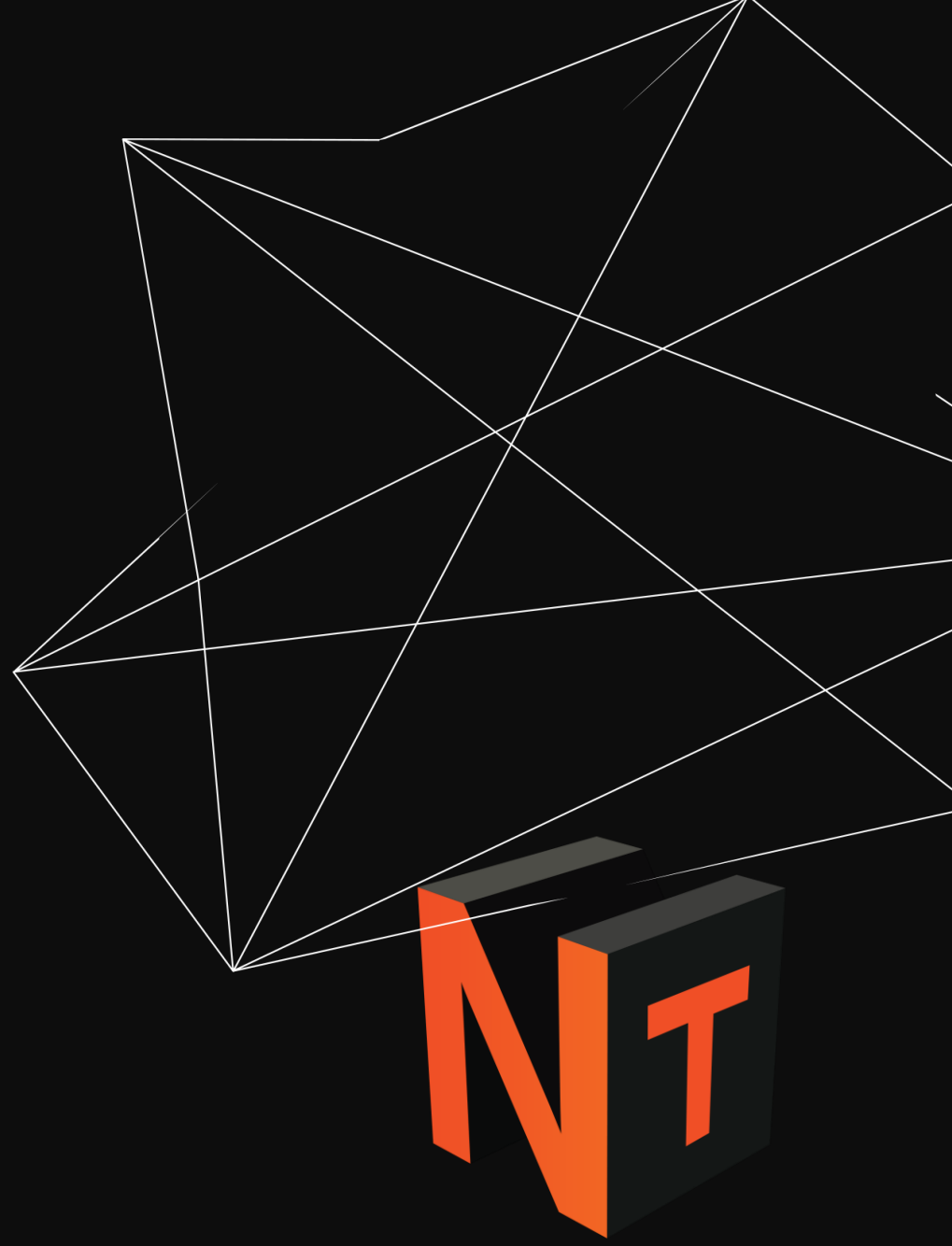
Microsoft

Ko se heker in razvijalec srečata na virtualni kavi

Milan Gabor
Gregor Spagnolo



#ntk18

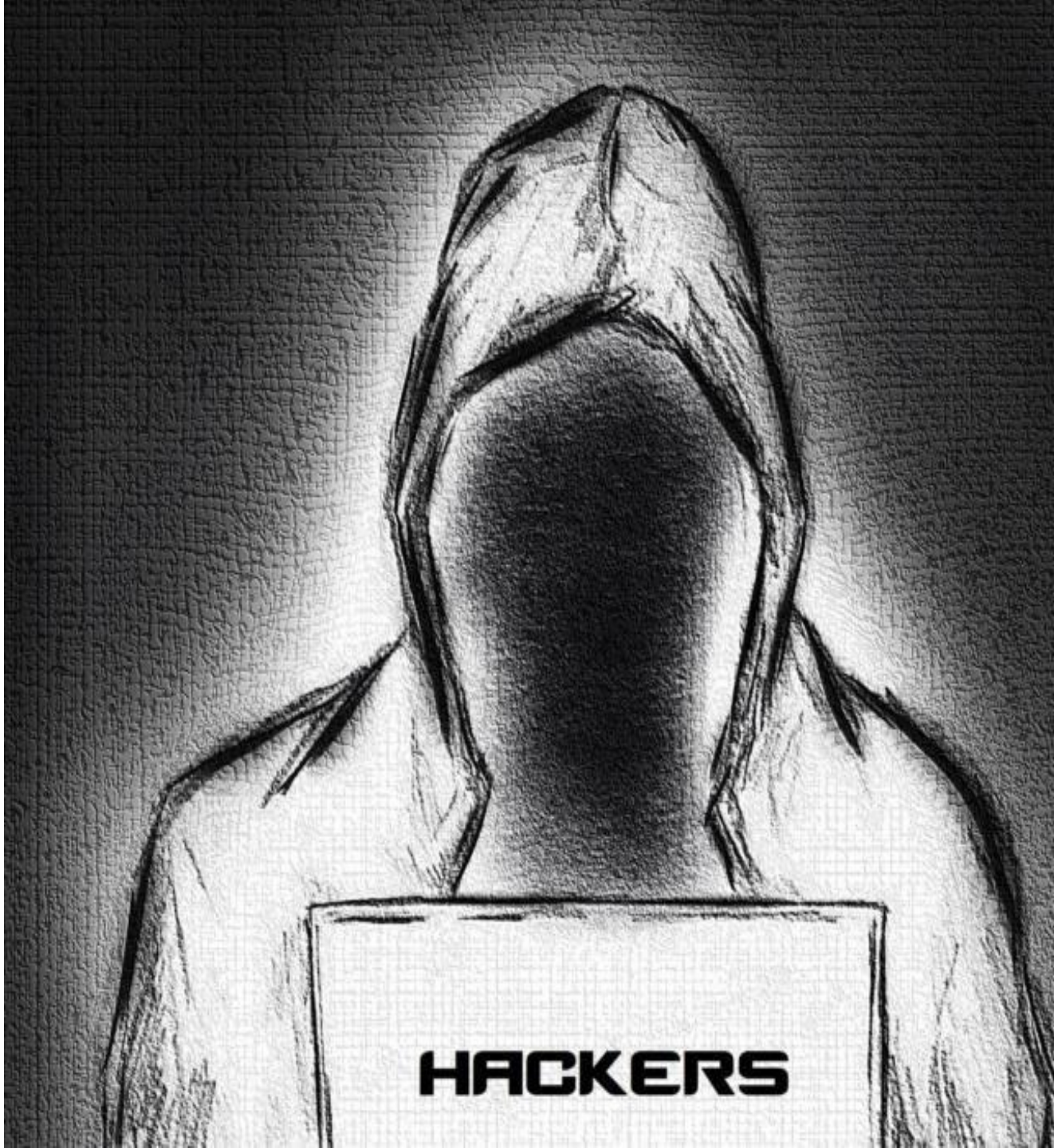
2018
NT Konferenca
Portorož | 22. - 24. maj 2018

Heker

Ni razvijalec

Rad razbija stvari

Posebej rad ima nevešče razvijalce



Orodja

Kali Linux

Razvijalec

G33k

Latest&Gratest

Ni še bil na izobraževanju s tega področja

Orodja

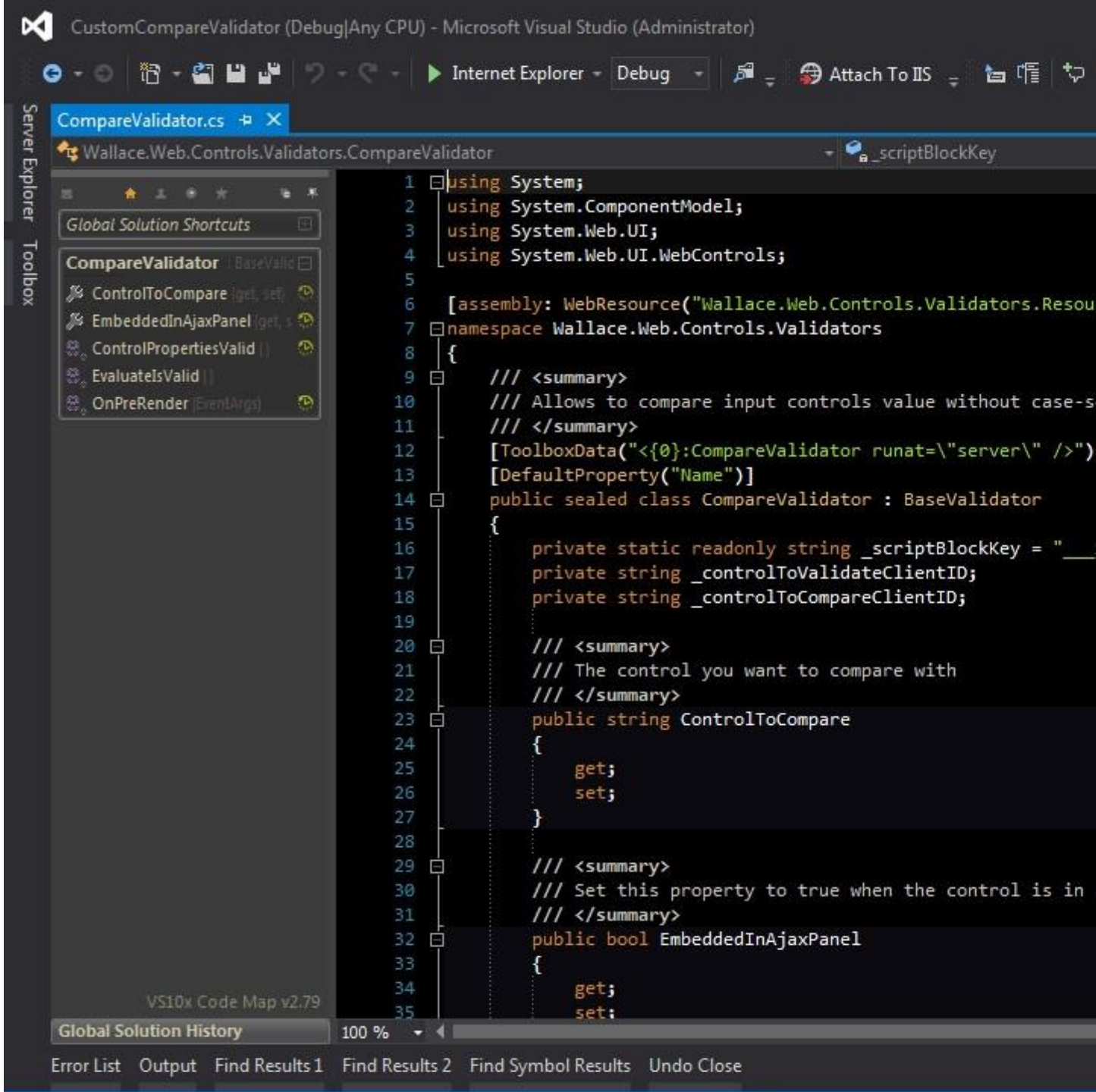
Visual studio

Git

Docker

Linux

#ntk18



Aplikacije

Velika množica pregledanih aplikacij

Veliko ponavljajočih se napak

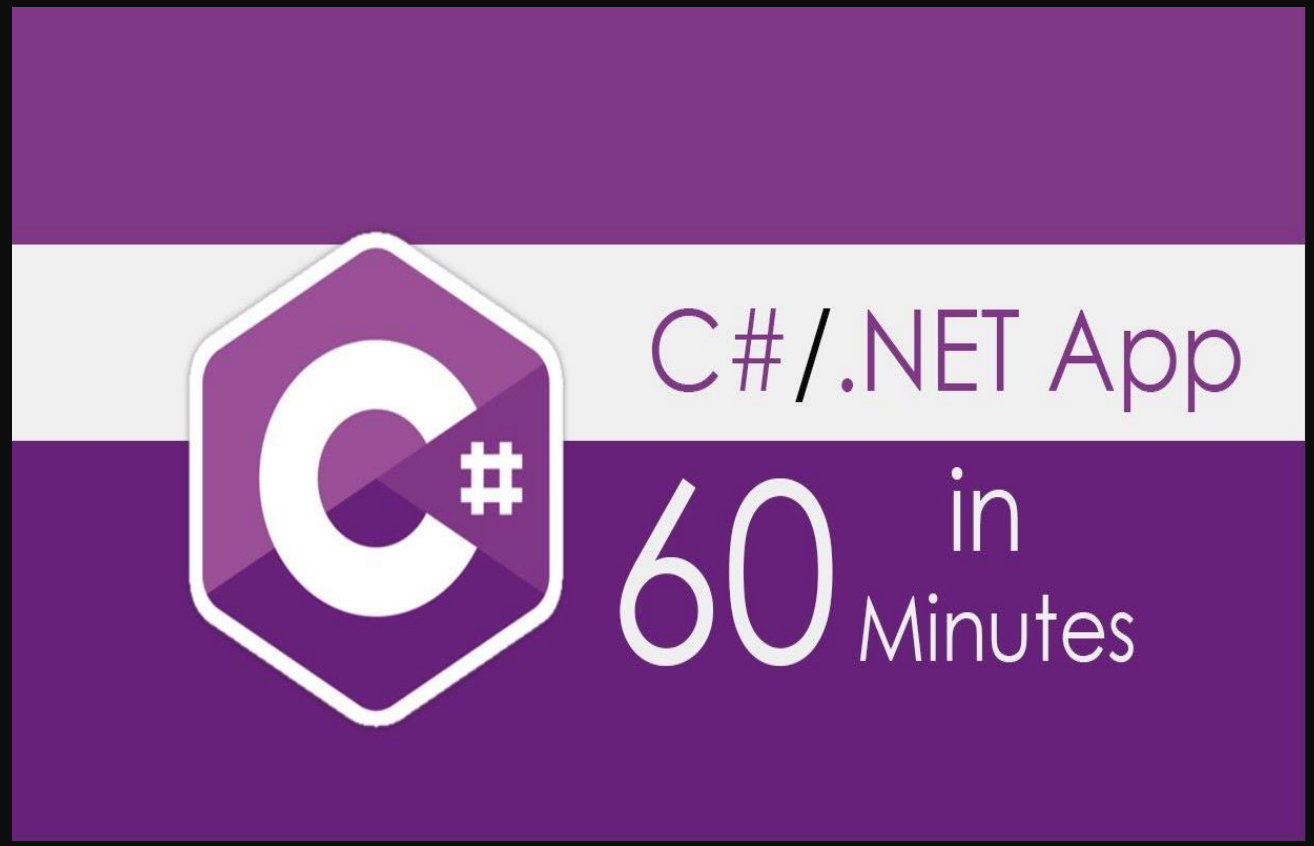
Niso odvisne od tehnologije

Copy paste

Roki

O aplikaciji

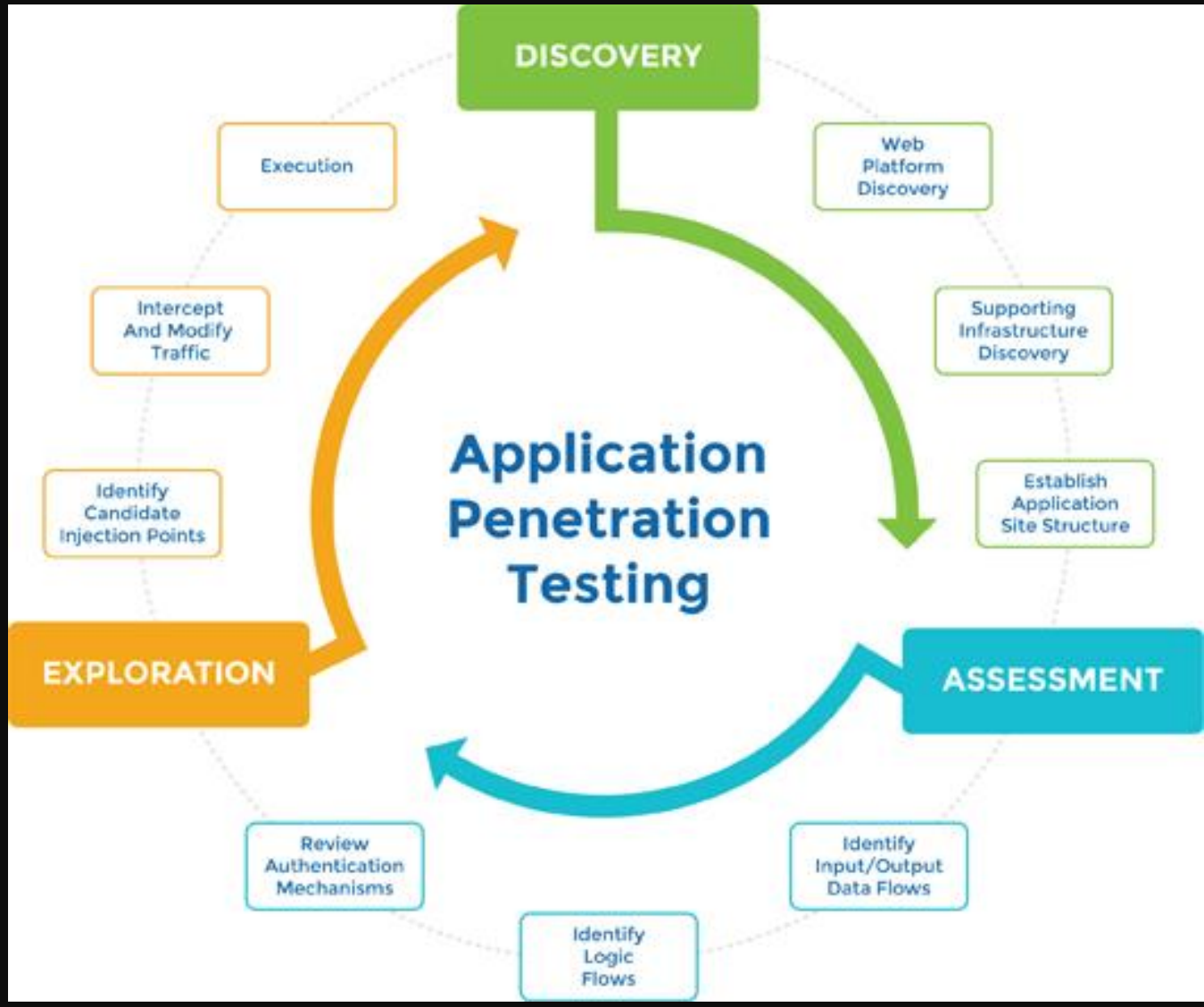
.Net Core
Jquery
API
Docker build
Git SC




Virtual
Coffee
Date

Faze

1. OSINT
2. Avtomatska analiza
3. Analiza in identifikacija
4. Kraja podatkov, razmaličenje, ...
5. Izkoriščanje



OSINT

Google
Shodan
Drugi iskalniki

Aktivno skeniranje

Nikto

OWASP ZAP

Burp

Drugi namenski skenerji in proksiji

Aktivno izkoriščanje

OWASP TOP 10
OWASP Testing metodologija
Druge aktivnosti na podlagi izkušenj
Včasih nujne nore ideje

Najdene stvari

- git
- swagger
- auth controller logging passwords
- APITransaction -> brez autorizacije
- Logs (exposed)
- transaction create stored XSS
- transaction create senderId se lahko spreminja
- search sql injection

OWASP

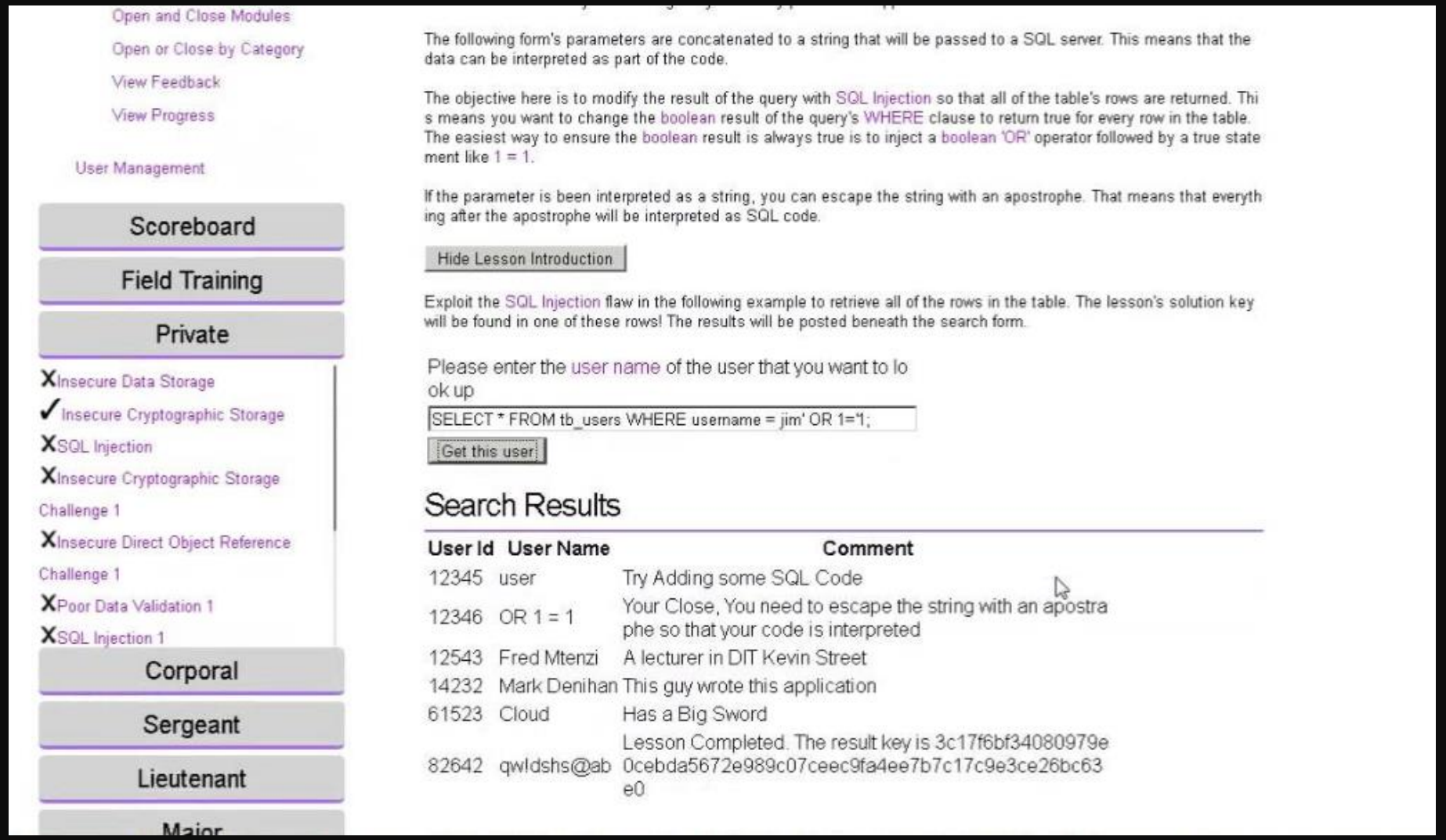
- Open Web Application Security Project
  - Odprta skupnost
  - Neprofitna organizacija
- Glavni cilj
  - Varna programska oprema

- https://www.owasp.org

OWASP TOP 10

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Primer: OWASP Security Shepherd



Priporočila za varnejše spletne Aplikacije

- Sistem
  - Popravki
  - Ustrezne verzije
  - Nadzor
  - Odstranitev nepotrebnih aplikacij
- Aplikacije
  - Zadnja verzija?
  - Nepotrebni moduli?
  - Izveden pregled ali vsaj avtomatski sken?

Kako zaščiti aplikacije/sisteme

- Vgraditi varnost v cel življenjski cikel
  - Uporabiti varnostne principe v vseh fazah in aktivnostih
- Izobraževanje
  - Zavedanje se potencialnih napadov
  - Pošiljanje ljudi na različne izobraževanja (tudi NTK šteje)

Izobraževati

- **Razvijalce** – Najboljše prakse iz varnega razvoja SW
- **Testerje** – Metode za identifikacijo ranljivosti
- **Varnostne inženirje** – Proces varnega razvoja SW
- **Lastnike, menedžment** – Razumeti tveganja in zakaj je to sploh pomembno za varnost spletnih aplikacij

Ustrezna kombinacija

Sharing is caring

Skupaj za istim ciljem

Varno programiranje

Seznanitev s tipičnimi napakami
Uporaba zadnjih tehnologij
Za noobs in seniors
Kombinacija napada in obrambe
Developer + Hacker

#ntk18

@MilanGabor

@GregorSpagnolo