Laboratorijske vježbe iz kolegija **“Dinamičke web aplikacije”** 2015/2016
Stručni studij računarstva
Tehničko veleučilište u Zagrebu

Priprema za 6. laboratorijsku vježbu

Zadatak

Potrebno je
1. popraviti sigurnosne greške na svim PHP stranicama koje ste do sada radili (login stranica, stranica s ispisom svih proizvoda, stranica za unos tih proizvoda, stranica s životopisom).

Kao baza za popravak pogledati Xtreme Vulnerable Web Application (https://github.com/s4n7h0/xvwa). Preporuka je instalirati na lokalno računalo, no moguće je neke napade testirati i online (http://xvwa.samsclass.info/xvwa/).

Napomene:

1. Pogledati source kod svake od stranica koju napadate u XVWA. Lako ćete uočiti uzorke programskog koda koji nije dobar.

2. Naročito obratiti pozornost na SQL injection i XSS. Preporuka je popraviti i druge moguće probleme na stranicama.

Stranicu možete testirati učitavanjem u bilo koji browser. Preporuka je testirati sa Firefox i Chrome pretraživačima.

Stranica treba biti spremljena u poddirektoriju *lab6.* Slobodno koristiti programski kod i dizajn s prijašnjih vježbi (u osnovi ga i popravljate).

Literatura: dani link, prezentacija sa predavanja, svi drugi materijali na Internetu.