

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Darija Filipović, Danko Delimar, Toni Kukec, Neven Lukić, Lara Grgurić, Gregor Mihaljević, Iva Klobučar (Arhitektonski fakultet), Vatroslav Jakopec, Ana Francesca Stama, Milan Vrankić, Toma Petrušić

RAZVOJ STUDENTSKIH KOMPETENCIJA I ZAJEDNICE KIBERNETIČKE SIGURNOSTI NA FER-U

ZAGREB, 2025.

Ovaj rad izrađen je u sklopu udruge X.FER, osnovane na Fakultetu elektrotehnike i računarstva, pod vodstvom mentora izv. prof. dr. sc. Ante Đereka, izv. prof. dr. sc. Marina Vukovića i izv. prof. dr. sc. Stjepana Groša predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2024./2025. u kategoriji "Nagrada za društveno koristan rad u akademskoj i široj zajednici".

CTF – *Capture the Flag* (tip natjecanja u vještinama kibernetičke sigurnosti)

Sadržaj

Uvod i motivacija

Kibernetička sigurnost predstavlja jedno od najbrže rastućih i najdinamičnijih područja unutar informacijskih znanosti. Brzi razvoj tehnologije, digitalizacija poslovanja i rast složenosti informacijskih sustava dovode do značajnog povećanja broja i složenosti kibernetičkih prijetnji. Unatoč važnosti ove domene, studenti tehničkih fakulteta često nemaju priliku sustavno razvijati praktične vještine iz sigurnosti, niti dovoljno razumiju širi regulatorni i organizacijski kontekst kibernetičke zaštite. Istovremeno, industrija i javni sektor iskazuju sve veće potrebe za stručnjacima koji razumiju i tehničke i regulativne okvire sigurnosti te su spremni raditi na pozicijama koje zahtijevaju interdisciplinarne vještine. Prvu ideju za promicanje područja kibernetičke sigurnosti osmislio je dio organizacijskog tima prilikom povratka s europskog natjecanja u kibernetičkoj sigurnosti na kojemu su primijetili nedovoljan broj predstavnika iz Republike Hrvatske. Za vrijeme tog puta bili su zacrtani prvi planovi promicanja kibernetičke sigurnosti na zagrebačkom sveučilištu.

Da bismo adekvatno pristupili ovom nedostatku, pokrenuli smo dva usko vezana projekta: **studentsku vještinu “Natjecateljske vještine u kibernetičkoj sigurnosti (NaVKiS)”** te **FER-ovu akademsku konferenciju o sigurnosti (FAKS)**. Kroz studentsku vještinu studentima smo željeli omogućiti sustavan uvod u praktične sigurnosne teme i natjecateljske formate poput CTF-a, dok je konferencija osmišljena kao platforma za povezivanje studenata, akademske zajednice, industrijskih stručnjaka i regulatornih tijela. Oba projekta proizašla su iz zajedničke motivacije organizacijskog tima da unaprijedi obrazovne kapacitete FER-a na području sigurnosti i potakne razvoj aktivne, motivirane zajednice studenata zainteresiranih za kibernetičku sigurnost.

Na taj način doprinosimo dugoročnom cilju FER-a i Sveučilišta u Zagrebu da obrazuje vrhunske inženjere i stručnjake spremne odgovoriti na suvremene izazove digitalnog društva.

1. Vještina “Natjecateljske vještine u kibernetičkoj sigurnosti”

1.1. Organizacija

U organizaciji projekta sudjelovalo je četvero studenata s Fakulteta elektrotehnike i računarstva: Milan Vrankić, Toni Kukec, Gregor Mihaljević i Danko Delimar te Benjamin Nadarević zaposlenik na FER-ovom Laboratoriju za sustave i signale (LSS). U projektu su sudjelovali još i tri profesora s Fakulteta elektrotehnike i računarstva izv. prof. dr. sc. Ante Đerek, izv. prof. dr. sc. Marin Vuković te izv. prof. dr. sc. Stjepan Groš.

Međusobno smo se podijelili po segmentima organizacije kako bismo što lakše i efikasnije ideju proveli u stvarnost, no preklapanja su svakako bila prisutna zbog složenosti projekta.

Milan Vrankić i Danko Delimar bili su zaduženi za organizaciju predavanja te su napravili raspored predavanja. Teme predavanja su (kronološki poredane): OSINT (Open Source Intelligence), linux, digitalna forenzika, kriptografija, sigurnost web aplikacija 1, sigurnost web aplikacija 2, x86 assembly, binarna eksploatacija, reverzno inženjerstvo.

Uz to Milan je osmislio i izradio web stranicu (ctf.xfer.hr) koja bi bila mjesto gdje će se postavljati obavijesti o radionicama, opće informacije, materijali vezani za gradivo kako u pisanom obliku (prezentacije, urađeni zadaci s prošlih natjecanja i poveznice na vanjske izvore za polaznike koji žele znati više) tako i u audiovizualnom obliku (snimke predavanja za studente koji nisu mogli njima prisustvovati u danom terminu). Također, dogovorio je sponzorstvo za projekt od strane Erste banke i njihovog Cyber Guardian programa koji je financiran od strane Europske unije.

Danko Delimar bio je zadužen za komunikaciju s polaznicima vještine, izradu obrazaca za prijavu i promociju vještine među studentima održavanjem štandova i pisanjem objava za društvene mreže. Izradio je i kratke provjere znanja koje su korištene u nastavnom procesu.

Studenti Milan Vrankić, Gregor Mihaljević, Toni Kukec, Danko Delimar, zaposlenik LSS-a Benjamin Nadarević, stručnjak iz industrije Mateo Hanžek i profesor Ante Đerek održali su predavanja na različite teme kibernetičke sigurnosti definirane u planu i programu predavanja. Uz to studenti su napravili, napisali i objavili zadatke na platformi za CTF natjecanja (CTFd) gdje su polaznici testirali svoje znanje o predavanim temama te napisali pitanja za kratke provjere znanja koje su se održavale između predavanja te polaznicima najavljene u rasporedu.

1.2. Plan nastave

Bodovanje studenata provodilo se kroz tri vrste bodovanja.

Tablica 1. Udjeli nastavnih aktivnosti u završnom broju bodova

Vrsta bodovanja	Udio u završnoj ocjeni
Međuispit	40%
Završni ispit	40%
Kratke provjere znanja	20%

Ovo su neke od tema obrađene u ovogodišnjem izdanju vještine:

Open Source Intelligence (OSINT)

Osnove prikupljanja i analiziranja informacije iz javno dostupnih izvora poput interneta, društvenih mreža i javnih dokumenata. Upoznat će alate kao što su Google Dorks za napredno pretraživanje, theHarvester za automatsko prikupljanje podataka, Osmedeus za distribuirano skeniranje i Sherlock za pretragu korisničkih imena na društvenim mrežama.

Računalna forenzika

Uvodna znanja o analizi i očuvanju digitalnih dokaza s elektroničkih uređaja, poput računala i mobitela, te prepoznavanju tragova malicioznih aktivnosti. Upoznat će i steganografiju, odnosno tehnike skrivanja podataka unutar drugih datoteka, te metode otkrivanja skrivenih poruka u slikama i audio datotekama.

Kriptografija

Osnove kriptografije, uključujući simetrične i asimetrične algoritme, hash funkcije te primjenu kriptografskih metoda za zaštitu podataka i rješavanje CTF zadataka iz kriptografije.

Web sigurnost
Polaznici će steći znanja o osnovnim web ranjivostima i napadima, poput SQL injection, XSS i CSRF, te naučiti kako ih prepoznati i iskoristiti u kontekstu CTF zadataka, kao i osnovne metode zaštite web aplikacija.

Reverzno inženjerstvo
Osnove analiziranja kompajliranih programa i binarnih datoteka kako bi razumjeli njihovo ponašanje i pronašli skrivene informacije ili ranjivosti. Upoznat će osnovne alate za disasembly i dekompilaciju.

Binary exploitation
Polaznici će steći uvodna znanja o iskorištavanju ranjivosti u binarnim programima, poput buffer overflow napada, te osnovama pisanja exploit skripti za preuzimanje kontrole nad programom ili dobivanje zastavica u CTF zadacima.

Slika 1. Predavanje računalne forenzike

1.3 Rezultati i evaluacija vještine

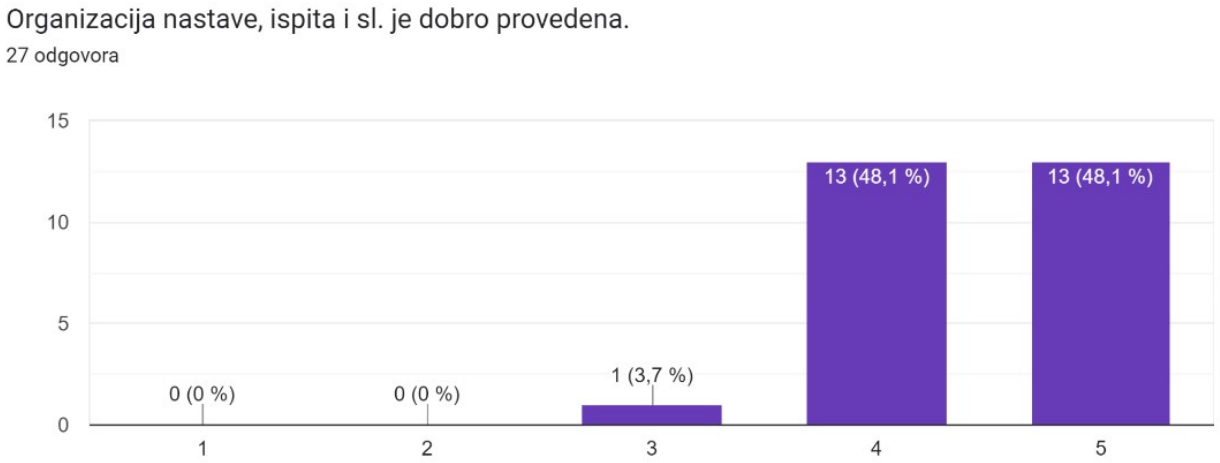
Studentska vještina “Kibernetička sigurnost” predstavlja prvu takvu vještinu na Sveučilištu u Zagrebu, namijenjenu stjecanju praktičnih znanja iz područja kibernetičke sigurnosti. Vještina je u najnovijoj generaciji okupila 142 prijavljena studenta, od kojih je 90 pristupilo međuispitu, dok su završni ispiti još u tijeku.

Rezultati ankete provedene nakon završetka vještine prethodne akademske godine pokazali su visok stupanj zadovoljstva studenata. Organizaciju nastave, ispita i zadataka 96% studenata ocijenilo je ocjenom 4 ili 5, ističući dobru strukturiranost i pripremljenost materijala. Komunikacija na kolegiju također je visoko ocijenjena, gdje je više od 90% studenata odgovorilo s 4 ili 5, naglašavajući dostupnost organizatora i dobru međusobnu suradnju.

Više od 85% studenata navelo je da su im snimke predavanja značajno pomogle u učenju, što pokazuje važnost hibridnog pristupa za usvajanje kompleksnog gradiva. Na pitanje o težini vještine, većina studenata ju je ocijenila kao umjereno tešku (3/5), dok je manji broj smatrao da je lakša ili teža od očekivanog, što ukazuje na dobro pogođen balans težine vještine.

Kao najzanimljivije teme, studenti su istaknuli binary exploitation, reverzno inženjerstvo i forenziku, dok su OSINT i hardversko hakiranje dobili manje glasova, vjerojatno zbog manjeg broja zadataka ili praktičnih primjera iz tih područja. U slobodnim komentarima (prošlogodišnje ankete) istaknuli su praktičnost, primjenjivost znanja i motivaciju za daljnje učenje, uz prijedloge za dodatne zadatke i produbljivanje pojedinih tema u budućim izdanjima vještine.

Sveukupno, evaluacija vještine pokazuje da ona uspješno ispunjava svoju svrhu razvijanja praktičnih kompetencija iz kibernetičke sigurnosti te poticanje studenata na daljnje usavršavanje i sudjelovanje u CTF natjecanjima i sigurnosnim projektima.



Slika 2. Prikupljeni odgovori polaznika na pitanje "Organizacija nastave, ispita i sl. je dobro provedena"

2. FER-ova akademska konferencija o sigurnosti (FAKS)

2.1. Organizacija

2.1.1 Organizacijski tim i podjela odgovornosti

Na planiranju i provedbi konferencije radio je organizacijski tim od deset studenata, uz mentorsko vodstvo izvanrednog profesora Marina Vukovića. Tim je od samog početka podijeljen na funkcionalne podskupine ili individue, pri čemu je svaka preuzela odgovornost za jedan aspekt projekta. Redovitim zajedničkim sastancima usklađivali smo aktivnosti i pratili napredak kako bi osigurali da svaki segment organizacije bude pokriven i kvalitetno izveden.

Glavne cjeline organizacijskog rada uključivale su: **sadržajni dio**, gdje smo kontaktirali predavače, dogovarali teme i izrađivali raspored predavanja i radionica; **tehničku pripremu CTF natjecanja**, koja je obuhvaćala izradu i testiranje zadataka, održavanje infrastrukture i postavljanje platforme; **promociju i odnose s javnošću**, u sklopu koje su članovi tima pripremali objave za društvene mreže, web-stranicu i medije, te komunicirali s PR službom FER-a; **suradnju s partnerima i sponzorima**, koja je uključivala traženje financijske i logističke podrške te dogovaranje sponzorskih paketa; **logistiku i operativnu provedbu**, koja je obuhvaćala planiranje prostora, tehničke opreme i rasporeda na dan događaja; te **vizualni identitet konferencije**, gdje su izrađeni logo, vizuali za društvene mreže, plakate i web-stranicu.

2.1.2 Tehnička organizacija CTF natjecanja

Konferencija je uključivala CTF natjecanje kao središnji praktični dio, čija je tehnička organizacija zahtijevala detaljno planiranje. Odabrali smo platformu CTFd za provedbu natjecanja. Razvili smo web stranicu za konferenciju (faks.xfer.hr), a platforma za samo natjecanja bila je pokrenuta na kućnom poslužitelju jednog od članova tima.

Izradu zadataka vodili su iskusni članovi našeg tima, uz konzultacije s vanjskim stručnjacima iz industrije i akademske zajednice, kako bismo osigurali primjerenu težinu i kvalitetu izazova. Svaki zadatak je prethodno temeljito testiran kako bi se uklonile nepredviđene ranjivosti ili mogućnosti varanja. Također smo implementirali nadzor nad platformom tijekom natjecanja radi uočavanja tehničkih poteškoća ili sumnjivih aktivnosti.

Natjecanje se sastojalo se od dvaju dijelova: online kvalifikacija i završnog CTF finala uživo. Prije same konferencije organizirali smo dvotjedne online kvalifikacije (7.–20. travnja 2025.) za odabir najboljih timova. Zainteresirani natjecatelji prijavili su se u timovima do 5 članova, kroz kvalifikacije smo odabrali timove koji su ostvarili najbolje rezultate te ih pozvali na finale uživo drugog dana konferencije. Finalno natjecanje održano je u prostorima FER-a 8. lipnja 2025., gdje su se kvalificirani timovi natjecali rješavajući novu seriju težih zadataka u ograničenom vremenu, najbolja tri tima prigodno smo nagradili. Ctf natjecanje proteklo je glatko.

2.1.3 Struktura programa konferencije

Konferencija je bila osmišljena kao dvodnevni događaj koji spaja stručna predavanja i natjecateljski dio. Prvi dan (7. lipnja 2025.) bio je posvećen predavanjima i radionicama te je sadržajno podijeljen na dva tematska smjera (tracka) koji su se odvijali usporedno. Organizirali smo “policy” predavanja usmjerena na šire aspekte kibernetičke sigurnosti kao zakonske regulative, strateške inicijative, standarde, privatnost i “tech” smjer, fokusiran na realne scenarije kibernetičkih napada, otkrivanje ranjivosti i analizu napada. Ovakva podjela omogućila je sudionicima da odaberu predavanja prema vlastitim interesima.

Program je otvoren zajedničkim dijelom i uvodnim obraćanjem, nakon čega su uslijedila ključna predavanja (keynotes) i paralelni “trackovi”. Za svaki “track” predvidjeli smo istaknuto “keynote” predavanje: jedno u domeni “tech” (trajanja 60 minuta) i jedno u domeni “policy” (45 minuta). Keynote govornici bili su ugledni stručnjaci koji su pružili pregled aktualnih trendova u obje domene, čime su postavili ton za ostatak konferencije. Nakon keynote izlaganja, tijekom dana se odvijalo ukupno više od deset predavanja. Svako pojedinačno predavanje trajalo je oko 25 minuta izlaganja plus 5 minuta za pitanja publike, kako bismo omogućili interakciju i diskusiju. Predavanja su pokrila raznolike teme: od analize konkretnih sigurnosnih incidenata i studija slučaja iz industrije, preko predstavljanja novih alata i metoda obrane, pa do pregleda regulatornih okvira poput EU NIS2 direktive i nacionalnih strategija kibernetičke sigurnosti. Predavači su bili birani tako da predstavljaju mješavinu akademske zajednice, industrije i javnog sektora. Zahvaljujući tome, sudionici su mogli čuti perspektive iskusnih profesionalaca iz vodećih tvrtki i institucija (npr. nacionalnog CERT-a, sigurnosnih firmi i globalnih tech kompanija) kao i istraživače s fakulteta, što je pridonijelo kvaliteti i vjerodostojnosti programa.

Tijekom dnevnog programa ubacili smo i neformalni segment **“Flash talks”**, osmišljen za kratke, spontane prezentacije. Flash talkovi su bile brze petominutne prezentacije na kojima su sudionici konferencije (primarno studenti) mogli podijeliti vlastite ideje, projekte ili iskustva vezana uz sigurnost.

Drugi dan (8. lipnja 2025.) konferencije bio je u potpunosti posvećen CTF natjecanju i pratećim aktivnostima. U popodnevnim satima drugog dana održali smo svečano zatvaranje konferencije uz proglašenje pobjednika CTF natjecanja i podjelu nagrada, nakon čega je uslijedilo neformalno druženje sudionika i organizatora.

2.1.4. Partneri, sponzori i suradnja s predavačima

Konferencija FAKS 2025 ostvarena je uz značajnu podršku partnera, sponzora i stručnjaka iz akademske zajednice i industrije. Projekt su financirali Europska unija (program Digitalna Europa kroz Europski centar za kompetencije za kibernetičku sigurnost) te Erste Banka u sklopu inicijative Erste Cyber Guardian, čime su osigurana osnovna sredstva za infrastrukturu, opremu i promociju. Uz glavne pokrovitelje, projekt su financirali ReversingLabs i Infigo IS.

Proces ugovaranja sa sponzorima tekao je uz jasno definirane uvjete koji su štitili akademski karakter konferencije, uz zabranu agresivnog marketinga i regrutacijskih aktivnosti tijekom predavanja s glavnim ciljem povezivanja akademske zajednice s industrijom te jačanje studentske sigurnosne zajednice i budućih stručnjaka.

Izdvojili smo neke od izlaganja:

Regulativni okvir kibernetičke sigurnosti u Republici Hrvatskoj
Predavanje Nacionalnog centra za kibernetičku sigurnost predstavilo je novi regulativni okvir temeljen na Zakonu o kibernetičkoj sigurnosti (NN 14/2024) i transpoziciji NIS2 direktive. Obrađene su obveze upravljanja rizicima, kategorizacija subjekata, prijava incidenata te nadzor i provedbene mjere koje novi okvir donosi u javnom i privatnom sektoru.

Kako pronaći ranjivosti u web preglednicima
Ivan Fratrić (Google Project Zero) objasnio je osnovne principe sigurnosti web preglednika, najčešće vrste ranjivosti i metode njihovog otkrivanja, te demonstrirao iskorištavanje nedavne kritične ranjivosti u Firefoxu, pokazujući praktične korake napada.

Kako danas izgledaju ransomware napadi?
Predavanje NCSC-a prikazalo je anonimne primjere stvarnih ransomware napada u Hrvatskoj, od inicijalnih vektora napada, eskalacije privilegija do krađe i eksfiltracije podataka, s ciljem edukacije administratora i sigurnosnih stručnjaka za detekciju i obranu.

NIS2 u praksi, izazovi s terena
Davor Stanec je kroz praktične primjere opisao izazove provedbe NIS2 direktive u Hrvatskoj, uključujući procjene rizika, implementaciju sigurnosnih mjera i najčešće probleme organizacija pri usklađivanju s regulatornim zahtjevima.

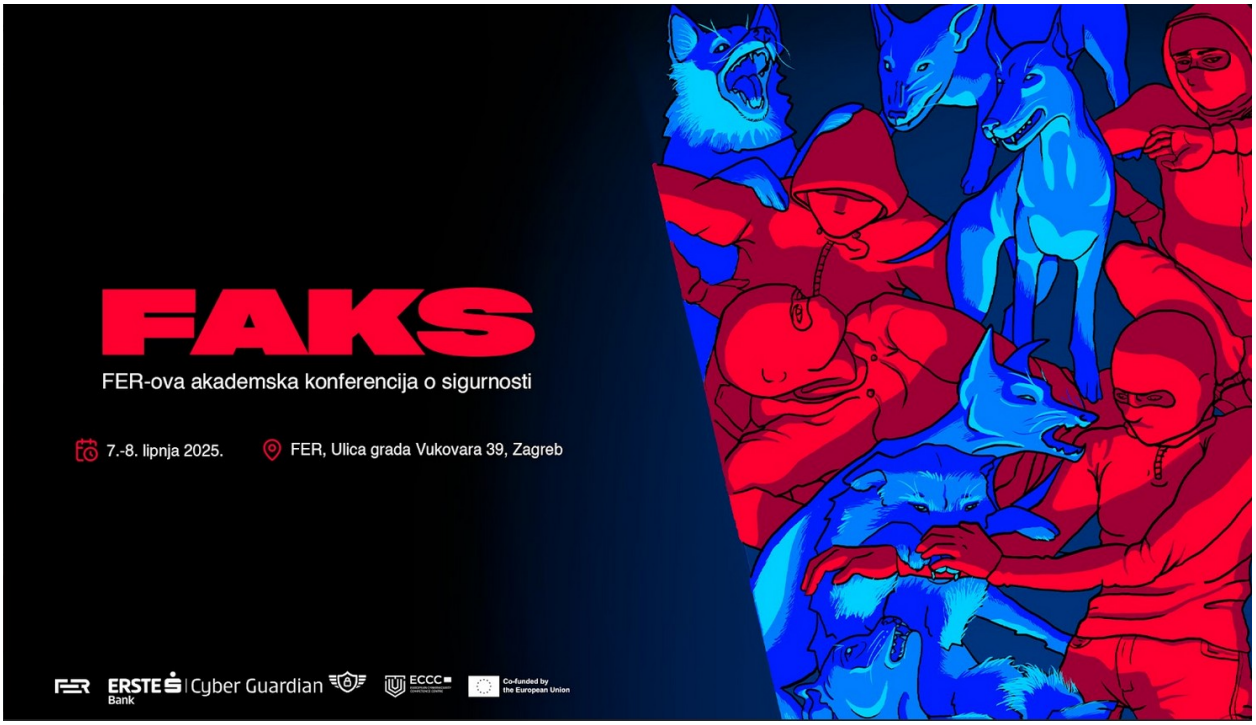
Od FER-a do Fortune 100: Kako izgleda stvarni svijet kibernetičke sigurnosti i zašto je super raditi u njemu
Biljana Cerin (Ostendo Consulting) podijelila je svoj profesionalni put od FER-a do savjetovanja najvećih američkih korporacija, prikazavši izazove i prilike rada u kibernetičkoj sigurnosti na globalnoj razini.

2.1.5 Vizualni identitet

Vizualni identitet konferencije FAKS 2025 razvijen je kako bi prenio poruku ozbiljnosti, dinamičnosti i suvremenosti područja kibernetičke sigurnosti. Dizajn je obuhvaćao sve aspekte događaja, od izrade logotipa i odabira boja, preko pripreme promotivnih vizuala za društvene mreže i web-stranicu, do dizajna akreditacija, bannera, press zida, projekcijskih predložaka za prezentacije, majica i torbi. Središnji motiv vizualnog identiteta bila je pamtljiva grafika koja prikazuje složenost i prijetnje digitalnog prostora, kombinirajući stilizirane figure napadača i zaštitnika u kontrastnim crveno-plavim tonovima, čime je stvorena upečatljiva i prepoznatljiva estetika konferencije.

Slika 3. Glavni vizual konferencije

Slika 4. Naljepnice poklonjene predavačima i posjetiteljima



Slika 5. Dizajn za naslovnicu web-stranice

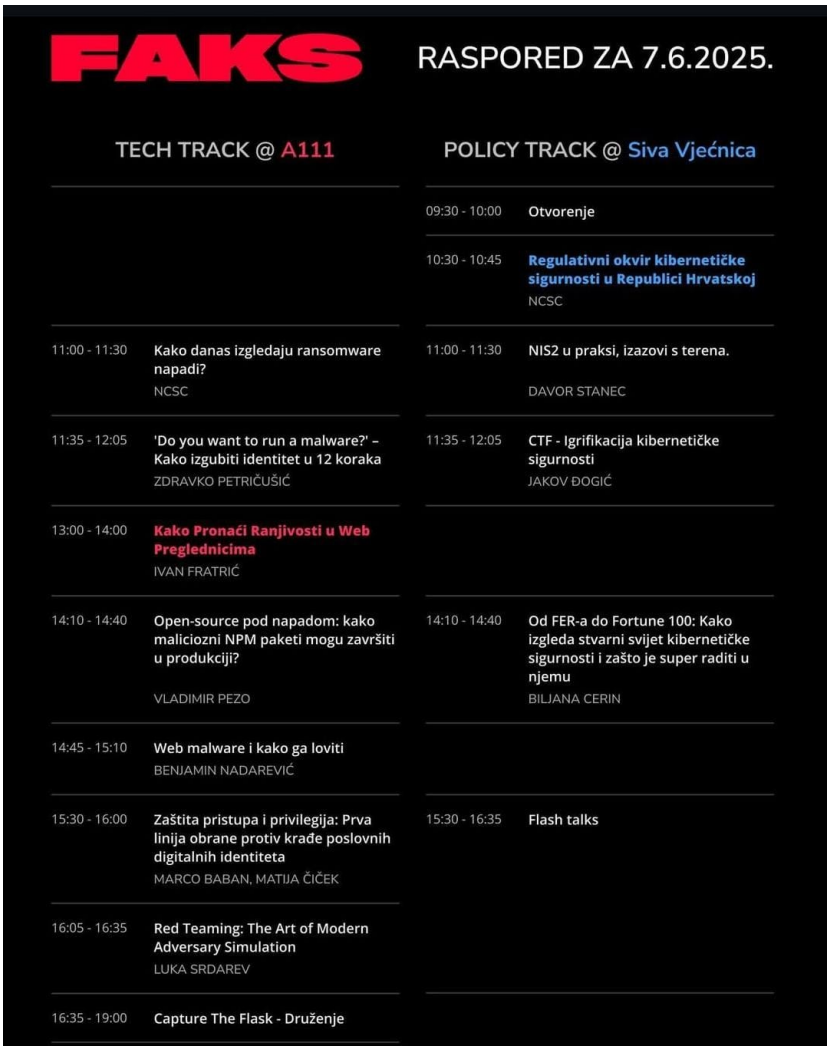
Slika 6. Dizajn simboličnih torbi poklonjenih predavačima

2.1.6. PR i medijska prisutnost

Od početka smo osmislili jasnu PR strategiju kako bi FAKS 2025 bio vidljiv studentima i široj javnosti. U suradnji s FER-ovim PR uredom planirali smo sve objave, preko poziva na sudjelovanje i CTF prijave, do predstavljanja predavača i praktičnih informacija uoči samog događaja, te je FER također interno reklamirao naš projekt. Koristili smo društvene mreže, studentske Discord servere i forume. Objave su bile prilagođene platformama, a za veći doseg, dio objava promovirali smo plaćenim oglasima prema studentima i mladim IT profesionalcima, tijekom eventa objavljivali smo redovite storyje na Instagramu kako bismo prikazali sva predavanja i aktivnosti tijekom konferencije.

Konferencija je bila najavljena na učeničkom portalu Srednja.hr gdje je bio objavljen članak. Informacije su dijeljene i fakultetima poput FOI-a i PMF-a. Zahvaljujući tome, konferencija je bila izvrsno posjećena, a FAKS 2025 prepoznat kao koristan događaj za studente i sigurnosnu zajednicu.

Slika 7. Primjer objave na društvenim mrežama



Slika 8. Objava rasporeda prvog dana konferencije

2.2 Rezultati

Konferencija FAKS 2025 zabilježila je posjećenost višu od očekivane, svako od predavanja je okupilo između 40 i 100 posjetitelja što nas je uvjerilo u interes i aktualnost stručnog sadržaja na temu kibernetičke sigurnosti. Posebno smo ponosni na visoku stručnosti i raznolikost predavača koji su nam svojim odazivima i podrškom dali dodatan vjetar u leđa. Pozvani predavači dolazili su iz svih karijernih putova od svjetski prepoznatih stručnjaka u regulativnim i tehničkim aspektima kibernetičke sigurnosti do mladih nada hrvatske sigurnosne scene.

Slika 9. ”tech track” predavanje

Slika 10. Keynote predavanje

Tijekom konferencije održano je i CTF natjecanje. Sudjelovali su samo natjecatelji koji su prethodno uspješno prošli kvalifikacije, čime je osigurana visoka razina kompetitivnosti. Ovo natjecanje omogućilo je studentima praktičnu primjenu stečenih znanja u rješavanju sigurnosnih izazova te je dodatno doprinijelo dinamičnosti i interaktivnosti događaja.

Slika 11. Atmosfera za vrijeme natjecanja

Slika 12. Pobjednički tim “Brr Brr Patapim”

Zaključno, rezultati konferencije FAKS 2025 pokazuju da je događaj uspješno spojio visokokvalitetan stručni sadržaj sa studentima i ostalim zainteresiranima. Velik odaziv studenata i njihovo aktivno sudjelovanje u edukacijskim i natjecateljskim aktivnostima, uz vrhunske predavače, potvrđuju da su ispunjeni glavni ciljevi konferencije.

Sažetak

RAZVOJ STUDENTSKIH KOMPETENCIJA I ZAJEDNICE KIBERNETIČKE SIGURNOSTI NA FER-U

Konferencija FAKS 2025 okupila je velik broj studentica i studenata, stručnjaka i predavača iz područja kibernetičke sigurnosti. Program je obuhvatio predavanja i CTF natjecanje, čime je omogućena praktična primjena znanja i povezivanje s industrijom. Posebno se ističe visoka stručnost predavača i veliki interes studenata, što potvrđuje relevantnost i uspješnost konferencije. Organizacija je provedena uz značajan doprinos sponzora i podršku nastavnika, čime je postignut glavni cilj podizanja razine znanja i interesa za područje kibernetičke sigurnosti na Sveučilištu.

Summary

DEVELOPMENT OF STUDENT COMPETENCIES AND THE CYBERSECURITY COMMUNITY AT FER

The FAKS 2025 conference gathered a large number of students, experts, and lecturers in the field of cybersecurity. The program included lectures and a CTF competition, enabling practical application of knowledge and networking with the industry. The conference was marked by highly qualified speakers and strong student interest, confirming its relevance and success. The event was organized with significant contributions from the sponsors and support from faculty staff, achieving its main goal of raising the level of knowledge and interest in cybersecurity within the University.