**Opis predmetu zákazky**

**Penetračné testovanie mobilnej aplikácie a webových služieb VšZP a.s. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Predmetom penetračného testovania mobilnej aplikácie a webových služieb VšZP a.s. je odhalenie ich zraniteľností voči kybernetickým útokom. VšZP a.s. požaduje penetračné testovanie najmä týchto aktív:

1. Mobilná aplikácia (iOS/Android)
2. Webový portál ePobočka
3. Služba eRecept
4. Elektronická prihláška
5. Retestovanie/čiastkové penetračné testovanie vybraných funkcionalít – max v rozsahu 175 človekohodín

Predmetom penetračného testovania Mobilnej aplikácie Všeobecnej zdravotnej poisťovne, a.s. je odhaliť jej zraniteľnosti na platformách Android/iOS a v komunikačných rozhraniach (službách) poskytovaných zodpovedajúcou serverovou infraštruktúrou. Výsledkom overenia bezpečnosti aplikácie bude komplexná správa o nájdených zraniteľnostiach, zhodnotenie ich závažnosti a spôsobu, ako zraniteľnosti zreprodukovať (simulovať) a odstrániť.

Penetračné testy by mali simulovať útok na mobilné zariadenie a aplikáciu z vonkajšieho prostredia v rozsahu dostupnom pre poistenca a jej verejne prístupných častí. Testy požadujeme podľa zavedenej metodológie OWASP Mobile Security zamerané na lokálne bežiacu aplikáciu, jej správanie sa v mobilnom operačnom systéme, komunikáciu so serverom ale aj zabezpečenie servera a jeho webových služieb (bezpečnosť implementácie API rozhraní). Požadujeme, aby súčasťou testovania boli aj externé testy lokálnej infraštruktúry, do ktorej je pripojený back-end server a sieťové zariadenia predradené back-end serveru.

Pokiaľ ide o spôsob vykonania testov, verejný obstarávateľ požaduje, aby testovanie bolo zrealizované metódou black box, pričom boli pokryté všetky kategórie testov z Mobile Top 10 2016 (<https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10>):

M1 - Improper Platform Usage

M2 - Insecure Data Storage

M3 - Insecure Communication

M4 - Insecure Authentication

M5 - Insufficient Cryptography

M6 - Insecure Authorization

M7 - Client Code Quality

M8 - Code Tampering

M9 - Reverse Engineering

M10 - Extraneous Functionality

# Predmetom penetračného testovania webovej aplikácie ePobočka, služby eRecept a Elektronickej prihlášky Všeobecnej zdravotnej poisťovne, a.s. je odhaliť ich zraniteľnosti v komunikačných rozhraniach (službách) poskytovaných zodpovedajúcou serverovou infraštruktúrou. Výsledkom overenia bezpečnosti webových aplikácií bude komplexná správa o nájdených zraniteľnostiach, zhodnotenie ich závažnosti a spôsobu, ako zraniteľnosti zreprodukovať (simulovať) a odstrániť.

# Penetračné testy by mali simulovať útok na webovú aplikáciu z vonkajšieho prostredia v rozsahu dostupnom pre poistenca a jej verejne prístupných častí. Testy požadujeme podľa zavedenej metodológie OWASP Top Ten zamerané bežiacu webovú aplikáciu, komunikáciu so serverom ale aj zabezpečenie servera a jeho súvisiacich webových služieb (bezpečnosť implementácie API rozhraní). Požadujeme, aby súčasťou testovania boli aj externé testy lokálnej infraštruktúry, do ktorej je pripojený back-end server a sieťové zariadenia predradené back-end serveru.

# Pokiaľ ide o spôsob vykonania testov, požadujeme, aby boli pokryté všetky kategórie testov z OWASP Top Ten (<https://owasp.org/www-project-top-ten/>):

1. Injection (SQL, NoSQL, OS, LDAP)

2. Broken Authentication

3. Sensitive Data Exposure

4. XML External Entities (XXE)

5. Broken Access Control

6. Security Misconfiguration

7. Cross-Site Scripting XSS

8. Insecure Deserialization

9. Using Components with Known Vulnerabilities

10. Insufficient Logging & Monitoring

Špecifikácia penetračného testovania:

* Lokalita, v ktorej bude testovanie prebiehať: cez VPN alebo z externého prostredia
* Používatelia mobilnej aplikácie: externí používatelia mimo prostredia VšZP (klienti aj neklienti VšZP)
* Spôsob testovania: realizované najmä z pohľadu klienta (alebo aj neklienta), a to z externého prostredia
* Zadanie testovania: na objednávku od zadávateľa, najneskôr 14 dní vopred

Ďalšie podmienky plnenia predmetu zákazky sú uvedené v návrhu zmluvy *(návrh zmluvy v prílohe č. 2).*

**Podmienky účasti uchádzačov:**

Uchádzač musí spĺňať podmienky účasti týkajúce sa osobného postavenia podľa § 32 ods. 1 písm. e) a f) zákona.

§ 32 ods. 1:

e) je oprávnený dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu – preukazuje sa dokladom o oprávnení dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu, ktorý zodpovedá predmetu zákazky

f) nemá uložený zákaz účasti vo verejnom obstarávaní potvrdený konečným rozhodnutím v Slovenskej republike alebo v štáte sídla, miesta podnikania alebo obvyklého pobytu - preukazuje sa čestným vyhlásením