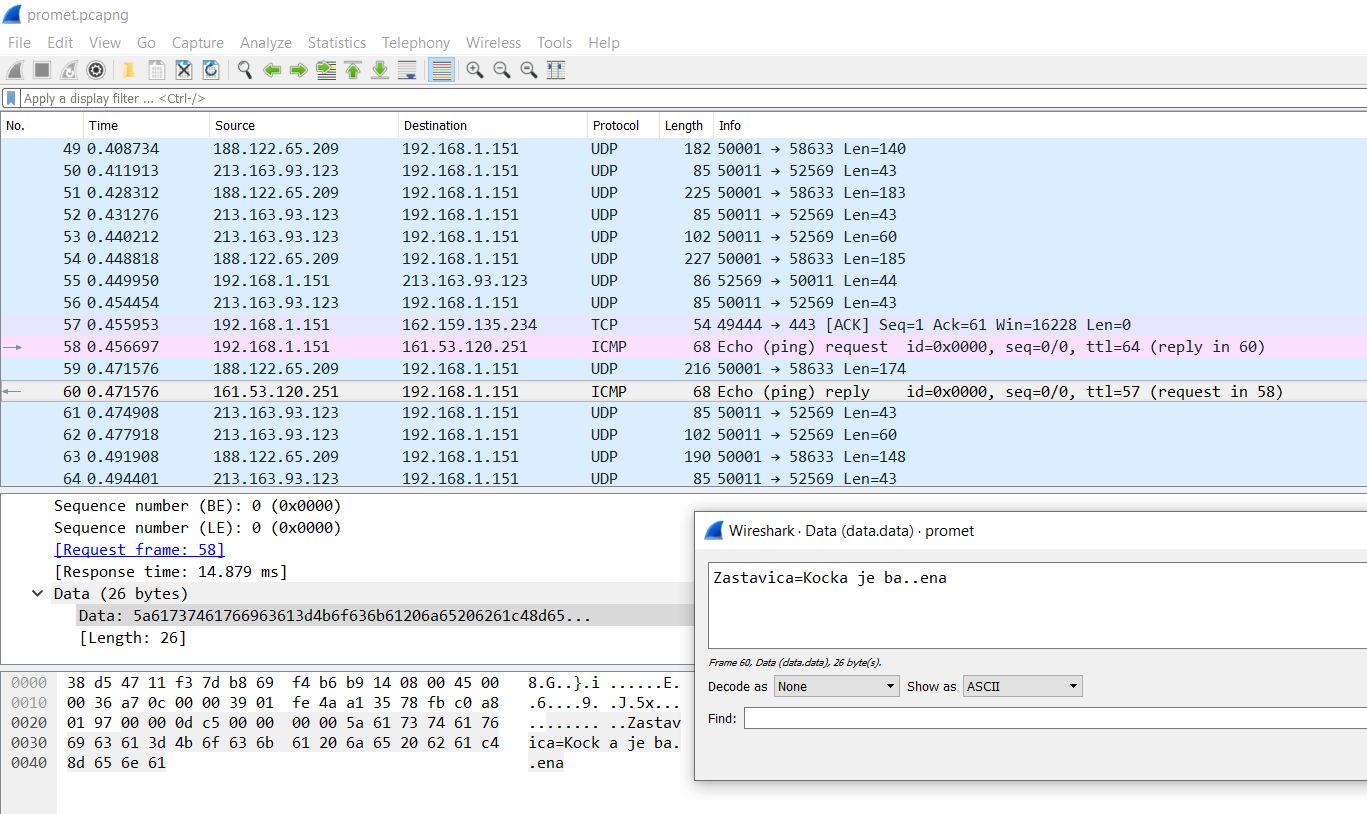


Slika 11: Prikaz zadatka digitalne forenzike, prvi dio [3]



Slika 12: Prikaz zadatka digitalne forenzike, drugi dio [3]

Do rješenja dolazimo na način da otvaramo priloženu snimku prometa u alatu *Wireshark* te ga analiziramo. Primjećujemo dva retka koji su drugačije boje te im pridajemo pažnju i vidimo da se radi o zahtjevu i odgovoru. Klikom na odgovor vidimo što sve taj paket sadrži. Možemo vidjeti da sadrži podatke veličine 26 byte-a te pravilnim pozicioniranjem odmah možemo vidjeti vrijednost zastavice. Alternativni način za pronalazak rješenja je klik na paket, proširenje *Internet Control Message Protocol,* pozicioniranje na *Data* te proširenje istog i posljednji korak desni klik na redak koji sadrži vrijednost podataka i opcija *Show packet bytes.* Oba načina vidljiva su na slici 13.

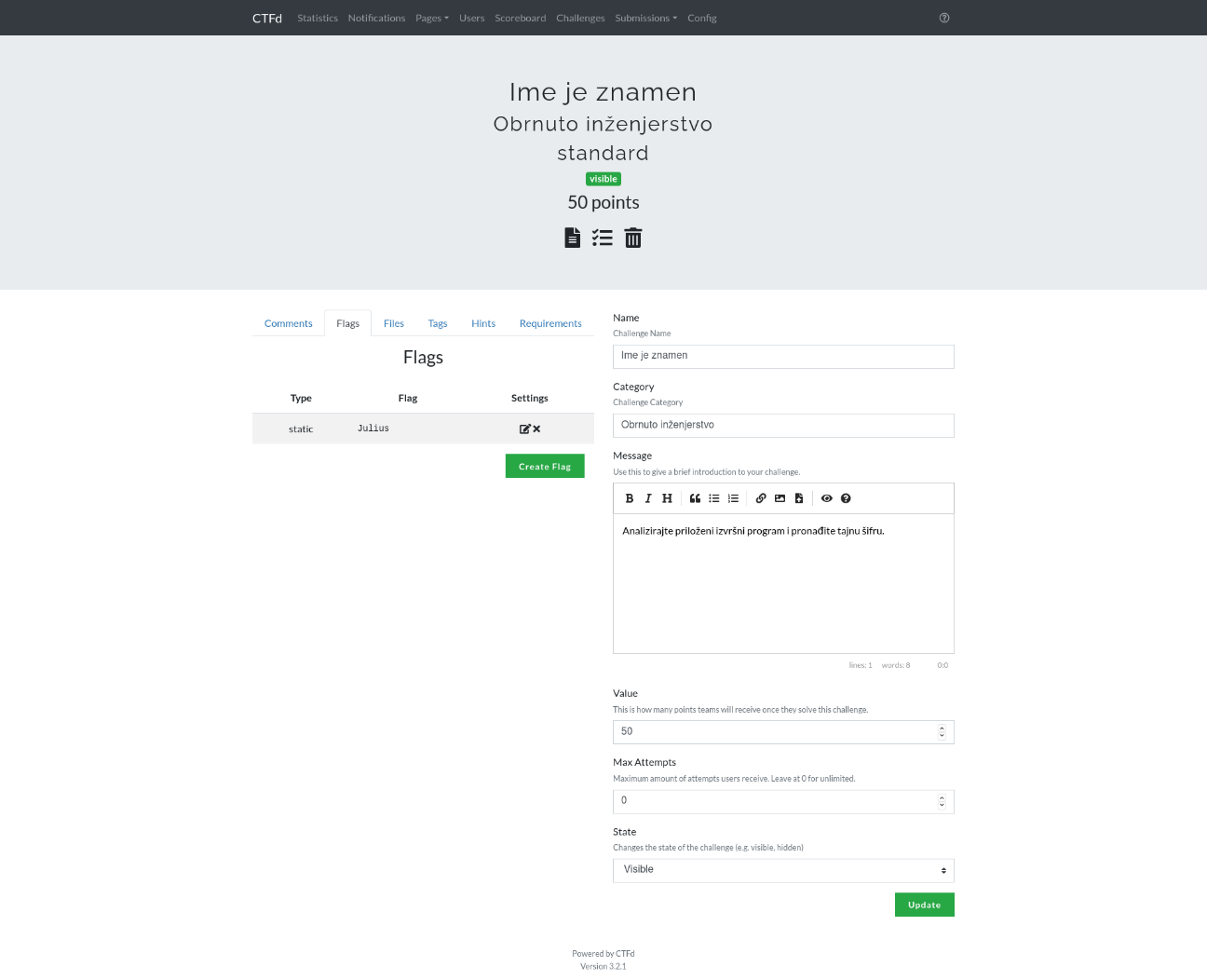


Slika 13: Prikaz analize mrežnog prometa u wiresharku [3]

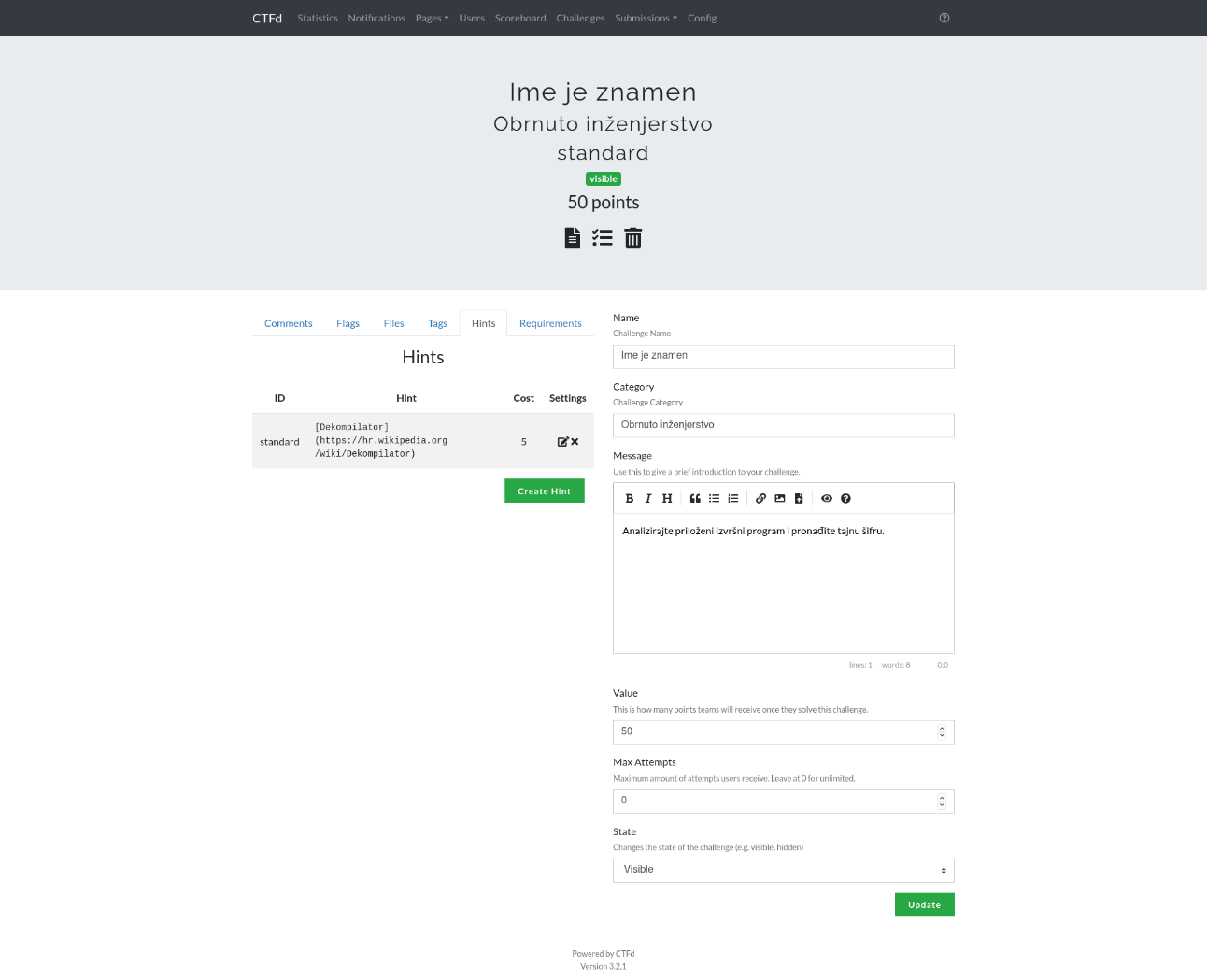
Vidimo kako nam podaci govore da je zastavica jednaka rečenici „Kocka je ba..ena“ zbog nepodržavanja dijakritičkih znakova, ali lako je zaključiti da se radi o riječi bačena. S obzirom da je zastavica također postavljena na vrijednost „Kocka je bačena“, što možemo vidjeti na slici 11, ukoliko je vrijednost unesena na odgovarajuće mjesto za unos odgovora na zadatak tada je zadatak uspješno riješen. Pomoć kod rješavanja zadataka vodi direknto na paket koji treba biti analiziran.

* 1. Ime je znamen

Zadatak Ime je znamen pripada kategoriji obrnutog inženjerstva i s obzirom na kompleksnost njegovog rješavanja donosi 50 bodova. Zadatak, njegova zastavica i pomoć postavljeni su kao što je vidljivo na slikama 14 i 15. Ovaj zadatak sadrži priloženu izvršnu datoteku koju je potrebno analizirati pomoću dekompilatora.

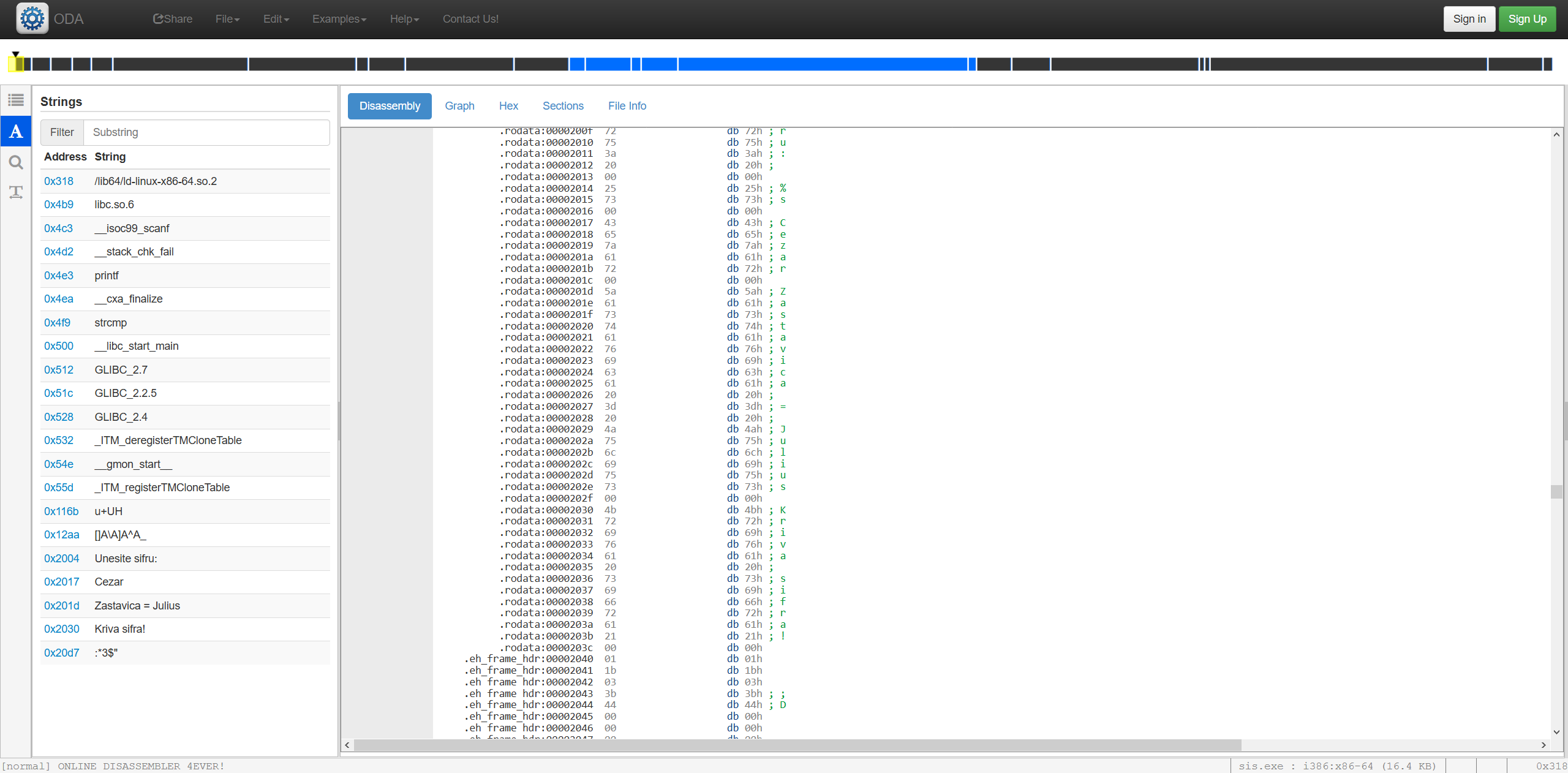


Slika 14: Prikaz zadatka iz obrnutog inženjerstva, prvi dio [3]



Slika 15: Prikaz zadatka iz obrnutog inženjerstva, drugi dio [3]

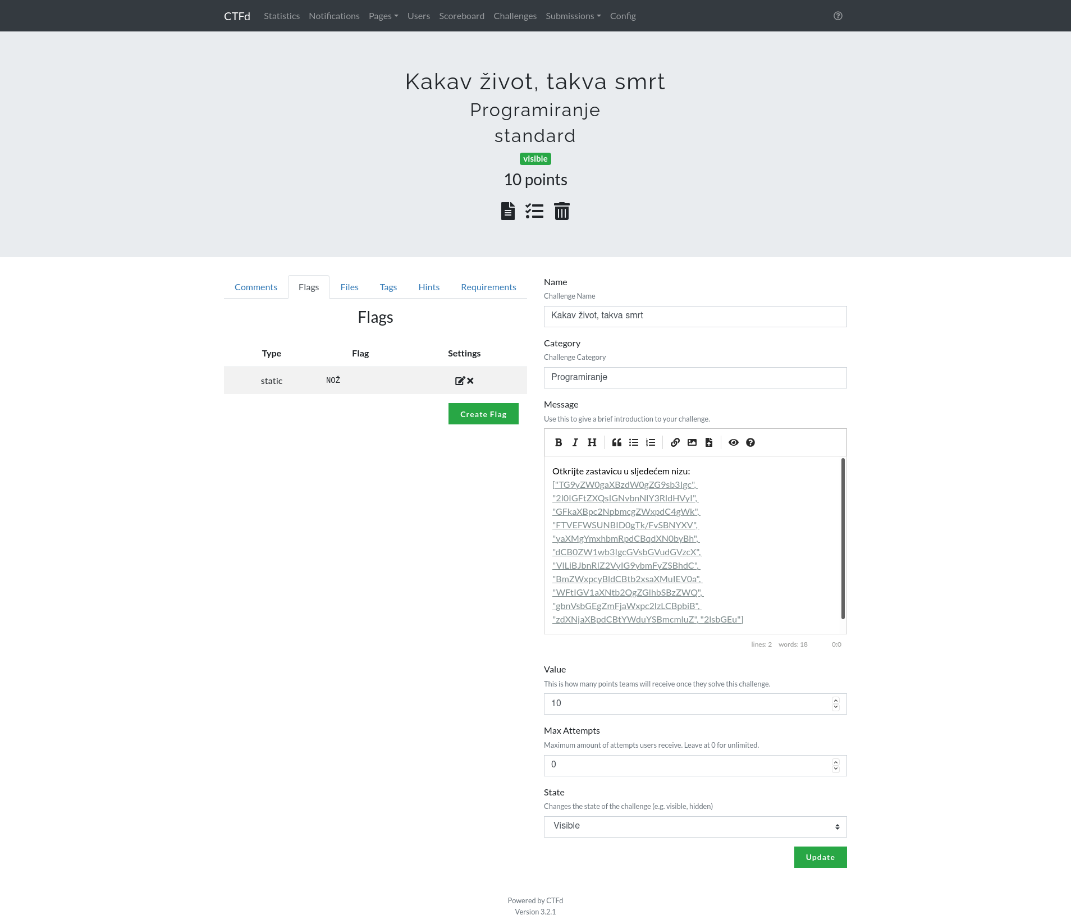
Do rješenja zadatka dolazi se na način da se otvori priložena izvršna datoteka i pomoću skrivenog naputka iz naslova pronalazi ime vezano uz tematiku CTF-a.



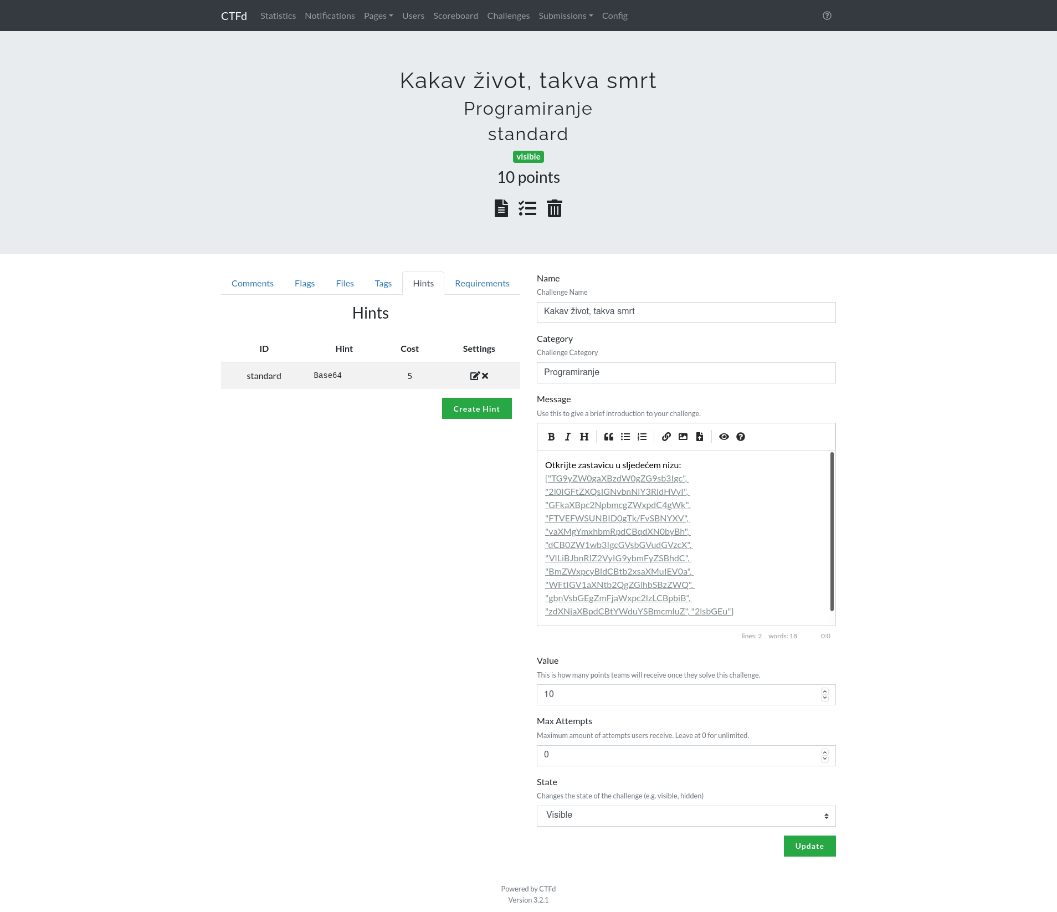
Slika 16: Prikaz korištenja online dekompilatora za pronalaženje zastavice [3]

* 1. Kakav život, takva smrt

Posljednji zadatak pod nazivom Kakav život, takva smrt pripada kategoriji progamiranja, a donosi 10 bodova. Zadatak sadrži niz nakova koje je potrebno dekodirati kako bi se pronašla zastavica, a zadatak je postavljen na način kao što je prikazano na slikama 16 i 17.



Slika 17: Prikaz zadatka iz programiranja, prvi dio [3]

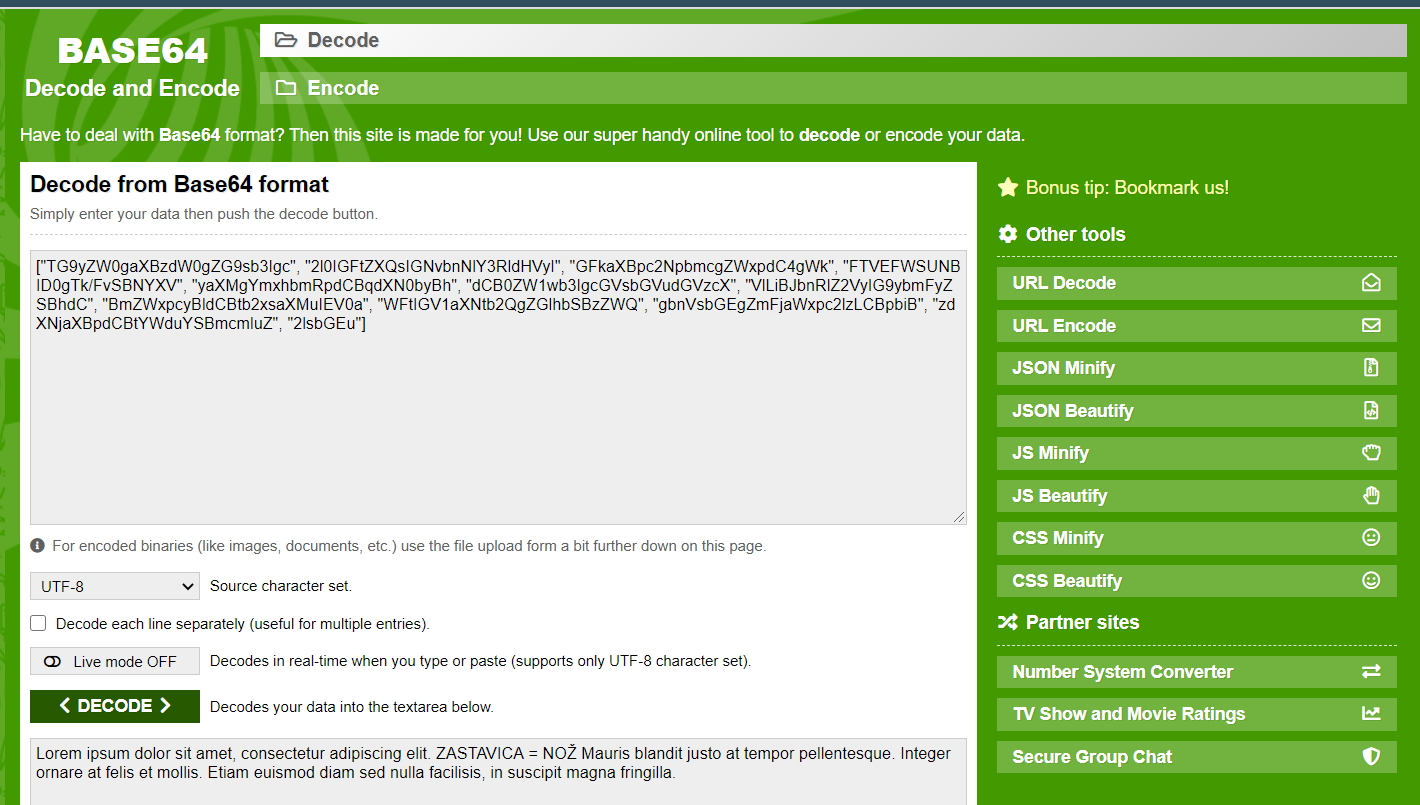


Slika 18: Prikaz zadatka iz programiranja, drugi dio [3]

Kako bi riješili ovaj zadatak prvo je potrebno dekodirati zadani niz koji glasi:

["TG9yZW0gaXBzdW0gZG9sb3Igc", "2l0IGFtZXQsIGNvbnNlY3RldHVyI", "GFkaXBpc2NpbmcgZWxpdC4gWk", "FTVEFWSUNBID0gTk/FvSBNYXV", "yaXMgYmxhbmRpdCBqdXN0byBh", "dCB0ZW1wb3IgcGVsbGVudGVzcX", "VlLiBJbnRlZ2VyIG9ybmFyZSBhdC", "BmZWxpcyBldCBtb2xsaXMuIEV0a", "WFtIGV1aXNtb2QgZGlhbSBzZWQ", "gbnVsbGEgZmFjaWxpc2lzLCBpbiB", "zdXNjaXBpdCBtYWduYSBmcmluZ", "2lsbGEu"].

Nameće se pitanje kako znati kojom na koji način je potrebno dekodirati niz, a odgovor se nalazi u pomoći ukoliko sudionik ne želi isprobavati različite alate i metode. Rješenje se dobiva dekodirajući gore navedeni niz u alatu *base64decode*.



Slika 19: Prikaz postizanja rješenja iz programiranja [3]

Upotrebom navedenog alata dobijemo rješenje kako je zastavica riječ „NOŽ“ (potrebno je pripaziti na velika i mala slova prilikom unosa rješenja), a ona je ugnježđena u isječak Lorem ipsum teksualnog predloška.

1. Zaključak

U svijetu gdje tehnologija raste ubrzanim tempom, a opasnosti koje joj prijete prate jednakom brzinom, javlja se potreba za stručnjacima koji mogu odgovoriti na ta izazovna vremena visokom spremnošću.

Upravo neki od tih stručnjaka za mrežnu, ali i razne druge sigurnosti počeli su svoj put na CTF natjecanjima. Natjecanjima koja uče kako razmišljati poput napadača na sustav te kako se na vrlo informativan, ali zabavan način osposobljavati za karijeru budućeg cyber profesionalca.

U radu je ukratko navedena povijest CTF natjecanja, neke od njezinih posebnosti, tipova zadataka, ali i načina na koji se oni rješavaju te kako se sakriva zastavica od natjecatelja. Kasnije je bilo riječi o alatima koji su vrlo korisni u takvim natjecanjima kako bi olakšali u pronalaženju puta do zastavice.

U drugom dijelu rada prikazan je praktični dio obuhvaća različite tipove zadataka koje je potrebno riješiti kako bi se sakupili određeni bodovi i kako bi natjecatelj nešto naučio. Poanta tih zadataka je i edukativne prirode te svaki ima i svoj „hint“ koji u sebi sadrži link na neki vanjski izvor koji može igraču pomoću u rješavanju istoga.

Možemo zaključiti kako su CTF natjecanja vrlo korisna u današnjem svijetu gdje su cyber napadi postali svakodnevica kako bi pripremili buduće profesionalce za obranu sustava, ali i kako bi kasnije mogli vježbati na svojim vještinama. CTF natjecanja su također i zabavna te svatko tko želi nešto naučiti, a pritom se i zabaviti te usput naučiti neku novu vještinu, odabrao je pravi put.

Popis literature

1. Tim Harmon (2016). Cyber Security Capture The Flag (CTF): What Is It?. Preuzeto 10.01.2021. sa [https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it#:~:text=A%20cyber%20security%20CTF%20is,have%20learned%20during%20their%20training](https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it%23:~:text=A%20cyber%20security%20CTF%20is,have%20learned%20during%20their%20training)
2. adityajoshi15 (2019). What is CTFs (Capture The Flag). Preuzeto 10.01.2021. s <https://www.geeksforgeeks.org/what-is-ctfs-capture-the-flag/?ref=rp>
3. Siddhant Dubey (2019). An Introduction to Cybersecurity, Capture the Flag Contests, and Basic Security Concepts. Preuzeto 10.01.2021 s <https://medium.com/better-programming/an-introduction-to-cybersecurity-capture-the-flag-contests-and-basic-security-concepts-80f3fbf62bbc>
4. Ford, Vitaly & Siraj, Ambareen & Haynes, Ada & Brown, Eric. (2017). Capture the Flag Unplugged: an Offline Cyber Competition. 225-230. 10.1145/3017680.3017783.
5. CTF101 (bez dat.). Binary Exploitation. Preuzeto 10.01.2021. s <https://ctf101.org/binary-exploitation/overview/>
6. Trailofbits (bez dat.). Forensics. Preuzeto 10.01.2021. s <https://trailofbits.github.io/ctf/forensics/>
7. CTF101 (bez dat.). Reverse Engineering. Preuzeto 10.01.2021. s <https://ctf101.org/reverse-engineering/overview/>
8. CTFd (bez. dat.). CTF open source. Preuzeto 10.01.2021. s <https://awesomeopensource.com/project/CTFd/CTFd>

Popis slika

Popis slika treba biti izrađen po uzoru na indeksirani sadržaj, te upućivati na broj stranice na kojoj se slika može pronaći.

Slika 1: CTF zastavica [1-**https://portswigger.net/** ] 2

[Slika 2: Sakrivena riječ „root“ [2-**https://dl.acm.org/doi/pdf/10.1145/3017680.3017783** ] 4](#_Toc61261117)

[Slika 3: Zrcaljeni tekst na slici [2-**https://dl.acm.org/doi/pdf/10.1145/3017680.3017783**] 5](#_Toc61261118)

[Slika 4: Prikaz zadatka kriptografije, prvi dio [3-**autorski rad**] 10](#_Toc61261119)

[Slika 5: Prikaz zadatka kriptografije, drugi dio [3**-autorski rad**] 11](#_Toc61261120)

[Slika 6: Prikaz postizanja rješenja iz kriptografije [3**-autorski rad**] 12](#_Toc61261121)

[Slika 7: Slika koja sadrži skrivenu poruku [4**-https://en.wikipedia.org/wiki/Assassination\_of\_Julius\_Caesar**] 12](#_Toc61261122)

[Slika 8: Prikaz zadatka steganografije, prvi dio [3**-autorski rad**] 13](#_Toc61261123)

[Slika 9: Prikaz zadatka steganografije, drugi dio [3**-autorski rad**] 13](#_Toc61261124)

[Slika 10: Prikaz postizanja rješenja zadatka steganografije [3**-autorski rad**] 14](#_Toc61261125)

[Slika 11: Prikaz zadatka digitalne forenzike, prvi dio [3**-autorski rad**] 15](#_Toc61261126)

[Slika 12: Prikaz zadatka digitalne forenzike, drugi dio [3**-autorski rad**] 15](#_Toc61261127)

[Slika 13: Prikaz analize mrežnog prometa u wiresharku [3**-autorski rad**] 16](#_Toc61261128)

[Slika 14: Prikaz zadatka iz obrnutog inženjerstva, prvi dio [3**-autorski rad**] 17](#_Toc61261129)

[Slika 15: Prikaz zadatka iz obrnutog inženjerstva, drugi dio [3**-autorski rad**] 18](#_Toc61261130)

[Slika 16: Prikaz korištenja online dekompilatora za pronalaženje zastavice [3**-autorski rad**] 19](#_Toc61261131)

[Slika 19: Prikaz postizanja rješenja iz programiranja [3**-autorski rad**] 21](#_Toc61261132)

Prilog 1

1. Link na GitHub repozitorij: https://github.com/bzitkovic/edukativni-ctf