Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 2, 842 16 Bratislava 4

Scenáre

Tímový projekt

Tím č. 19

Vypracoval: Nikola Karakaš
Vedúci projektu: Ing. Pavol Helebrandt Phd.

Úvodné privítanie

Vybrali ste si cestu stať sa kybernetickým expertom, ktorý nie vždy funguje na tejto strane zákona. Často hľadáte spôsob, ako ľahšie získať peniaze alebo iný materiálny úžitok. Momentálne prechádzate niekoľko zaujímavých webových stránok, na ktorých prebiehajú peňažné transakcie, a narazili ste na e-shop. E-shop ponúka príležitosti na nákup produktov online. Táto stránka má navyše databázu používateľov, a umožňuje tak novým používateľom vytvárať vlastné profily a prihlásiť sa k nim. Konfiguráciou profilu používateľ ušetrí veľa času pri ďalších nákupoch, pretože už nebude musieť uvádzať informácie o nákupe (adresa, spôsob platby). Okrem toho získa zľavy na niektoré z nasledujúcich nákupov. Užitočnou vecou na webe je tiež nákupný košík, ktorý trvale uchová produkty, ktoré si chcú používatelia objednať. Tiež ste si všimli, že web umožňuje používateľom, ktorí zabudli svoje heslo, resetovať si heslo zadaním e-mailu? Okrem týchto možností už priemerný používateľ nemá prístup k skrytému rozhraniu webu, napríklad k rozhraniam na správu používateľov a produktov. Skúste teda zistiť, ako získať informácie o účte s oprávneniami správcu.

Scenáre

Scenár I

Prvý scenár je na zahriatie. O to by sa pokúsila veľká väčšina - uhádnuť používateľské meno a heslo účtu s väčšími prístupovými právami. Neskúsený používateľ použije slabšie heslo a často sa stáva, že sa heslo a používateľské meno úplne zhodujú. Pohrajte sa trochu s rôznymi menami, ktoré by vložil neopatrný užívateľ, aby ste si ho ľahšie zapamätali. Pamätajte: cieľom je prístup k účtu, ktorý má väčšie prístupové práva ako bežný používateľ.

Scenár II

a) Podarilo sa vám získať účet s väčšími prístupovými právami. V ďalších krokoch Vás čaká niekoľko zaujímavých výziev. Všimli ste si, že v tomto účte web zobrazuje rozhrania, ktoré sú pre priemerného používateľa skryté. Jednou zo zaujímavých vecí je správa používateľov. V tejto výzve je vaším cieľom prístup a hacknutie používateľského účtu s oprávneniami správcu. Predpokladáte, že eshop používa nejakú SQL databázu, v ktorej sú

umiestnené všetky užívateľské účty. Popremýšľajte, ako preniknúť do databázy SQL a pokúsiť sa nájsť ten správny účet.

b) Po nájdení správneho účtu chcete mať nad ním úplnú kontrolu. Jedným zo spôsobov je zmena prihlasovacích údajov.

Scenár III

Už sa vám podarilo dostať do účtu administrátorov a zmeniť jeho prihlasovacie údaje. Máte možnosť robiť si, čo chcete. Stále však chcete produkt zdarma. Pre túto výzvu nebudete až tak potrebovať účet správcu, ale bude vám prínosom vedieť, ako pracovať s nástrojom na testovanie penetrácie webových aplikácií.

Jedným z týchto programov je BurpSuite. Je to najpopulárnejší nástroj medzi profesionálnymi výskumníkmi bezpečnosti webových aplikácií a lovcami chýb. Vďaka ľahkému použitiu je vhodnejšou voľbou medzi bezplatnými alternatívami, ako je OWASP ZAP. Burp Suite je k dispozícii ako komunitné vydanie, ktoré je zadarmo, ale existuje aj platená verzia s ďalšími funkciami. Bezplatná verzia aplikácie BurpSuite obsahuje zachytávajúci server proxy, ktorý umožňuje používateľovi vidieť a upravovať obsah požiadaviek a odpovedí počas prepravy. Umožňuje tiež používateľovi poslať požiadavku / odpoveď pod monitorovaním na iný relevantný nástroj v BurpSuite, čím sa odstráni bremeno kopírovania a vkladania.

Proxy server je možné nastaviť tak, aby fungoval na konkrétnom IP a porte so spätnou väzbou. Proxy je možné nakonfigurovať aj na filtrovanie konkrétnych typov párov požiadavka-odpoveď. To je presne cieľ tejto výzvy. Skúste podať žiadosť o kúpu nového produktu a potom túto požiadavku zachytite a upravte. Cieľom je dostať správu, že produkt bol úspešne objednaný bez toho, aby ste zaň zaplatili.