ATTACKS AND DEFENSES ON WEB APPLICATIONS LAB

1. PRIPREMA

ALATI I PLATFORME

1. Svako od studenata bi trebalo da kreira nalog na PS Akademiji (https://portswigger.net/users/register).
2. Možete pogledati i dodatne alate (BurpSuite je obavezan):
    a. Burp Suite (https://portswigger.net/burp)
    b. Cyber Chef (https://cyberchef.org/)

• UVOD

Ranjive aplikacije i edukativni alati, poput onih koje nudi **PortSwigger Web Security Academy**, predstavljaju simulirana okruženja dizajnirana za vežbanje i razumevanje napada na veb aplikacije. 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. Edukativne platforme se razlikuju po pristupu, težini zadataka, stepenu realističnosti i tehničkoj dubini. Ove godine, odlučili smo se za **PortSwigger Web Security Academy** iz sledećih razloga:

- **Zvanična je edukativna platforma kreatora Burp Suite-a**, najkorišćenijeg alata za testiranje bezbednosti veb aplikacija.
- **Sadrži veliki broj tematski organizovanih laboratorija**, od osnovnih do naprednih, koje pokrivaju širok spektar napada: od XSS i SQL injection-a, preko CSRF-a i IDOR-a, do SSRF-a i napada na mehanizme autentifikacije.
- **Laboratorije su realistične i fokusirane** - svaka simulira konkretan scenario i omogućava izvođenje ciljanog napada, uz automatsku verifikaciju uspeha.
- **Pružena su teorijska objašnjenja i demonstracije** - svaka tema uključuje detaljno tekstualno objašnjenje koncepta, ilustracije i često i video snimke.
- **Pristup platformi je potpuno besplatan**, a zadaci se izvršavaju direktno iz browsera, bez potrebe za lokalnim hostovanjem aplikacije.

• ZADACI

Za sve zadatke sa ove platforme postoji i vodič za rešavanje (tzv. *writeup*) u sekciji *solutions*, dajući smernice i rešenja. Prilikom odabira prikladnog podskupa zadataka, 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 teški

- Težina izazova varira od 1 do 3 (zeleni, plavi, i ljubičasti). Za rešavanje izazova težine 3 može biti potrebno dan-dva za čoveka koji zna šta radi, dok za jednostavnije (zelene i plave) treba manje od sat vremena čak i početniku.
- Trebalo bi imati na umu i važnost izazova u odnosu na realni svet

Analiza odbrane

Kako PS akademija pored platforme za izvođenje napada govori i 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.

Po 2 klase izazova su obavezna za svakog studenta u timu (klase pregledajte na https://portswigger.net/web-security/all-topics, jedna mora biti iz server-side a druga iz client-side sekcije, advanced topics zaboravite za sada):

- Za svaku klasu napada napisati sve gore navedeno
- Za svaku klasu uraditi bar 5 zadataka (2 zelena i 3 plava, ako data klasa nema 5, uradite nešto dodatno i za tu ekstra klasu ne morate pisati ovo iznad, ukupno morate imati 10 zadataka, 4 zelena, 6 plavih)
- Za svaki zadatak napisati writeup kako je rešen sa sve screenshot-ovima bitnih koraka
- Ko položi BSCP sertifikat ima automatski sve bodove za ovaj zadatak 🙂