A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 6***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 44******42***

**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:

1. Injection
2. Cross-site scripting (XSS)
3. Broken Authentication and Session managment
4. Insecure Direct object references
5. Cross Site Request Forgery (CSRF)
6. Security Missconfiguration
7. Insecure Cryptographic Storage
8. Failure to Restrict URL Access
9. Insufficient Transport Layer Protection
10. Unvalidated Redirects and Forwards

**Rešenje zadataka**

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

A screen shot of a computer program

Description automatically generated

Od top 10 najkritičnijih rizika web sajtova ja sam izabrala Injection odnosno SQL injection i sada sledi opis svega toga.

SQL injection je ubacivanje koda koja između ostalog može da obriše našu bazu podataka. Ovo je jedna on 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 User

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.