Tim 7

Penetraciono testiranje

Uvod

Penetraciono testiranje (eng. Penetration Testing) je proces simuliranja napada na sistem ili aplikaciju kako bi se identifikovale potencijalne sigurnosne ranjivosti. Cilj penetracionog testiranja je da se pruži uvid u stepen sigurnosti sistema ili aplikacije i da se identifikuju bilo kakve ranjivosti koje bi mogle biti iskorišćene od strane napadača.
Ovo testiranje obično obuhvata ispitivanje mreže, aplikacija, baza podataka, sistema i drugih informacionih tehnologija korišćenjem raznih tehnika i alata, uključujući automatizovana skeniranja, ručne testove i druge tehnike. Rezultati penetracionog testiranja se koriste za identifikovanje i ispravljanje ranjivosti i jačanje sigurnosti sistema ili aplikacije.
Penetraciono testiranje je važan deo procesa upravljanja sigurnošću informacija i pomaže korisnicima da identifikuju potencijalne probleme i ranjivosti, kako bi ih ispravili prije nego što budu iskorišćeni od strane napadača. To takođe omogućava korisnicima da razumeju kakvi su napadi mogući i kako se zaštititi od istih.

Implementacija

U procesu testiranja bio je korišćenje OWASP ZAP alata, koji je besplatni i otvorenog koda. Ovaj alat pruža širok spektar funkcionalnosti, uključujući aktivno i pasivno skeniranje aplikacije, praćenje sesije, automatsko i manuelno menjanje zahteva poslatih ka cilju da bi se identifikovale specifične ranjivosti sistema.
Pasivno skeniranje se sprovodi manuelnim istraživanjem aplikacije ili spideringom (crawling sajta sa ciljem prikupljanja informacija o strukturi i sadržaju stranica koje čine aplikaciju). Ovaj proces ne uključuje izmenu podataka, već samo praćenje zahteva i odgovora između sistema, sa ciljem identifikacije potencijalnih ranjivosti.
Nasuprot tome, aktivno skeniranje se vrši napadanjem sistema, tj. menjanjem zahteva poslatih ka cilju sa ciljem da se eksploatišu ranjivosti. Tokom ovog procesa, ranjivosti se detektuju i prikazuju kroz alerts tab, a njihov stepen rizika može biti visok, srednji, nizak ili samo informativan.

Testiranje je počelo manualnim ispitivanjem svih stranica i funkcionalnosti aplikacije. Zatim je obavljeno automatsko skeniranje stranica pomoću AJAX spider-a kako bi se prikupile potpune informacije i pronašli eventualno propušteni delovi. U procesu pasivnog skeniranja, utvrđeno je da postoje aplikacije koje slušaju na portovima 4201 i 8090 i koje su nastavljene sa aktivnim testiranjem. U ovom koraku, automatski generisani zahtevi su poslati da bi se otkrili različiti potencijalni problemi. Nakon automatskog aktivnog skeniranja, urađen je i test "forced browsing". Cilj mu je bio da pokuša pristupiti fajlovima i/ili direktorijumima iz predefinisane liste, kako bi se eventualno pronašle ranjivosti sistema. Međutim, sistem nije podlegao ovom testu.

Tim 7

Kristina Stojić

Đorđe Krsmanović

Rastislav Kukučka

Sanja Drinić