# Naučite se prepoznati, preprečiti in odzvati se na sodobne kibernetske grožnje.

SRIP GoDigital

zit SeKV

CyberHub Slovenia

## Akademija kibernetske varnosti

Brezplačna akademija kibernetske varnosti v obsegu 4 tečajev v izvedbi Fakultete za elektrotehniko, računalništvo in informatiko (UM FERI) in z možnostjo pridobitve mikrodokazila.

**Trajanje : med 14. 10. 2024 in 22. 11. 2024**

Sofinancira Evropska unija
Financira Evropska unija NextGenerationEU
Sofinancira program Evropske unije Erasmus+

# TEČAJ 1: Spletna varnost in vdorno testiranje

**Predavatelj**: izr. prof. dr. Muhamed Turkanović (UM FERI), izr. prof. dr. Marko Hölbl (UM FERI) in Milan Gabor (Viris)
**Datum: 14. 10. 2024 do 23. 10. 2024**
**Kreditne točke: 2 ECTS**

**Kratek opis:**
V okviru tečaja bodo udeleženci spoznali področje spletne varnosti in vdornega (penetracijskega) testiranja.
Predstavljena bodo načela etičnega hekanja ter s tem povezane faze etičnega hekanja, procesi, orodja in ogrodja za izvedbo le tega. Fokus bo vdorno testiranje povezano s spletnimi aplikacijami, pri čemer pa bo predstavljeno tudi izvidništvo, skeniranje omrežja, sistemsko vdiranje, itn.

V drugem delu bodo predstavljena načela spletne varnosti z vidika odjemalca, strežnika in komunikacijske povezave. Kot eden ključnih vidikov spletne varnosti bo obravnavan spletni varnostni model in njegovi gradniki (SOP, CSP, SRI, CORS), ki zagotavlja varnost na strani odjemalca. Prav tako bo predstavljen strežniški del spletne varnosti preko seznama najbolj pogostih ranljivosti (OWASP Top 10). Pri tem bodo obravnavane omenjene ranljivosti in kako se pred njimi zaščititi. Del tečaja bo tudi namenjen mehanizmom varovanja komunikacijske povezave med strežnikom in odjemalcev, kar je mogoče s pomočjo varnostnega protokola HTTPS in ustreznega upravljanja sej.

**Izobraževanje je namenjeno posameznikom**, ki bi radi pridobili/nadgradili znanja s področja celovite spletne varnosti in vdornega testiranja, ki predstavljata dopolnjujoči se temi kibernetske varnosti.

**Želena predznanja in oprema:**.
- Priporočljivo osnovno poznavanje tehnologij, ki jih bomo uporabljali: HTML, CSS, JavaScript, SQL ipd
- Osnovno znanje računalniških omrežij
- Osnovno znanje programiranja
- Na dan vaj bodo udeleženci potrebovali tudi lastne prenosnike

**Po zaključku izobraževanja bo udeleženec sposoben:**
- razumeti mehanizme, metode in protokole za zaščito spletih aplikacij, spletni varnosti model in varovanje komunikacijske povezave
- razumeti tipično spletno infrastrukturo in načine napadov
- opisati faze etičnega hekanja
- opisati etične in pravne posledice etičnega hekanja
- načrtovati vdorni test
- opisati orodja namenjenega vdornemu testiranju in njihove glavne zmogljivosti

**Urnik izobraževanja**

| Dan | Vsebina | Datum | Predviden obseg | Lokacija | Predavatelj |
|---|---|---|---|---|---|
| 1. dan | Predavanja | 14. 10. 2024 | 6 šolskih ur 9.00 do 15.00 | GZS, dvorana F | izr. prof. dr. Muhamed Turkanović (UM FERI), in Milan Gabor (Viris) |
| 2. dan | Predavanja | 15. 10. 2024 | 6 šolskih 9.00 do 15.00 | GZS, dvorana F | izr. prof. dr. Marko Hölbl (UM FERI) |
| 3. dan | Vaje | 16. 10. 2024 | 8 šolskih ur 9.00 do 16.00 | GZS Dvorana F | dr. Viktor Taneski (UM FERI) |
| 4. –7. dan | Samostojno delo | 17. – 22. 10. 2024 | | / | |
| 8. dan | Izvedba pisnega preverjanja znanja | 23. 10. 2024 | 2 šolski uri | Na daljavo | |

## TEČAJ 2: Identifikacija, overjanje in avtorizacija

**Predavatelj:** izr. prof. dr. Muhamed Turkanović (UM FERI)
**Datum: 4. 11. 2024 do 8. 11. 2024**
**Kreditne točke: 1 ECTS**

**Kratek opis:**
Izobraževanje bo zajemalo osrednje koncepte identifikacije, overjanja in avtorizacije (ang. Identification, authentication and authorization – IAA), pri čemer bomo začeli z uvodom v IAA, ključnimi koncepti in terminologijo. Raziskali bomo modele digitalnih identitet, vključno s silosnimi, centraliziranimi, federativnimi in decentraliziranimi pristopi, ter primere uporabe posameznih modelov. Nadaljevali bomo z metodami identifikacije in overjanja, kot so gesla, PIN kode, žetoni, pametne kartice, biometrija, ter overjanje na nivoju mobilnih in spletnih rešitev.
V okviru infrastrukture bomo pokrili infrastrukturo javnih ključev, X.509 certifikate, kvalificirana in nekvalificirana digitalna potrdila ter ponudnike digitalnih identitet, kot so federativno poslovni ali Google in Microsoft. V implementaciji overjanja bomo raziskali protokole in standarde, kot so OAuth2.0, OpenID Connect in SAML, ter upravljanje sej s pomočjo JWT žetonov. Poudarek bo tudi na več faktorskem overjanju z uporabo WebAuthn in FIDO2/U2F. Avtorizacijo in nadzor dostopa bomo obravnavali skozi ogrodja RBAC in ABAC ter implementacijo v sodobnih IT arhitekturah, vključno z mikrostoritvami in spletnimi storitvami. V zadnjem delu izobraževanja se bomo posvetili praktičnim aplikacijam in prihajajočim tehnologijam, kot so decentralizirane in samo-upravljane identitete, podprte z verigami blokov, ter digitalne denarnice in uredbe, kot je eIDAS 2.0.

To izobraževanje bo udeležencem omogočilo celovit vpogled v identifikacijo, overjanje in avtorizacijo, ter jih opremilo s praktičnimi znanji za učinkovito upravljanje digitalnih identitet in izboljšanje kibernetske varnosti.

**Izobraževanje je namenjeno posameznikom**, ki bi radi pridobili/nadgradili znanja za potrebe »full stack« razvijalca spletnih aplikacij, kjer bodo razvili zaledne komponente interaktivne spletne aplikacije na poljubno izbrani problemski domeni.

**Želena predznanja:**
- Osnovno razumevanje tehnologij svetovnega spleta (npr. HTTP, HTML, CSS)
- Poznavanje sistemov za nadzor verzij (npr. git) in platform (npr. GitHub)
- Poznavanje vsaj enega objektno usmerjenega programskega jezika (priporočljivo JavaScript)
- Osnovno poznavanje okolij/orodij, ki jih bomo uporabljali: Node.js, MongoDB, Docker, Visual Studio Code

**Po zaključku izobraževanja bo udeleženec sposoben:**
- razumeti koncepte digitalne identitete, overjanja in avtorizacije
- razpravljati o prednostih in slabostih različnih metod overjanja
- razumeti, kako izbrati najprimernejšo metodo overjanja,
- opisati in primerno uporabiti tehnologije za upravljanje identitet ter zagotavljanje overjanja
- izvajati in upravljati varno overjanje z uporabo protokolov in standardov, kot so OAuth2.0, OpenID Connect, SAML, ter upravljati seje s pomočjo JWT žetonov

**Urnik izobraževanja**

| Dan | Vsebina | Datum | Predviden obseg | Lokacija | Predavatelj |
|---|---|---|---|---|---|
| 1. dan | Predavanja | 4. 11. 2024 | 8 šolskih ur 9.00 do 16.00 | GZS, dvorana F | izr. prof. dr. Muhamed Turkanović (UM FERI) |
| 2. dan | Vaje | 5. 11. 2024 | 6 šolski uri | Na daljavo | Asistenti Vid Keršič, dr. Viktor Taneski (UM FERI) |
| 3. in 4. dan | Samostojno delo | 6. – 7. 11. 2024 | | / | |
| 5. dan | Izvedba pisnega preverjanja znanja | 8. 11. 2024 | 1 šolska ura | Na daljavo | |

## TEČAJ 3: Digitalna forenzika

**Predavatelj**: izr. prof. dr. Marko Hölbl
**Datum: 11. 11. 2024 do 15. 11. 2024**
**Kreditne točke: 1 ECTS**

**Kratek opis:**
Obravnavali bomo pojem in načela digitalne forenzike ter predstavili postopek forenzične analize. Pogledali si bomo metodologijo preiskave in s tem povezan pojem skrbniške verige, postopek zbiranja digitalnih dokazov ter poročanje in dokumentacijo, ki sta pomemben sestavni del digitalne forenzike. Obravnavali bomo tudi orodja in tehnike, ki se uporabljajo v postopku, kot so forenzično ustrezen zajem podatkov, časovni podatki in obnovitev izbrisanih podatkov. Prav tako bomo na kratko podali povezano tehnično ozadje, kot so datotečni sistemi in specifične pomnilniške naprave. Za zaključek bomo digitalno forenziko pogledali skozi prizmo različnih okolij, ki vključujejo forenziko brskalnikov, omrežij in elektronske pošte.

**Izobraževanje je namenjeno posameznikom,** ki bi radi pridobili znanja o digitalni forenzika, njenem tehničnem ozadju in uporabi.

**Želena predznanja:**
- Osnovno poznavanje informacijske varnosti
- Osnovno poznavanje računalniških sistemov (npr. operacijski sistemi)
- Osnovno poznavanje računalniških omrežij;
- Osnovno poznavanje programiranja

**Po zaključku izobraževanja bo udeleženec sposoben:**
- opisati postopek zbiranja digitalnih dokazov in njihovo analizo
- aplicirati načela zbiranja dokazov
- uporabiti orodja in tehnike za analizo digitalnih dokazov
- prepoznati in ovrednotiti ključne tehnike forenzične analize
- kritično ovrednotiti forenzične dokaze

**Urnik izobraževanja**

| Dan | Vsebina | Datum | Predviden obseg | Lokacija | Predavatelj |
|---|---|---|---|---|---|
| 1. dan | Predavanja | 11. 11. 2024 | 6 šolskih ur 9.00 do 15.00 | GZS, dvorana F | izr. prof. dr. Marko Hölbl (UM FERI) |
| 2. dan | Vaje – asinhrone vsebine (video s predstavitvijo orodja in naloge) | 12. 11. 2024 | 4 šolske ure | Na daljavo | doc. dr. Marko Kompara (UM FERI) |
| 3. in 4. dan | Samostojno delo | 13. – 14. 11. 2024 | | / | |
| 5. dan | Izvedba pisnega preverjanja znanja | 15. 11. 2024 | 1 šolska ura | Na daljavo | izr. prof. dr. Marko Hölbl (UM FERI) |

## TEČAJ 4: Upravljanje informacijske varnosti

**Predavatelj**: doc. dr. Lili Nemec Zlatolas in doc. dr. Marko Kompara
**Datum: 18. 11. 2024 do 22. 11. 2024**
**Kreditne točke: 1 ECTS**

**Kratek opis:**
Tečaj upravljanja informacijske varnosti je osnovan na podlagi in vključuje vsebine, potrebne za ISACA certifikat CISM (Certified Information Security Manager). V skladu s tem je tudi tečaj razdeljen na štiri področja:

- Vodenje informacijske varnosti: organizacijska kultura, strukture, vloge in odgovornosti, strategija informacijske varnosti, ogrodja in standardi upravljanja informacij, metode pregleda informacijske varnosti…
- Upravljanje tveganj informacijske varnosti: ogrodja za obvladovanje/upravljanje tveganj, ocena, vrednotenje tveganj, odziv na informacijska tveganja, spremljanje, poročanje in sporočanje o tveganjih…
- Program informacijske varnosti: razvoj programa informacijske varnosti in sredstva/viri, standardi in ogrodja IV, metrike programa, varnostne kontrole…
- Upravljanje incidentov: upravljanje incidentov in načrti odzivanja nanje, obvladovanje incidentov, obveščanje, odpravljanje, obnova in pregled incidenta, vpliv na poslovanje in neprekinjeno delovanje, načrtovanje obnovitve po nesreči…

**Izobraževanje je namenjeno posameznikom**, ki bi se radi naučili ali nadgradili znanja o upravljanju informacijske varnosti. Posebej je primerno za tiste, ki delujejo ali bi želeli delati na delovnih mestih, ki usmerjajo informacijsko varnost v podjetjih (vodja informacijske varnosti, vodja informatike, CISO ipd.). Izobraževanje je tudi dobra začetna točka za tiste, ki razmišljajo o certificiranju CISM.

**Želena predznanja:**
- Osnovno poznavanje konceptov informacijske varnosti

**Po zaključku izobraževanja bo udeleženec sposoben:**
- prepoznati standarde, ogrodja in zahteve za upravljanje informacijske varnosti
- razpravljati o prednostih in pomanjkljivostih skladnosti z varnostnimi zahtevami
- oblikovati strateški varnostni načrt in varnostno politiko
- razumeti običajna tveganja in kontrole na področju informacijske varnosti
- razumeti kompleksnost upravljanja ljudi, procesov in tehnologije za doseganje informacijske varnosti
- prepoznati osnovne ekonomske zahteve in zahteve po virih, ki so potrebni za doseganje ciljev organizacije na področju informacijske varnosti

**Urnik izobraževanja**

| Dan | Vsebina | Datum | Predviden obseg | Lokacija | Predavatelj |
|---|---|---|---|---|---|
| 1. dan | Predavanja | 18. 11. 2024 | 6 šolskih ur 9.00 do 15.00 | GZS, dvorana F | doc. dr. Lili Nemec Zlatolas (UM FERI), doc. dr. Marko Kompara (UM FERI) |
| 2. dan | Predavanja in vaje | 19. 11. 2024 | 4 šolske ure | Na daljavo | doc. dr. Lili Nemec Zlatolas (UM FERI) |
| 3. in 4. dan | Samostojno delo | 20. – 21. 11 2024 | | / | |
| 5. dan | Izvedba pisnega preverjanja znanja | 22. 11. 2024 | 1 šolska ura | Na daljavo | doc. dr. Lili Nemec Zlatolas (UM FERI) |