VAJA: SQL ranljivosti

Namen

Namen te vaje je raziskati in razumeti, kako napadalci izkoriščajo ranljivosti v aplikacijah za izvajanje neavtoriziranih SQL ukazov. Skozi praktično delo bodo udeleženci spoznali različne metode in tehnike SQL Injection napadov ter se naučili, kako zaznati in preprečiti takšne ranljivosti v svojih aplikacijah.

Uvod

Sodobne spletne aplikacije pogosto uporabljajo relacijske baze podatkov za shranjevanje in obdelavo podatkov. Komunikacija med aplikacijo in bazo podatkov se izvaja z uporabo SQL (Structured Query Language), standardnega jezika za upravljanje in dostop do podatkov v bazi. SQL Injection je vrsta varnostnega napada, pri katerem napadalec vstavi ali "vrine" zlonamerne SQL ukaze v vhodih, ki so namenjeni za obdelavo s strani aplikacije. Če aplikacija neposredno posreduje te vhode v SQL poizvedbe brez ustrezne sanacije ali preverjanja, lahko napadalec izvrši arbitrarno SQL kodo, kar mu omogoča manipulacijo z bazo podatkov, dostop do občutljivih informacij, izbris podatkov ali celo prevzem nadzora nad celotno bazo. Namen te vaje je torej ne samo spoznati, kako takšni napadi delujejo, ampak tudi kako jih prepoznati in se pred njimi učinkovito zaščititi.

Naloge:

1. Spoznavanje osnov SQL sintakse

Razumevanje osnovnih SQL poizvedb, kot so »SELECT«, »UPDATE«, »DELETE« in kako te lahko izkoristimo za pridobivanje, spreminjanje ali brisanje podatkov v bazi.

```
SELECT * FROM users WHERE name= '$username' AND password = '$password'
```

2. Razumevanje mehanizma vrivanja SQL stavkov (SQL Injection)

Spoznajmo, kako lahko nezadostna sanacijo vhodnih podatkov vodi do SQL injection ranljivosti. Primerjajmo varne in nevarne načine obdelave uporabniških vhodov.

3. Praktični primeri vrivanja SQL

Oglejmo si primer z uporabniškim imenom in geslom. Kako lahko napadalec izkorišča pomanjkljivo preverjanje vhodnih podatkov?

```
SELECT * FROM users WHERE name= 'admin' AND password = 'krneki' OR 1 == 1
```

Analizirajmo, zakaj je vrinjeni stavek "OR 1 = 1" tako učinkovit pri obhajanju avtentikacijskih mehanizmov.

4. Praktična vaja: Spletna stran

Obiščimo spletno stran: https://cybersec.ltfe.org/sql . Raziskujmo izvorno kodo spletne strani in identificirajmo možne točke za SQL injection.

Izvedimo SQL injection napad. Kateri SQL stavek smo vrinili za uspešno prijavo? Zakaj je deloval?

Odprimo še spletno stran: https://cybersec.ltfe.org/sqlcar .

S pomočjo SQL injection tehnike pobrišimo bazo (tabelo). Komentirajte dogajanje.

5. Vajo nadaljujte z bolj naprednim napadom z orodjem SQLMAP:

https://cybersec.ltfe.org/vaje/sqlmap.pdf