BPR - Uloha 4: SQL injection

Ukoly

1. Prozkoumejte webovou aplikaci.
2. Zjistěte kde je aplikace zranitelná na útok typu SQL Injection. (1b)
3. Zjistěte jaké tabulky aplikace (celkem 3) existují v databázi (.5b), včetně uvedení postupu získání (.5b)
4. Zjistěte jaká data se v těchto tabulkách nacházejí (2b)
5. Zjistěte heslo administrátora webových stránek (1b)
6. Navrhněte konkrétní opatření, která povedou k nápravě všech nalezených chyb (3b).

Riesenia

Zdrojovy kod riesenia je v subore `injection.sh` a vystup jeho cinnosti je v `injection.out`

1. Webova aplikacia ma 2 formulare - prihlasenie uzivatela a "booking" girl. Tu sa oplati hladat zranitelnost. Svoj utok zacinam pokusom o vyvolanie chyby. Snazim sa vyvolat chybu *You have an error in your SQL syntax* `TODO: Zdrojak`
2. U prihlasovacieho formulara sa pri nespravnom vstupe zobrazi len biela stranka, zaujimavejsi je Booking dievciny. Ma sice input hidden, ale to utoku nijak nebrani. Po zadani apostrofu (') sa vyskytne chyba, zjavne sa cast za nim vykona ako SQL dotaz.
3. Najdene tabulky: `bpr.girls, bpr.news, bpr.users`. Postup je vo funkcii `get_tables` zdrojoveho kodu.
4. Data su viditelne v subore `injection.out`
5. Heslo administratora je zahashovane pomocou algoritmu `MD5`. Existuje niekolko webovych sluzieb na crackovanie tohto hesla, tak som si jednu skusil: MD5Decrypter.co.uk Vysledok ma potesil. Heslo admina je **KrAgQUT4**. `35b459f73f6e86818c989c4744de3848 = "KrAgQUT4"` `913c8c25da9eb8900ee68f01b7bbfaa5 = "KRAK FOREVER"` Trochu ma sklamalo, ze k VIP fotkam som sa nedostal :D
6. Rieseni je niekolko na roznych urovniach

a) Asi najznamejsie opatrenie je escapovanie uvodzoviek a inych skodlivych znakov v retazci vkladanom do SQL dotazu - realizuje sa pomocou budto `mysql_real_escape` alebo tzv. *prepared statements*
b) Dalsim opatrenim je definicia tvaru mena a hesla pomocou regularneho vyrazu a nasledna kontrola pri odoslani formulara.