Sigurnost i kontrola podataka – par saveta

Za razliku od statičnih veb sajtova, koji samo prezentuju svoj sadržaj, dinamičke veb aplikacije imaju interakciju sa korisnikom, te se vrši obrada ulaznih podataka. Međutim, veb programer se ne sme osloniti na to da će se korisnik ponošati na očekivan način – na primer, korisnik u polje koje je potrebno popuniti brojnom vrednošću može uneti tekst, što bi aplikaciju, potencijalno dovelo do greške. Ovakav problem može biti rezultat slučajne greške korisnika, ali isto tako može biti izazvan radi zloupotrebe veb aplikacije i podataka kojima ona raspolaže. Iz ovih razloga, neophodno da je da se unapred predvide mogući problemi, i da se odmah reše.

1. Sigurnosti propust koji se najčešće može sresti kod veb aplikacija jeste mogućnost „ubrizgavanja“ SQL inekcija. Pod ovim pojmom se podrazumeva prosleđivanje teksta sajtu takvog da on prouzrokuje izvršavanje SQL upita koji korisnik odabere.

Na primer, aplikacija može koristiti prosleđen podatak na sledeći način:
```
SELECT * FROM `table` WHERE `user` = 'test'
```
Ovaj upit je ispravan.

Međutim, ako korisnik umesto test unese test'; DELETE * FROM 'table' WHERE "=', dobiće se sledeći upit usled kog će biti izbrisani svi podaci u tabeli:
```
SELECT * FROM 'table' WHERE 'user' = 'test'; DELETE * FROM 'table' WHERE ''=''
```

Da do ovoga ne bi došlo, svi podaci se pre ubacivanja u upit „tretiraju“ sa dve funkcije – mysql_real_escape_string za tekstualne podatke i intval za celobrojne podatke.
Nakon njihove upotrebe, podaci se mogu proslediti MySQL serveru.

2. Osim prosleđivanja SQL upita, korisnik takođe može da prosledi i JavaScript kod ili neki drugi tekst koji narušava HTML strukturu veb stranica. Ovo se rešava uz pomoć funkcije htmlspecialchars koja karaktere koji su potencijalna pretnja pretvara u njihove HTML ekvivalente, čineći ih bezopasnima.

3. Čak i pored ovih mera bezbednosti, može se dogoditi da zlonamerni korisnik uz pomoć sigurnosnih propusta samog veb servera dođe u posed sadržaja baze podataka. Zbog ove mogućnosti, praksa je da se lozinke registrovanih korisnika ne čuvaju u svom originalnom obliku, već da budu enkriptovane. Na taj način se iz enkriptovanog teksta ne može dobiti lozinka, a provera lozinke pri prijavljivanju se lako proverava enkripcijom unetog teksta.

4. Najzad, veb aplikacija mora onemogućiti pristup tzv. botovima, odnosno skriptama koje su napisane da se ponašaju kao živi korisnik, uglavnom radi zloupotrebe veb aplikacije za reklamiranje. Jedan od načina da se ovaj problem reši jeste da se od korisnika pri registraciji traži adresa elektronske pošte na koju se šalje aktivacioni link. Ove skripte jako retko imaju mogućnost da proveravaju elektronsku poštu, pa se tako eliminiše veliki broj botova.