

- Базата за податоци е програма од збирка на податоци. Дatabазата за податоци нуди APIs за креирање, пристап и управување на податоците кој ги држе. И базата за податоци (Database-DB) може да биде интегрирана за нашата веб страна за да можеме да пристапиме до податоците кои ги сакаме без тешкотија. Базата за податоци држи повеќе критични информации исто како : Кориснички имиња, лозинки, кредитни картички и други приватни информации кој можат да наштетат на многу клиенти. Значи базата за податоци мора да биде заштитена, но многу бази за податоци, сервери кој работат не се заштитени од нивните ранливости поради големи грешки во програмирањето. Да наброиме некој севери како на пример : MySQL(Open source), MSSQL, MS-ACCESS, Oracle, Postgre SQL(open source), SQLite и други...

- Што е SQL Injection

- Па можеме да речеме дека тоа е форма за логирање само на регистрирани корисници и е дозволен пристап да влезат на тоа место. Сега ние сакаме да го забиколиме логирањето на корисникот и да влеземе како одобрен корисник. Ако скрипатата не е добро средена од програмерот ќе имате среќа да влезете во базата на страницата. И можете да се конектирате на корисничкото име и лозинка како реален корисник меѓусобно со базата за податоци. Избираме корисничко име од databазата КАДЕ корисник='admin' и лозинка='7-MADRID' Ако ја селектираме командата и податоците се точни ќе имаме пристап. Замислете што би можело да направите ако е скриптата не средена. Тоа ја отвара вратата за "Хакерите" незаконски пристап до страната. Во овој пример напаѓачот може да ги внесе следните податоци за корисничко име или лозинка:

Корисник : а или 1=1--

Лозинка : празно

Селектирај корисник од databазата Каде корисник='а' or 1=1-- и лозинка=""

Сега овај упад делува вистинито дури и ако не постои корисник со назив "а" затоа што 1=1 е секогаш вистински. И таму ја има администрационата панела на страницата. Таму можат да бидат и други комбинации за корисничко име и лозинка за играње на загрозени страници. Можат и да се направат сопствени комбинации за пристап до администрациониот панел еве некој примери :

корисник:' or 1='1 лозинка:' or 1='1

корисник:' or '1'='1' лозинка:' or '1'='1'

корисник:or 1=1 лозинка:or 1=1

- Accessing Secret Data

SQL Injection не се работи само со забиколување на пристап до администрациониот панел туку истотака котистење за пристап до осетливи и приватни податоци од databазата.

- Проверување на ранливост

На пример има некоја страна како следниот пример:

----- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE PREUZETI NA SAJTU. -----

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com