Scenáre pre SQL Injekcie

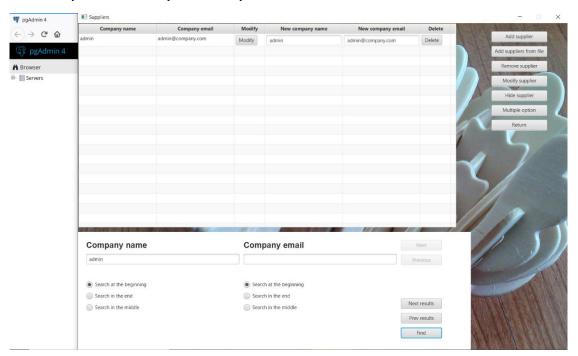
Modifikácia podľa loginu dodávateľa pri neznalosti emailu

Používateľ nepozná cieľový email, ale pozná login. Jeho úlohou je zmeniť login aj email. Systém ale vyžaduje znalosť emailovej adresy pri modifikácii. Cieľom by mohlo byť podhodiť nepravé informácie a odchytiť emaily zo súkromnej emailovej adresy.

Výpis databázy:

Data Output Expla			ain Messages Notificati	ons Query History
4	company [PK] integ		company_name character varying (50)	company_email character varying (60)
1		2	admin	admin@company.com

Položku by bolo možné vyhľadať v systéme:



Postup exploitácie

1. Nájdenie formulára, ktorý po aplikovaní znaku ' sa nezatvorí, alebo neinformuje o chybe (zlyháva):



2. Tvorba injekcie:

Útočník predpokladá, že SQL príkaz vyzerá nasledovne:

UPDATE supplier SET company_name=......



3. Exploitácia dopadla úspešne:

4	company_id [PK] integer	company_name character varying (50)	company_email character varying (60)
1	2	SQL Inject	inject@inject.com

Vysvetlenie:

V databáze nie je ošetrený SQL príkaz. Tvorí sa zjednotením reťazcov textu, ktoré sa nekontrolujú a ani parametricky do tohto reťazca nevkladajú. Útočník v prvom kroku zistí, že cieľová stanica neošetruje vstupy zadaním znaku ' do kolónky pre login. Ten spôsobí, že sa reťazce nesprávne uzatvoria. V prípade neošetrenia vstupu, to jednoznačne skončí výnimkou. Útočník v ďalšej faze môže hádať SQL príkaz. Keďže má prístup k formuláru pre zmenu emailu na základe loginu a ešte neošetrenom heslom, stačí mu vložiť SQL kód do kolónky pre login. Najprv zadá login v systéme a uzavrie ho znakom ', tým povie, že chce zmeniť tohto používateľa, následne ale pridá podmienku 1=1, čím indikuje, že prvá podmienka nemusí platiť, lebo táto platí vždy. Pre úplnosť zakomentuje zvyšok SQL príkazu použitím komentáru pre postgres, pokiaľ vie o tomto type databázy. Inak môže vyskúšať aj ďalšie typy komentárov, napríklad znak #, ktorý je typickým komentárom v Maria DB. Takýto príkaz, ale zmení všetkých používateľov, preto podmienka 1=1, nemusí byť vložená.

Zadaný príkaz vyzerá po dosadení injekcie nasledovne:

UPDATE supplier SET company_name='SQL Inject', company_email='inject@inject.com'
WHERE company_name='admin' or 1=1 --' 'AND company_email='skip@skip.com'

Podmieka nie je nutná:

UPDATE supplier SET company_name='SQL Inject', company_email='inject@inject.com'
WHERE company_name='admin' --' 'AND company_email='skip@skip.com'

Chybný kód na strane servera:

```
public void modifySupplier(String companyName, String companyEmail,String
       companyModifiedName, String companyModifiedEmail) throws SQLException
   {
     String prepareModifySupplier;
     PreparedStatement preparedStatement;
     prepareModifySupplier =
      "UPDATE supplier
      SET company_name='"+ companyModifiedName +
      "', company_email=""+ companyModifiedEmail +""
      WHERE company_name="" + companyName +""
      AND company_email="" +companyEmail +""";
      preparedStatement = connectionToDatabase.getConnection()
                          .prepareStatement(prepareModifySupplier);
     preparedStatement.executeUpdate();
     preparedStatement.close();
  }
```

Modifikácia podľa loginu dodávateľa pri neznalosti emailu - riešenie

Pri hľadaní a ošetrení SQL injekcií je potrebné nájsť slabinu v kód umožňujúcu SQL injekciu. V praxi sa odporúčajú používať parametrizované query, prípadne vstup kontrolovať pomocou regexov, alebo iného overenia na možné injekcie. Rovnako ako útočník môžeme pri hľadaní podhodiť znak ' do okna formuláru a pozrieť sa do logov, či niečo pri vyhodnocovaní query nezlyhalo.

Postup ošetrenia

1. Nájdenie formulára, ktorý po aplikovaní znaku ' sa nezatvorí, alebo neinformuje o chybe (zlyháva):



2. Tvorba parametrizovaného query: