

PTWEBDISCOVER

Nástroj pro efektivní mapování webových aplikací
během penetračního testování

Willi Lazarov, Zdeněk Martinásek, Roman Kümmel

č. projektu TJ04000456



T A
Č R

Tento projekt je spolufinancován se státní
podporou Technologické agentury ČR v rámci
Programu ZÉTA.

www.tacr.cz
Výzkum užitečný pro společnost.

Vize



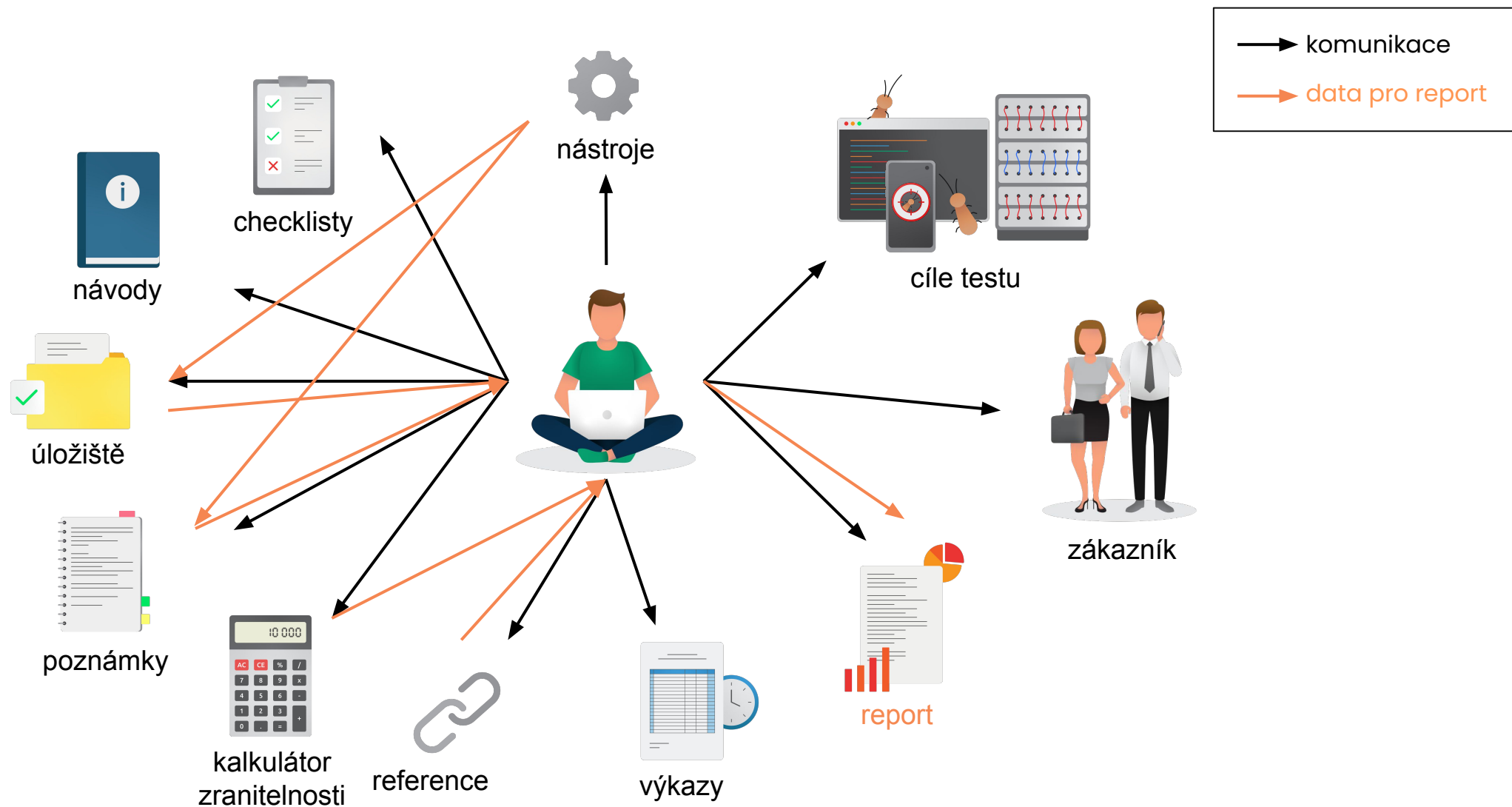
Usnadnit a zrychlit práci penetračním testerům.

Problém

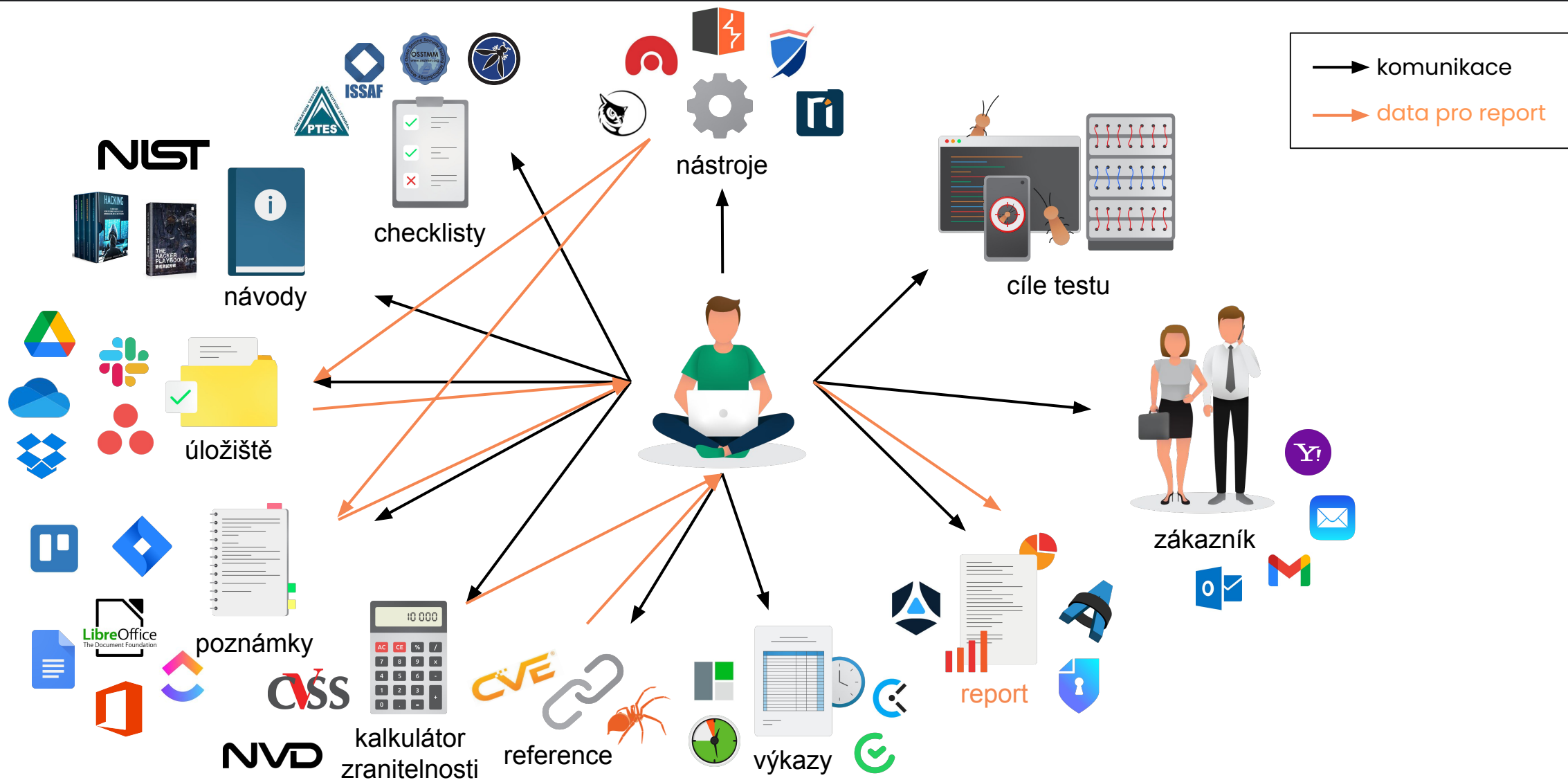
- Penetrační testování je závislé na zkušenostech testera.
- Specializace testera na konkrétní oblast.
- Nedostatek kvalitních (zkušených) pracovníků.
- Neexistují „step-by-step“ návody pro realizaci testů.
- Během testování se používá velké množství různých nástrojů.
- Výsledky automatizovaných nástrojů se přepisují do poznámek.
- Tester hodnotí nálezy podle definovaného standardu (kalkulačky).
- Report se píše v textovém editoru a jeho tvorba je velice náročná.
- Tester by si měl vést výkaz práce a odpracovaných hodin.

Tester věnuje až 90% svého času jiným věcem, než samotnému testování.

Penetrační testování dnes



Penetrační testování dnes

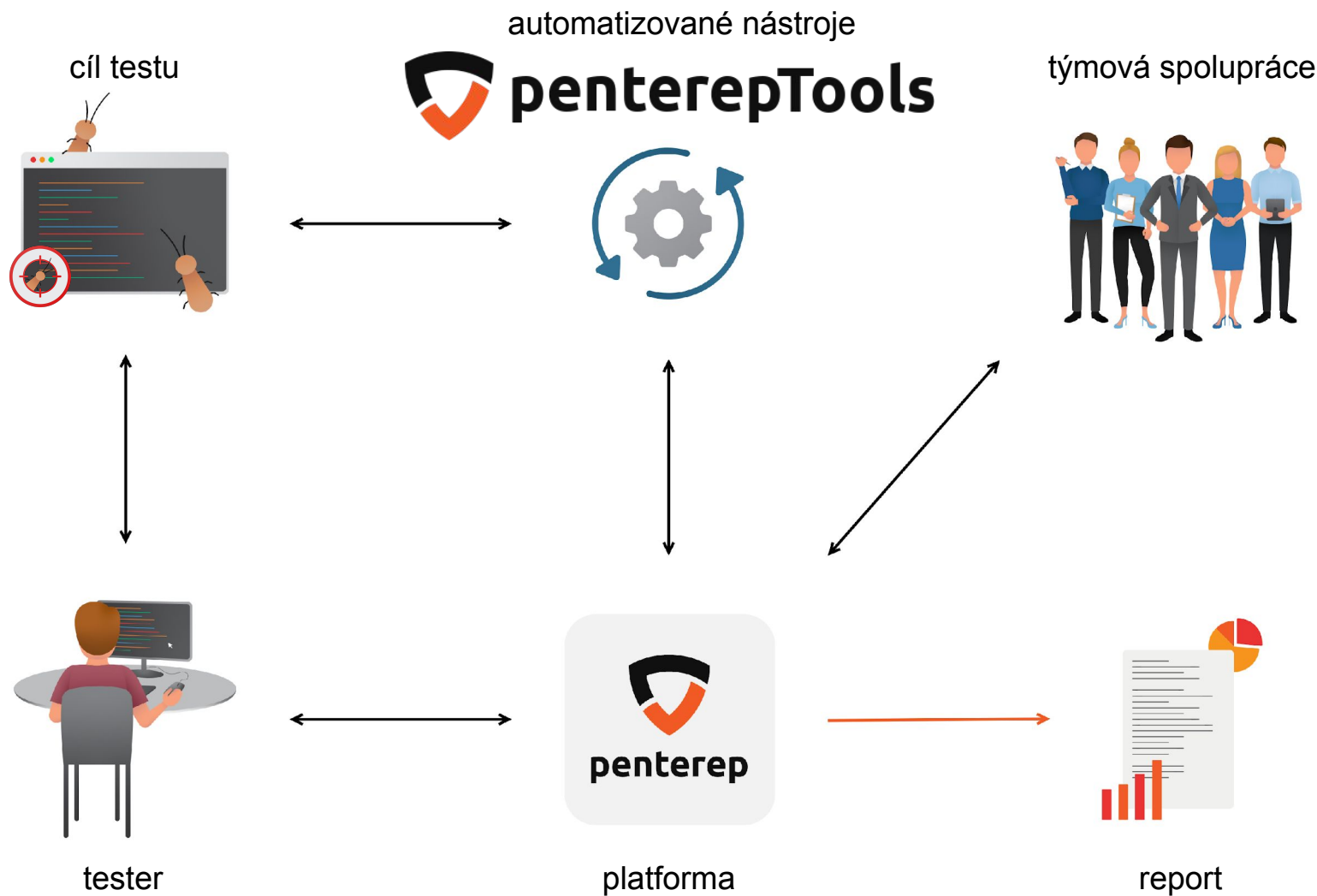


Řešení

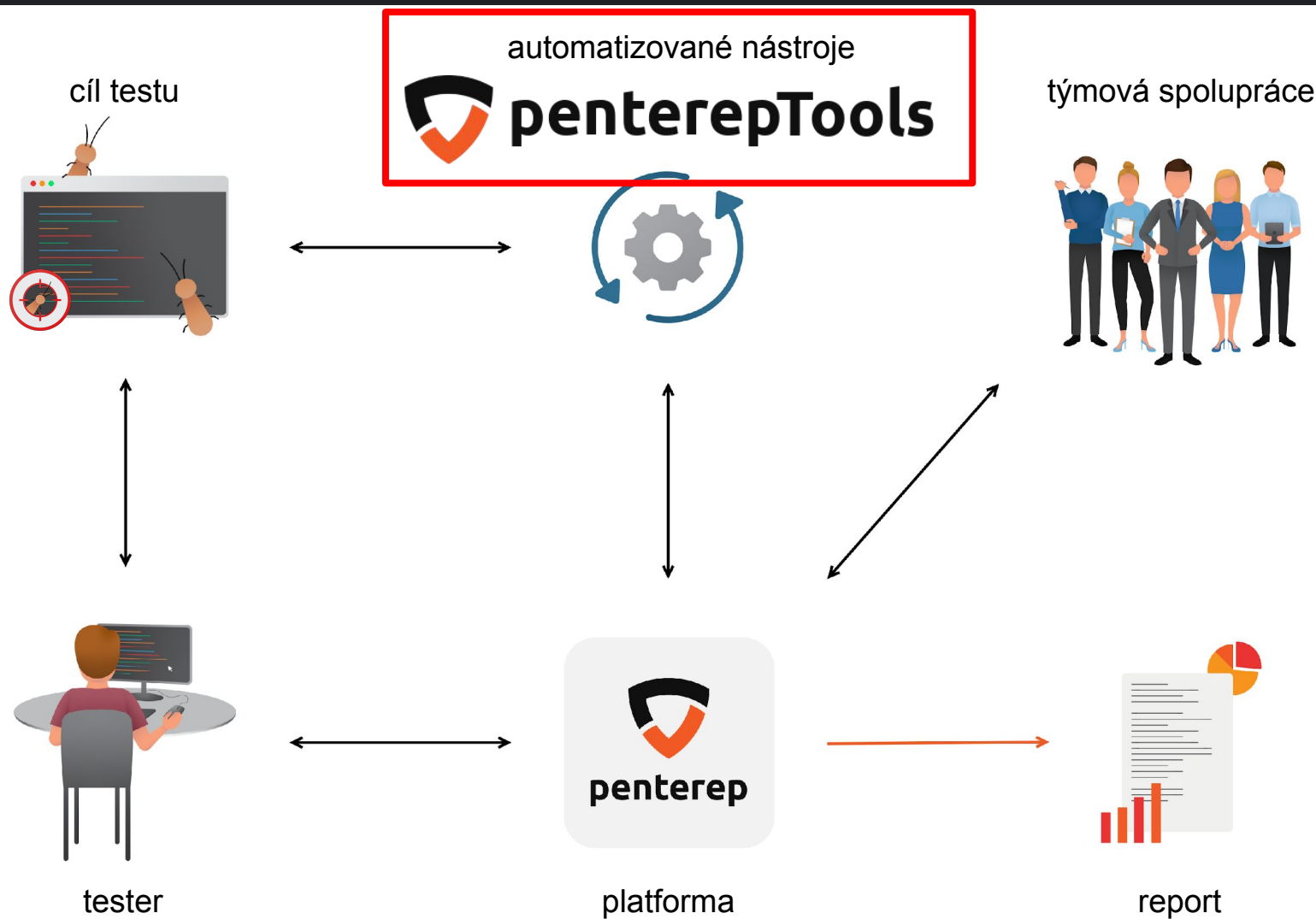
- Řešením problému je vytvoření platformy, která:
 - poskytne „step-by-step“ návod, jak provést penetrační test,
 - propojí automatizované a manuální testování,
 - umožní ukládat všechny relevantní informace na jednom místě,
 - umožní týmovou spolupráci,
 - automaticky vytvoří pracovní výkazy,
 - automaticky vygeneruje report ze sesbíraných dat,
 - poskytuje odhad pracnosti a manažerské přehledy.

Tester může věnovat více než 90% času samotnému testování.

Řešení s platformou Penterep



Řešení s platformou Penterep



Ukázka Penterep

- Ukázka platformy <https://www.youtube.com/watch?v=JlEhrZwI-4M>
- Představí mistr **Roman Kümmel** :)



PenterepTools

- Cílem je vývoj **nástrojů podporující manuální penetrační testování**.
- Skripty testují **specifické zranitelnosti** (20 nástrojů).
- Kompatibilita s nástrojem Penterep.
- Nástroje jsou dostupné pod licencí **GNU GPLv3**.
- Stažení **37 000+** k 29.5.2022

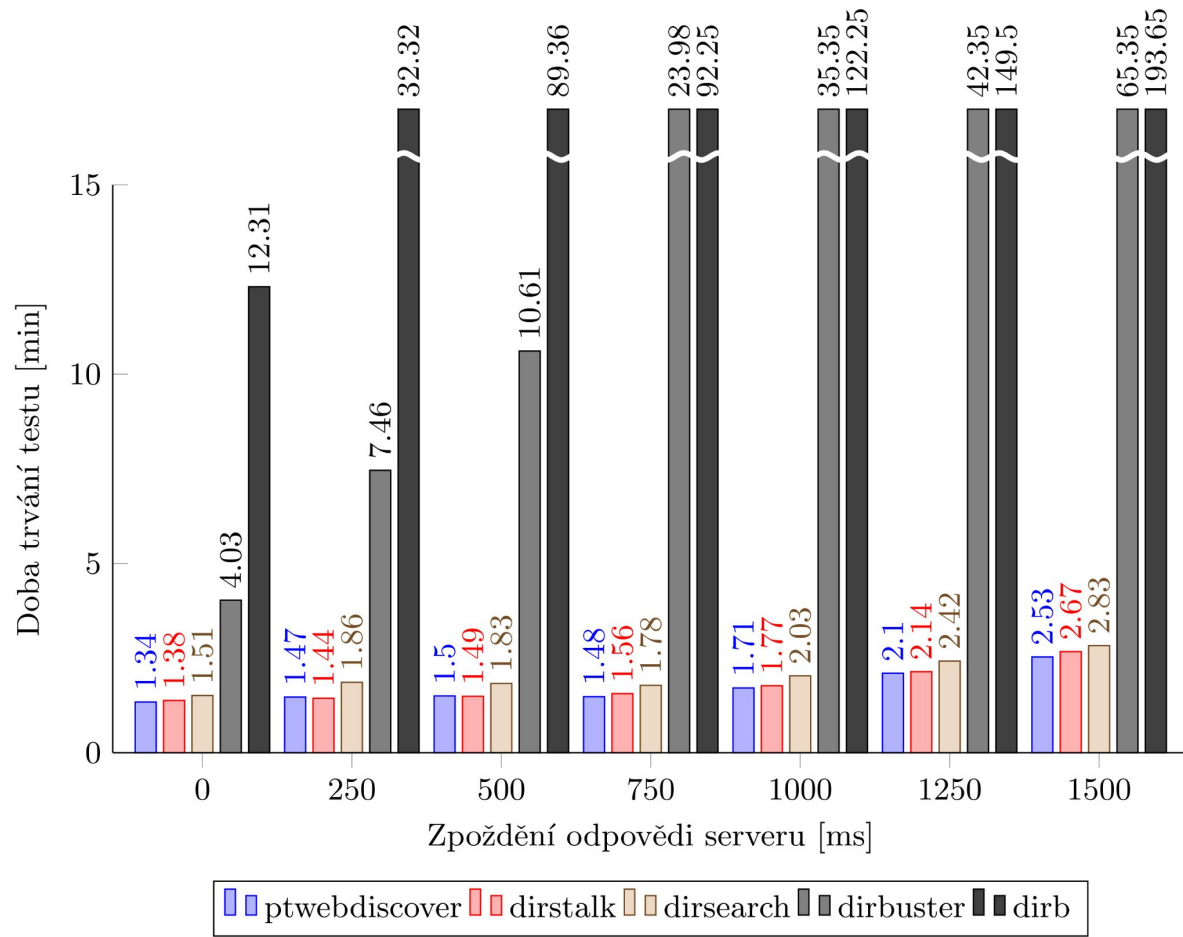
Název nástroje	Účel nástroje
ptdos	Skript pro testování DoS zranitelností
ptvulnsearcher	Skript pro vyhledávání známých zranitelností ke konkrétním technologiím
pttechident	Skript pro identifikaci použitých technologií
ptmanager	Správce nástrojů a automatizovaných testů
ptwebdiscover	Nástroj pro mapování webových aplikací
ptsess	Skript pro otestování zranitelností Autentizace a Session managementu
	Automatické přihlášení/odhlášení
	Ověření přihlášené session
	Otestování zranitelnosti Session Fixation
	Otestování, zda server odmítá session, které sám nevygeneroval
	Otestování, zda server nepřevezme session z URL
	Otestování cookies
ptsamesite	Otestování zranitelnosti Same-Site-Scripting
ptaxfr	Otestování zranitelnosti DNS Zone Transfer
ptmethods	Zjištění seznamu povolených HTTP metod
ptcrossdomain	Otestování Cross Domain Policy
ptptssi	Otestování zranitelnosti PRSSI
ptcrossdomain	Otestování výskytu a obsahu souboru Crossdomain.xml
ptsecurixt	Otestování výskytu souboru security.txt
ptgetpage	Nástroj pro načtení obsahu webové stránky
ptinsearcher	Nástroj pro zjištění kontaktních informací uvedených na webové stránce
	Nástroj pro zjištění seznamu formulářů na webové stránce
	Nástroj pro vytažení komentářů z HTML kódu webové stránky
	Nástroj pro získání metadat ze souboru
ptcookiepedia	Nástroj pro zjištění informací o cookie z webu cookiepedia.co.uk
ptiistild	Otestování zranitelnosti IIS Tilde Enumeration
ptiistild	Získání seznamu souborů skrz zranitelnost IIS Tilde Enumeration
ptmultiviews	Otestování zranitelnosti Apache Multiviews
ptssl	Nástroj pro kontrolu kvality SSL klíčů
	Nástroj pro kontrolu povolených šifrovacích algoritmů
	Nástroj pro kontrolu zranitelnosti Heartbleed a Ticketbleed
	Nástroj pro kontrolu zranitelnosti Poodle, ROBOT, BEAST a Crime
	Nástroj pro kontrolu zranitelnosti OpenSSL CCS vuln.
	Nástroj pro kontrolu zranitelnosti OpenSSL Padding Oracle vuln.
ptburpcon	Nástroj pro kontrolu SSL/TLS compression a OpenSSL 0-Length
ptburpcon	Burp Suite Connector

Nástroj ptwebdiscover

- Nástroj pro průzkum prostředí webové aplikace.
- Výhody oproti současným nástrojům.
- **Inteligentní vyhledávání záloh.**
- **Flexibilita a efektivita** vyhledávání.
- **Rychlost** vyhledávání.
- Možnost uložení a parsování obsahu.

Funkcionalita	ptwebdiscover	dirstalk	dirb	dirbuster	dirsearch
Hledání souborů	✓	✓	✓	✓	✓
Hledání adresářů	✓	✓	✓	✓	✓
Hledání subdomén	✓	✗	✗	✗	✗
Fuzzing parametrů	✓	✗	✗	✗	✗
Hledání v libovolné části URL	✓	✗	✗	✗	✗
Použití hrubé síly	✓	✗	✗	✓	✗
Použití slovníků	✓	✓	✓	✓	✓
Filtrování slovníků	✓	✗	✗	✗	✗
Testování přípon	✓	✗	✓	✓	✓
Možnost načtení přípon ze souboru	✓	✗	✓	✗	✓
Nastavení minimální délky řetězce	✓	✗	✗	✓	✗
Nastavení maximální délky řetězce	✓	✗	✗	✓	✗
Použití prefixů a sufixů	✓	✗	✗	✗	✓
Identifikace použitých technologií	✓	✗	✗	✗	✗
Inteligentní vyhledávání záloh	✓	✗	✗	✗	✗
Rekurzivní procházení adresářů	✓	✗	✓	✓	✓
Upozorňování na directory listing	✓	✗	✓	✗	✓
Načtení URL adres pro otestování	✓	✗	✗	✗	✓
Použití libovolné HTTP metody	✓	✓	✗	✓	✓
Nastavení cookies	✓	✓	✓	✓	✓
Nastavení hlavičky User-Agent	✓	✓	✓	✓	✓
Nastavení HTTP request hlaviček	✓	✓	✓	✓	✓
Použití proxy serveru	✓	✓	✓	✓	✓
Běh ve více vláknech	✓	✓	✗	✓	✓
Nastavení prodlevy mezi requesty	✓	✓	✓	✗	✓
Pozitivní hledání řetězce v odpovědi	✓	✗	✗	✗	✗
Negativní hledání řetězce v odpovědi	✓	✗	✗	✗	✗

Porovnání rychlosti nástroje



Ukázka ptwebdiscover

- Ukázka nástroje <https://youtu.be/sBmAW7ku99A>
- Nechť tě provází síla PADAWANE !



Závěr

- Platforma **Penterep**:
 - **hlavní softwarový výsledek** juniorského projektu TA ČR ZÉTA (řešení 1.5.2020 až 30.4.2022)
 - příprava beta testování (NÚKIB a CyberRangers),
 - možnost spolupráce? (MU ?, finanční sektor ?).
- Nástroje **PenterepTools**:
 - penetrační testování webových aplikací,
 - aktuálně 20 nástrojů volně ke stažení,
 - `ptwebdiscover` (2 600+ stažení) a `ptinsearcher` (5 000+ stažení),
 - další nástroje budou cílit na testování síťové infrastruktury.

Tým



Roman Kümmel

- HACKER Consulting s.r.o.
- Penetrační tester
- r.kummel@penterep.com



Willi Lazarov

- Výzkumný pracovník na VUT
- Student IT bezpečnosti
- xlazar15@vut.cz



doc. Ing. Zdeněk Martinásek, Ph.D.

- Docent na VUT
- Vedoucí výzkumu
- martinasek@vut.cz

Děkuji za pozornost!

Dotazy ?