Attacks and defenses on web applications lab

# Priprema

### Alati

1. Svako od studenata bi trebalo da instalira i ispita OWASP Juice Shop alat (<https://www.owasp.org/index.php/OWASP_Juice_Shop_Project>).
2. Možete pogledati i dodatne alate:
   1. Burp Suite (<https://portswigger.net/burp>)
   2. Cyber Chef (<https://cyberchef.org/>)
   3. Dirsearch (<https://github.com/maurosoria/dirsearch>)

# Uvod

Ranjivi softverski paketi poput OWASP Juice Shop predstavljaju aplikacije koje sadrže ranjivosti i omogućavaju izvođenje napada radi rešavanja bezbednosnih izazova. Nakon što se poradi na razumevanju konkretnog napada, te se napad uspešno izvede, ispituje se perspektiva branioca. Diskutuju se ranjivosti i kontramere koje bi onemogućile da takav napad uspe.

Zrelost ranjivih softverskih paketa varira, od osnovnih primera koji demonstriraju par napada i ranjivosti, do sofisticiranih sistema koji obiluju različitim zadacima za učenje. Takođe, razlikuju se bezbednosni koncepti koji su pokriveni, kao i tehnologija kojom su napravljeni. Od mogućih opcija, odabrali smo OWASP Juice Shop Project iz sledećih razloga:

* To je zreo alat za učenje, i predstavlja značajni doprinos u oblasti bezbednosti aplikacija
* Ima bogat sadržaj, i pokriva širok spektar napada i odbrana. Trenutna verzija (16.0) sadrži preko sto izazova.
* Jednostavan je za korišćenje, pruža detaljnu dokumentaciju, prezentaciju i video materijale koji pomažu u korišćenju. Zatim, postoje i najrazličitija uputstva za rešavanje svakog od izazova.
* Kreiran je modernim i poznatim tehnologijama
* U pitanju je potpuno funkcionalan web shop sa standardnim funkcionalnostima

# Zadaci

Za OWASP Juice Shop postoji i prateći vodič ([online verzija](https://pwning.owasp-juice.shop/companion-guide/latest/), [besplatna knjiga](https://leanpub.com/juice-shop)) koji analizira izazove, dajući smernice i rešenja. Prilikom odabira prikladnog podskupa izazova, trebalo bi imati na umu:

* Koliko je student familijaran sa konkretnom klasom napada i odbrana, gde je cilj da se izbegnu izazovi koji su previše laki ili teški
* Težina izazova varira od 1 do 6. Za rešavanje izazova težine 6 može biti potrebno sat-dva, dok za jednostavnije jednostavnijih treba manje od sat vremena.
* Trebalo bi imati na umu i važnost izazova u odnosu na realni svet

## Analiza odbrane

Kako OWASP Juice Shop nudi platformu za izvođenje napada, ali ne govori mnogo o potencijalnim zaštitama, studenti moraju zabeležiti i prodiskutovati sledeće za svaku klasu napada:

* Objasniti klasu napada;
* Koji uticaj iskorištenje (*exploit*) određene klase ranjivosti može imati;
* Koje ranjivosti u softveru su dozvolile da napad uspe;
* Koje su primerene kontramere (što više detalja, to bolje) kako bi se sprečio napad.

Tri izazova su obavezna za svaki tim (izazove pregledajte na [localhost:3000/#/score-board](http://localhost:3000/#/score-board)):

* Saznati adminovu lozinku (pošto se nije potrudio da bude teška za otkriti:)
* Zaobići CAPTCHA zaštitu protiv automatizovanog davanja review-a
* Otkriti i skinuti easter egg

Svaki student u timu neka odabere 5 dodatnih izazova iz različitih klasa po svojoj volji.