Poboljsanje sigurnosti web aplikacije phpBB
Vrsta: Seminarski Broj strana: 7 | Nivo: Viša elektrotehnička škola |

Abstrakt
phpBB forum je u skoroj verziji 2.0.21 ispravio mnoge primećene sigurnosne propuste koje su bile često zloupotrebljavane, zahvaljujući rasprostranjenosti aplikacije. Aspekt koji nije u dovoljnoj meri pokriven do sada jeste prenos i čuvanje šifri registrovanih korisnika. Trenutno rešenje za smeštanje šifri u bazu, umesto originalnog sadržaja, primenjuje na njega hash algoritam md5, ali se na tome priča i završava. U transportu od klijenta do servera šifra putuje u čistom obliku podložna pasivnim napadima, što je neprihvatljiva situacija. Možda sama pomenuta aplikacija nema toliko važnu ulogu da bi briga oko zaštite identiteta imala veliki prioritet, ali sama činjenica da korisnici Internet usluga često za šifre raznih sistema koriste iste/slične podatke, nameće obavezu svakom davaocu usluga da te podatke i zaštiti, kako u transportu, tako i pri čuvanju na serveru.
Cilj
Ovaj seminarski rad se bavi mogućim rešenjem sigurnosnih nedostataka phpBB aplikacije kroz kombinovanu primenu enkripcije, hmac i hash algoritama. Problem je razložen na nezavisne celine i svakoj je ponuđen prigodan metod zaštite u kontekstu ove aplikacije. Uočene celine su: registracija, logovanje, promena šifre, izgubljena šifra i automatsko logovanje.
Zadaci
Prilikom razmatranja pojedinih celina i njihovih predloženih sigurnosnih unapređenja, treba voditi računa o nekoliko činjenica vezanih za sam phpBB.
Organizacija koda aplikacije je takva da se pravljenje dodataka, odnosno MODova (od Modifications), svodi na pravljenje fajla koji opisuje izmene u kodu, odnosno search and add or replace informacije. Ovakva organizacija otežava kompleksnije izmene, tako da je poželjno promene koda pojednostaviti i sam njihov broj maksimalno smanjiti. Rezultat ovog seminarskog bi trebao da bude jedan takav MOD koji bi se mogao primeniti na bilo kojoj instalaciji phpBB foruma.
Kao što je već pomenuto, trenutno se šifra korisnika u bazi na serveru čuva kao md5 hash. Ovo je moguće unaprediti, ali za sada se ostaje na tome, jer bi promena podataka ovog tipa uticala na upotrebljivost MODa, kao i na kompatibilnost sa drugima. Moguće unapređenje bi bila upotreba hmac algoritma sa vrednošću ključa jedinstvenim za svakog korisnika, kao i za konkretnu instalaciju aplikacije takođe. Ovo bi onemogućilo portabilnost hash-a šifre između različitih sistema, što predstavlja moguće mesto zloupotrebe.
Aplikacija omogućuje vizuelnu konfirmaciju prilikom registracije što pruža kanal za siguran prenos podataka od servera ka klijentu.
Registracija
Prilikom registracije se šifra korisnika prvi put pominje i mora se preneti do servera radi uskladištavanja. Trenutno se ona prenosi u originalnom obliku, što je neprihvatljivo. Viši nivo sigurnosti bi bio slanje hash-a, ali i sam hash je potrebno sačuvati od pasivnog napada, jer se i on može zloupotrebiti, bez znanja o samoj šifri koju predstavlja.
Za siguran prenos podataka do servera je potrebno koristiti enkripciju, što omogućava pomenuta vizuelna konfirmacija, koja bi se mogla koristiti i kao metod razmene ključa.
Rešenje je da se postojeći kod za vizuelnu konfirmaciju iskoristi kao ključ za enkripciju šifre (korišćeni algoritam za enkripciju je Blowfish). Polja forme za šifru i potvrdu šifre se zamenjuju enkriptovanim vrednostima md5 hash-a samih šifri upotrebom JavaScript-a prethodno slanju. Pomeranjem primene hash funkcije sa servera na klijenta, šifra se u potpunosti sakriva i od servera, odnosno osoba sa pristupom istom.