Izvještaj - SOSA LAB2 (Ivan Futivić 0036522493)

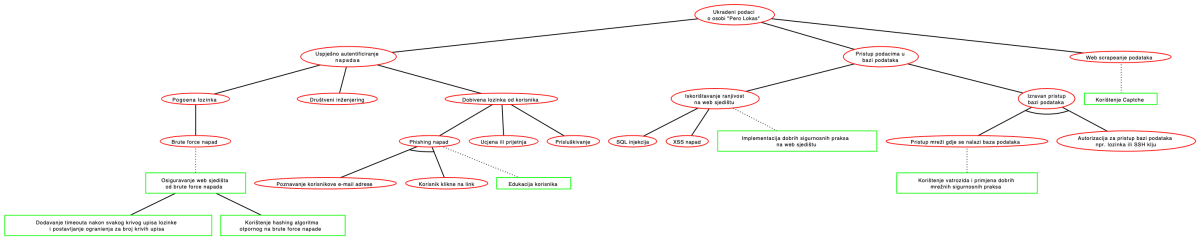
Odabir alata za crtanje

Kao alat za crtanje odabrao sam ADTool. Tijekom izbora uzeo sam u obzir sve alate navedene na prezentaciji o stablima napada. ENT i SeaMonster nisam uspio pokrenuti, dok Deciduous je gradio stabla obrnutim redoslijedom nego je sugerirano za ovu vježbu (odozgo prema dolje). AT-AT sam uspio pokrenuti, ali ubrzo sam shvatio da nema dobru podršku za veće količine teksta u čvorovima, tj. tekst je izlazio izvan granica čvorova. Jedini preostali izbor bio je ADTool kojeg nisam uspio pokrenuti na svojem laptopu (vjerojatno zbog ARM arhitekture procesora), ali ga jesam uspio pokrenuti unutar x86 virtualnog stroja.

Korištenje različitih oblika čvorova

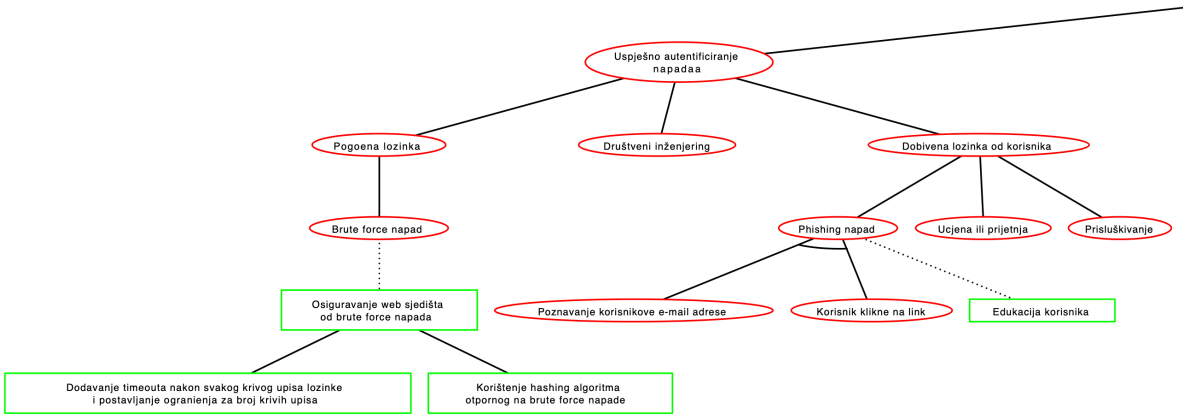
ADTool podržava dodavanja "protumjera" (eng. countermeasures) za bilo koji čvor u stablu napada. Ti čvorovi su u obliku pravokutnika, zelene su boje i povezani su sa "normalnim" čvorovima pomoću isprekidanih crta. ADTool također podržava "I" čvorove koji su označeni s lukovima između čvorova djece.

Stablo



Zbog problema sa ADToolom, nedostaju slova č, ć i đ

Grana 1 - Uspješno autentificiranje napadača



Ova grana sadrži sve načine kako napadač može pristupiti osobnim podacima korisnika, a da je za to prvo morao na neki način doći do korisnikove lozinke i korisničkog imena.

Pogođena lozinka:
Napadač ovim putem pokušava doći do lozinke bez da je na neki način sazna direktno od korisnika.

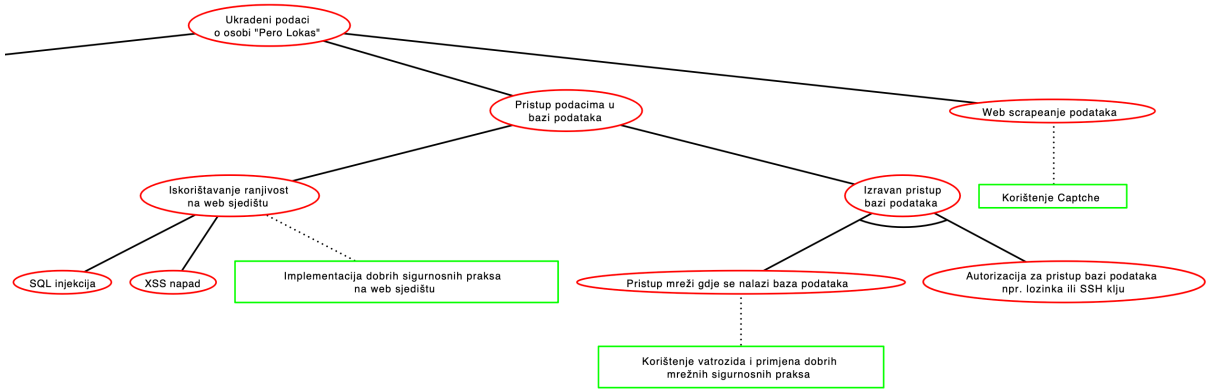
1) Brute force napad
   a) Kao protumjeru vlasnik web sjedišta može implementirati neke popularne zaštite od takvih napada. Može dodati timeout nakon određenog broja neuspješnih unosa lozinke te također može zablokirati pristup korisniku ako se i dalje događaju neuspješne prijave.
   b) U slučaju da podaci u bazi podataka postanu javni, moguć je offline brute force napad. Za zaštitu od takvog napada potrebno je koristiti prikladan hashing algoritam koji onemogućuje prebrzo generiranje hasheva.

Društveni inženjering:
Napadač može uvjeriti vlasnika web sjedišta kako je on zapravo taj korisnik i time dobiti pristup računu (npr. napadač uvjeri vlasnika web sjedišta da resetira lozinku za njega)

Dobivena lozinka od korisnika:
Napadač može fizički ili preko računala dobiti lozinku od samoga korisnika.

1) Phishing napad
   a) Napadač može korisniku poslati maliciozni link pomoću kojeg će on dobiti pristup njegovom računu. Ovaj pristup zahtjeva da napadač zna korisnikovu mail adresu te da korisnik istovremeno klikne na maliciozan link.
   b) Kao zaštitu od ovakvog napada potrebno je korisnika educirati o phishing napadima kako bi ih znao prepoznati i izbjeći
2) Ucjena ili prijetnja
3) Prisluškivanje
   a) Napadač može prisluškivati korisnika u nadi da spomene svoju lozinku

Grana 2 - Pristup podacima izravno iz baze podataka



Ova grana sadrži načine kako napadač može pristupiti korisnikovim osjetljivim podacima, bez autentificiranje, koristeći izravan pristup bazi podataka.

Iskorištavanje ranjivosti na web sjedištu:
Napadač može dobiti uvid u sadržaj baze podataka pomoću raznih ranjivosti na web sjedištu.

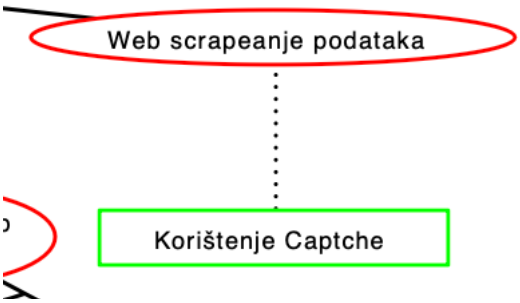
Kao protumjeru možemo implementirati razne sigurnosne prakse koje će smanjiti vjerojatnost pojave ranjivosti na web sjedištu.

1) SQL injekcija
   a) Napadač može koristiti SQL injekcije kako bi radio proizvoljne upite na bazu i dobio pristup podacima
2) XSS napad
   a) Napadač može poslati maliciozan kod prema web sjedištu kako bi dobio pristup podacima iz baze.

Izravan pristup bazi podataka
Umjesto da napadač dobi podatke iz baze pomoću web sjedišta, on može njima direktno pristupiti.
Kao protumjeru možemo koristiti enkripciju podataka.

1) Napadač mora za pristup bazi podataka prvo imati pristup mreži gdje se nalazi baza. Također mora imati potrebnu autorizaciju za pristup.
2) Kao protumjeru možemo postaviti vatrozid koji će štititi mrežu od nedozvoljenog pristupa te možemo za autorizaciju koristiti neku sigurnu lozinku ili još bolje, SSH ključeve.

Grana 3 - Web scrapeanje podataka



Napadač može dobiti neke javno dostupne podatke (korisničko ime, ime, prezime, mjesto rođenja) pomoću web scrapinga. Ova grana rezultira manjom količinom osobnih podataka jer nećemo dobiti neke osjetljive podatke za koje je potrebno autentificirati korisnika (oib, mjesto rođenja, godina rođenja, jmbg, adresa prebivališta).

Kao zaštitu od ovakvog napada možemo implementirati Captchu na web sjedištu kako bi otežali proces web scrapinga.