

*PREDMET: IT255 VEB SISTEMI I*

**ZADAĆA BR. 15**

Ime i prezime: **Igor Barašin**

Broj indeksa:  **2681**

# Cilj domaćeg zadatka:

Za domaći zadatak 15 potrebno je da pronađete sve moguće potencijalne propuste u Vašem kodu i kako su oni rešeni kod Vas u projektu.

# Rješenje domaćeg zadatka:

* SQL Injection:

SQL injekcija je tehnika unosa koda u veb sistem. Izrazi se ubacuju u polja za unos podataka (npr. username/password) da bi se dobili zaštićeni podaci iz baze podataka.

Program sam testirao protiv SQL Injection-a i nisam pronašao propuste.

* Remote File Inclusion:

Remote File Inclusion je propust koji omogućava napadaču da učita (JavaScript ili PHP) skriptu sa drugog servera. Napadač najčešće napravi ‘.txt’ fajl sa sadržajem PHP skripte i njega pokuša da učita kao PHP izvršnu skriptu. Ako programer nije filtirirao šta ulazi kroz POST i GET metode u *include* funkciju, napadač može da ubaci svoju ili neku gotovu shell skriptu i pristupi svim podacima na serveru.

Program je siguran protiv RFI jer ne sadrži učitavanje stranica preko POST i GET metoda.

* Denial of Service (DoS) i Distributed Denial of Service (DDos):

Napad uskraćivanja servisa (engl. Denial of Service) je napad kojim napadač privremeno onemogućuje svim klijentima pristup serveru koji napada. Distribuirani napad uskraćivanja servisa (engl. Distributed Denial of Service) je distribuirani napad, što znači da više računara u isto vreme napadaju web server i onemogućuju pristup istom. Ovi propusti se najčešće pojavljuju kod modula za Apache.

Protiv ovog napada servis je zaštićen jer je XAMPP, a samim tim i Apache server, ažuriran na najnoviju verziju.

* Cross-site scripting (XSS)

Propust izvršavanja skripte preko dve strane (engl. Cross-Side Scripting) ili XSS, je propust koji omogućava napadaču da izvrši injekciju koda (engl. Code Injection) na serverskoj strani. Ovaj propust se najčešće koristi za krađu sesija, kolačića, kao i svih informacija koje web čitač čuva o korisniku i sajtu. Napadač može poslati adresu u koju je uključena skripta koja će pokupiti kolačiće ili sesiju od korisnika, i zatim može te podatke da iskoristi kako bi se predstavio kao taj korisnik na sajtu.

Protiv ovog napada servis je zaštićen jer je XAMPP, a samim tim i Apache server, ažuriran na najnoviju verziju.