# Testerský slovník časť 18:

(postupne budem zverejňovať pojmy, ktoré som nazbierala)

**Stacktrace**

(alebo „výpis zásobníka volaní“) je technický výpis, ktorý ukazuje **reťazec volaní funkcií**, ktoré viedli k chybe alebo výnimke v programe.

**Feature toggles**

sú prepínače, ktorými možno zapnúť alebo vypnúť konkrétnu funkcionalitu bez nutnosti meniť kód.Umožňujú napríklad nasadiť funkciu na všetky prostredia, ale aktivovať ju len v niektorých z nich (napr. len v teste).

**SMTP**

(Simple Mail Transfer Protocol) je protokol na odosielanie e-mailov z aplikácie – typicky sa používa na zasielanie notifikácií, potvrdení objednávky alebo resetovacích odkazov. V testovaní je dôležité overiť, či je SMTP správne nakonfigurovaný, aby e-maily odchádzali a neboli zablokované alebo označené ako spam.

**Build number**

je číselný identifikátor konkrétneho zostavenia (build-u) aplikácie. Pomáha rozlíšiť jednotlivé verzie softvéru – napríklad ak vývojári vykonali zmeny a znova aplikáciu zbuildovali, každé nové zostavenie dostane nové „build number“, čo umožňuje presne sledovať, ktorá verzia je nasadená v ktorom prostredí.

**Commit hash**

je jedinečný identifikátor (zvyčajne dlhý reťazec znakov), ktorý označuje konkrétny commit v systéme na správu verzií (napr. Git). Vďaka nemu vieš presne určiť, aký kód bol nasadený – aj keď dve verzie aplikácie vyzerajú rovnako, rôzny commit hash odhalí, že pochádzajú z iného stavu vývoja.

**Version endpoint**

je špeciálne API rozhranie (napr. /version), ktoré vracia aktuálne informácie o nasadenej verzii aplikácie – ako napr. číslo buildu alebo commit hash. Tester si tak vie jednoducho overiť, či je v danom prostredí nasadená správna verzia softvéru.

**Debug logy**

sú detailné výpisy z aplikácie určené najmä pre vývojárov – obsahujú technické informácie, ktoré pomáhajú pri hľadaní chýb (napr. hodnoty premenných, priebeh funkcií). V produkčnom prostredí by nemali byť zapnuté, pretože môžu spomaliť aplikáciu a odhaliť citlivé informácie.

**Latency**

je oneskorenie medzi požiadavkou a reakciou – teda čas, ktorý uplynie od odoslania požiadavky (napr. klik na tlačidlo) po prijatie odpovede zo servera. V testovaní je dôležité sledovať, či toto oneskorenie neprekračuje akceptovateľné limity, najmä pri prechode na produkčné prostredie, kde môže byť infraštruktúra odlišná.

**HTTP**

(Hypertext Transfer Protocol) je základný komunikačný protokol, pomocou ktorého prehliadač posiela požiadavky na webový server a prijíma odpovede (napr. HTML stránky, obrázky, API odpovede). Je to nezabezpečený protokol – preto sa v praxi často používa jeho bezpečná verzia HTTPS, ktorá navyše šifruje komunikáciu.

**HTTPS**

(Hypertext Transfer Protocol Secure) je zabezpečená verzia protokolu HTTP, ktorá šifruje komunikáciu medzi prehliadačom a serverom pomocou SSL/TLS certifikátu. Vďaka tomu sú údaje chránené pred odpočúvaním, manipuláciou a falošnými stránkami.

**TLS**

(Transport Layer Security) je kryptografický protokol, ktorý zabezpečuje šifrovanie a integritu dát pri prenose medzi klientom a serverom – je nástupcom SSL. Používa sa v spojení s HTTPS a zabezpečuje, že komunikácia nemôže byť odpočúvaná ani zmenená.

**DNS**

(Domain Name System) je systém, ktorý prekladá názvy domén (napr. example.com) na IP adresy serverov, kde beží aplikácia. Ak DNS nefunguje správne alebo je zle nastavený, aplikácia sa nemusí načítať, pretože sa klient nedostane na správny server.

**Redirect**

je automatické presmerovanie používateľa z jednej adresy na inú – napríklad keď zadáš example.com a prehliadač ťa presmeruje na https://www.example.com. V testovaní kontrolujeme, či sú tieto presmerovania správne nastavené (napr. HTTP → HTTPS alebo staré URL → nové) a či nevedú na chybné alebo neexistujúce stránky.

**SSL certifikáty**

slúžia na zabezpečenie šifrovanej komunikácie medzi klientom a serverom (napr. pri HTTPS). Overením certifikátu zisťujeme, či je platný, vydaný dôveryhodnou autoritou a či zodpovedá doméne, na ktorej beží aplikácia.

**CSP**

(Content-Security-Policy)je bezpečnostný HTTP header, ktorý určuje, z akých zdrojov môže webová stránka načítať obsah (napr. skripty, obrázky, štýly). Pomáha zabrániť útokom ako Cross-Site Scripting (XSS), pretože obmedzuje, čo sa môže na stránke spúšťať a odkiaľ.

**X-Frame-Options**

je bezpečnostný HTTP header, ktorý určuje, či sa môže stránka zobraziť v rámci iného webu (napr. v <iframe>). Slúži ako ochrana pred útokmi typu „clickjacking“, kde by útočník mohol cez neviditeľné prekrytie manipulovať so stránkou bez vedomia používateľa.

**CORS**

(Cross-Origin Resource Sharing)je bezpečnostný mechanizmus, ktorý určuje, ktoré domény môžu pristupovať k zdrojom (napr. API) na inej doméne. Ak nie je CORS správne nastavený, aplikácia môže buď zbytočne blokovať požiadavky, alebo naopak umožniť prístup neoprávneným doménam, čo je bezpečnostné riziko.

Týmto nekončíme, len začíname. Dajte do komentov termíny alebo slovné spojenia, s ktorými ste sa pri testovaní stretli. Tie, ktoré vás zaujali, nevedeli ste, čo znamenajú a pod.

**#tester #testovacislovnik #manualnytester #automatizovanytester #ITtester #QA #ITkariera**

integrity constraints

orphan records

stavový diagram

UML

**session management**

batch processing

cache invalidácia

force refresh

**A/B testovanie**

HSTS

maintenance mode

feature flag

fuzzy match

spätná kompatibilita

**UTC**

Responzivita

Trigger

**REST API**

**SOAP API**

OAuth

deprecated polia

screenshot

layout

UI

UX

**Token**

multibyte znaky

**forgot password flow**

**performance test**

**MVP**

**MAU**

**PaaS**

**SEO**

**iOS**

**Android**

**BFF (Backend for Frontend)**

**API Gateway**

**rate-limit**

**ML pipeline**

**NSFW/duplikáty**

**Funnel**

**Cohorty**

**Elasticsearch**

**OpenSearch**

**Meilisearch**

**CDN**

**cache feed**

**RabbitMQ**

**SQS**

**Remote config**

**LaunchDarkly**

**Observabilita**

**OIDC (Sign-in Apple/Google)**

**krátke JWT + refresh tokeny v secure úložisku klienta**

**Signed URLs pre upload/download médií**

**WAF**

**Mikroslužby (scale-out)**

**JVM**

**Kotlin Multiplatform Mobile (KMM)**

**SwiftUI Compose bridge**

**CDN**

**Ne­funkčné požiadavky (NFR)**

**Monorepo**

**Polyrepo**

**SAST (CodeQL/semgrep)**

**canary/blue-green nasadenia**

**Terraform**

**Vault/SM**

**guardrail na postupné rollouty**

**BFF (ohľadne contract testov)**

**RPS**

**cold/warm cache**

**DAST (OWASP ZAP)**

**mobilné MASVS checky**

**Scope creep**

**nice-to-have**

**JS/TS doména**

**SDK**

**IDE**

**gRPC**

**ACID**

**MVCC**

**JSONB**

**ORM**

**PITR**

**PostgreSQL**

**MySQL**

**MSSQL**

**SQL**

**MariaDB**

**CockroachDB**

**SQLLite**

**SQLAlchemy**

**TypeORM/Prisma**

**Kafka**

**Tosca**

**Jira**

**Xray**

**AWS**

**Microsoft Azzure**

**Thumbnail**

**NSFW klasifikátor**

**OIDC**

**AWS Cognito**

**Ory/Keycloak (self-host)**

**sociálne prihlásenia**

**Docker**

**GitHub**

**GitLab**

**Grafana**

**GDPR**

**AI Act**

**WCAG**

**EAA**

**izolácia tajomstiev (Secrets Manager/Vault)**

**TypeScript**

**Python**

**Java**

**JavaScript**

**Ruby**

**C**

**C++**

**C#**

**Asembler**

**Golang (Go)**

**MS Dos**

**Basic**

**Rust**

**Fortran**

**COBOL**

**Pascal**

**PHP**

**podpora ICU kolácií**

**YugabyteDB**

**MongoDB**

**DynamoDB**

**Neo4j**

**ClickHouse**

**Stemming**

**syntetické TPS grafy**

**anti-abuse**

**Bayesovou korekciou**

**Wilsonovo skóre**

**Shadow-ban**

**Decay**

**Idempotentnosť**

**Re-compute job po batchi zmien**

**DAU**

**Survivorship bias**

**Redis cache agregátov**

**Antimissuse**

**facetové štatistiky**

**dostupnostná heuristika**

**endpoint**

**E2E testy**

**OIDC (OpenID Connect)**

**managed IdP**

**Authorization Code Flow**

**PKCE (S256)**

**URI**

**Bearer access token**

**hash RT**

**passwordless**

**magic link**

**passkeys**

**Argon2id**

**bcrypt s costom**

**unikátne salting**

**minimá + haveibeenpwned kontrola reťazcov**

**MFA**

**TOTP**

**WebAuthn**

**RBAC**

**ABAC**

**Claimy do access tokenu**

**exponenciálny backoff**

**heuristika**

**WAF**

**IP allow/deny list pre admin endpoints**

**rotácia signing keys v IdP**

**PII**

**JWKS podpisu**

**MASVS/ASVS checklist**

**bruteforce scenáre**

**CSRF**

**SSRF/redirect hijack**

**Cognito**

**CDN**

**pre-podpísané URL**

**MIME**

**Pipeline**

**EXIF**

**HEIC**

**AVIF/WebP**

**JPEG**

**AV sken**

**ClamAV**

**managed AV**

**NSFW detektor**

**pHash**

**vendor lock-in**

**smart crop**

**DPA**

**GPS**

**SSIM/PSNR**

**ROI**

**item-to-item**

**Save-rate@K**

**CTR@K**

**Cook-proxy@K**

**Churn guardrails**

**Precision@K**

**Recall@K**

**nDCG@K**

**Coverage**

**Intra-List Diversity (ILD) a novelty**

**Latency P95**

**serendipity proxy**

**popularity-bias index**

**Temporal split**

**Golden set párov**

**Skóre cosine embeddings**

**TF-IDF/Jaccard**

**top-K**

**Cold-start item**

**Cold-start user**

**ILD**

**Popularity-penalty**

**Ablácie**

**IPS/DR**

**Team-Draft Interleaving**

**Save-rate@K**

**Guardrails**

**CUPED**

**p-hacking**

**Simpsonov paradox**

**Shilling útoky**

**trust score**

**SPAM/NSFW**

**Low-data mód**

**BlurHash/ThumbHash**

**Lazy loading**

**TTFR**

**error budget**

**Android Studio/ADB**

**Network Link Conditioner**

**Chrome DevTools Throttling**

**chatty API**

**Protobuf/MessagePack**