



*Jesenji semestar, 2022/23*

*PREDMET: IT381 - Zaštita i bezbednost informacija*

**Domaći Zadatak br. 6**

Student: **Aleksa Cekić 4173**

Profesor: **dr Milena Bogdanović**

Asistent: **mr Goran Stamenović**

Datum izrade: **17.03.2023**

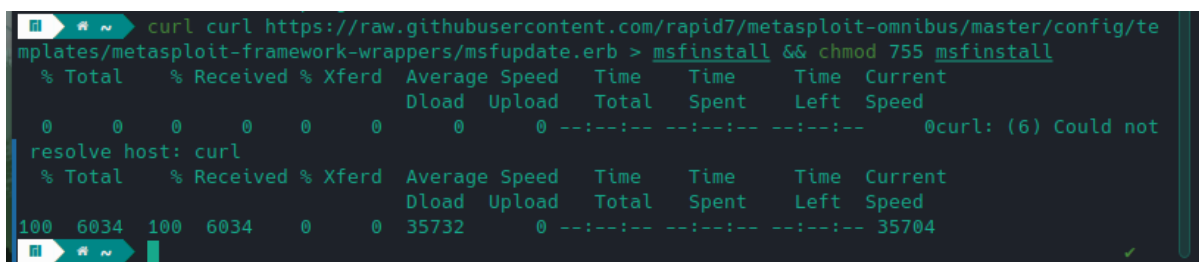
## Tekst Zadataka

Instalirati Metasploit framework na Linux distribuciji i poslati prikaze ekrana. Izabrati jedan od OWASP Top 10 najkritičnijih rizika web aplikacija objasniti ovaj rizik i po mogućnosti prikazati ga primeru koristeći Metasploit framework:

- Injection
- Cross-site scripting (XSS)
- Broken Authentication and Session management
- Insecure Direct object references
- Cross Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

## Rešenje zadataka

Za prikaz ovog domaćeg zadatka koristio sam O.S. Manjaro Linux.



```
curl -s https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall -i && chmod 755 msfinstall
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
  0     0    0     0    0     0      0      0  --:--:-- --:--:-- --:--:--    0curl: (6) Could not
resolve host: curl
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 6034 100 6034    0     0 35732    0  --:--:-- --:--:-- --:--:-- 35704
msfinstall
msfinstall is a shell script that will install Metasploit framework.
```

Od top 10 najkritičnijih rizika web sajtova ja sam izabrao Injection odnosno SQL injection i sada ću da ga opišem.

SQL injection je ubacivanje koda koja između ostalog može da obriše našu bazu podataka. Ovo je jedna od najčešćih tehnika web hakovanja nekog sajta.

Ovo se uglavnom dešava kada tražimo da user unese neke podatke kao npr. Username a umesto toga user unese pametan upit koji će se pokrenuti u našoj bazi podataka.

Ukoliko nema načina da se pametan upit reguliše pre kontakta sa bazom posledice mogu biti ogromne. Primer pametnog upita je npr. UserId : 121 OR 1=1 odnosno u polje koje je zahtevalo da unesemo neki naš ID a umesto toga unesemo SQL injection koji je baziran na principu 1=1 i ovo je uvek tačno a samim tim će se i upit realizovati. U bazi će ovaj naš input izgledati otprilike ovako SELECT \* FROM Users

WHERE UserId = 121 OR 1=1; budući da je ovaj upit tačan uvek tj OR 1=1 je uvek tačno a samim tim i upit. Ovaj upit vraća sve podatke koji su vezani za usera koji ima id 121. Ovo se takođe može koristiti da se dobiju podaci i za celu tabelu ili da se tabela Dropuje iz baze. Iz ovog razloga treba koristiti SQL Parametre zbog zaštite kako bi se svaki input koji unese korisnik tretirao baš samo kao input a ne kao potencijalni SQL upit.