

**ΟΙΚΟΝΟΜΙΚΟ  
ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΑΘΗΝΩΝ**



**ATHENS UNIVERSITY  
OF ECONOMICS  
AND BUSINESS**

**ΣΧΟΛΗ  
ΕΠΙΣΤΗΜΩΝ &  
ΤΕΧΝΟΛΟΓΙΑΣ  
ΤΗΣ  
ΠΛΗΡΟΦΟΡΙΑΣ**  
SCHOOL OF  
INFORMATION  
SCIENCES &  
TECHNOLOGY

**ΤΜΗΜΑ  
ΠΛΗΡΟΦΟΡΙΚΗΣ**  
DEPARTMENT OF  
INFORMATICS

# Ασφάλεια Δικτύων

## Εργαστηριακή Άσκηση SQL Injection

*Ευγένιος Γκρίτσης 3190045*

## Δημιουργία βάσης δεδομένων με MySQL στον CentOS 7

Η βάση η οποία χρησιμοποιήθηκε κατά την υλοποίηση της εργασίας, βρίσκεται στον υπολογιστή μου τοπικά και φαίνεται από τα screenshots των επόμενων ερωτημάτων.

Παρόλα αυτά, δημιουργήθηκε από την αρχή ένα copy της βάσης αυτής και στον CentOS 7 με σκοπό να βαθμολογηθεί. **Ο κωδικός του χρήστη root είναι: evgeniosgkritis NETSEC\_marias\_2023!**

Ακολουθούν οι εντολές mysql για την δημιουργία της βάσης GDPR και των tables users και logging:

```
CREATE DATABASE GDPR;
```

```
USE GDPR;
```

```
CREATE TABLE users (
```

```
    id INT AUTO_INCREMENT PRIMARY KEY,
```

```
    username VARCHAR(255) NOT NULL,
```

```
    password VARCHAR(255) NOT NULL,
```

```
    description VARCHAR(255),
```

```
    login_attempts INT DEFAULT 0,
```

```
    account_non_locked TINYINT DEFAULT 1,
```

```
    last_password_change TIMESTAMP,
```

```
    salt VARCHAR(255)
```

```
);
```

```
CREATE TABLE logging (
```

```
    id int auto_increment primary key,
```

```
    username varchar(255) not null,
```

```
    login_time timestamp not null default current_timestamp
```

```
);
```

```
INSERT INTO users (username, password, description, last_password_change, salt)
VALUES ('3190045', '$2a$12$yx8eswKetOQ9Q9.UHYPw2.sLE2OZl/5nIxPnDM1Dd4rpvlJmBvXVK', 'user',
NOW(), '[B@5679c6c6]');
```

```
INSERT INTO users (username, password, description, last_password_change, salt)
VALUES ('admin', '$2a$12$ltPqCFkGnA/t.OrzqFnkeJanEbFTOYQYLipX4Ruh/qnXhEKlc6/K', 'admin',
NOW(), '[B@27ddd392]');
```

```
mysql> show databases;
+-----+
| Database |
+-----+
| GDPR |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.00 sec)
```

```
mysql> show tables;
+-----+
| Tables_in_GDPR |
+-----+
| logging |
| users |
+-----+
2 rows in set (0.00 sec)
```

```
mysql> select * from users;
+----+-----+-----+-----+-----+-----+-----+-----+
| id | username | password | description | login_attempts | account_non_locked | last_password_change | salt |
+----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 3190045 | $2a$12$yx8eswKetOQ9Q9.UHYPw2.sLE2OZl/5nIxPnDM1Dd4rpvlJmBvXVK | user | 0 | 1 | 2023-01-24 09:50:15 | [B@5679c6c6 |
| 2 | admin | $2a$12$ltPqCFkGnA/t.OrzqFnkeJanEbFTOYQYLipX4Ruh/qnXhEKlc6/K | admin | 0 | 1 | 2023-01-24 09:55:34 | [B@27ddd392 |
+----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

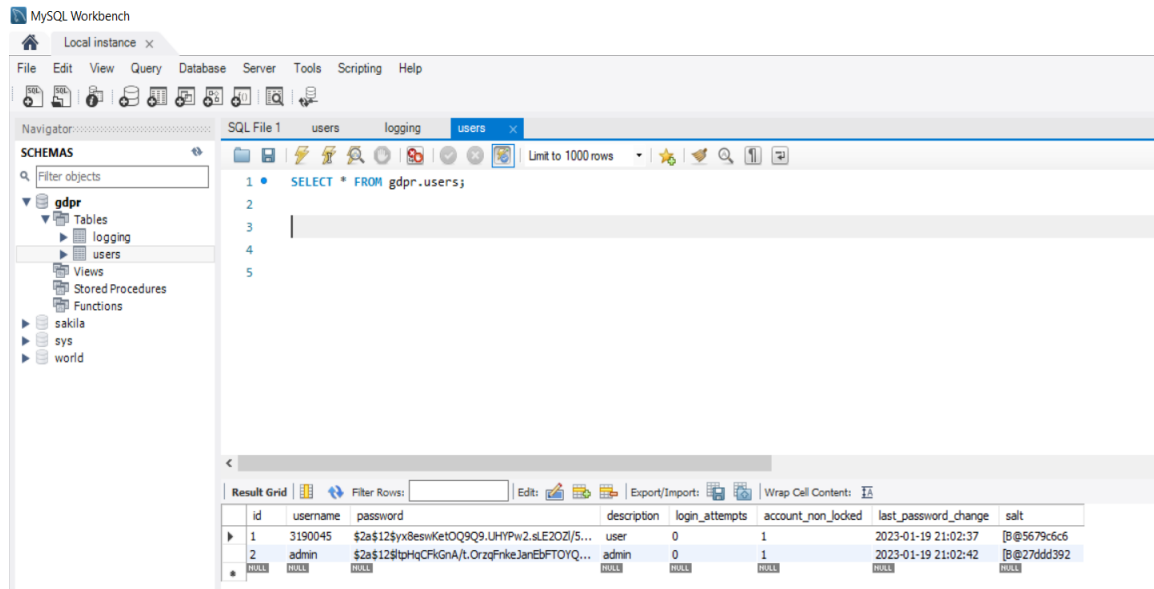
## Απάντηση:

Ένας συνηθισμένος τρόπος για να διασφαλιστεί το απόρρητο των κωδικών πρόσβασης των χρηστών σε περίπτωση μη εξουσιοδοτημένης εξαγωγής δεδομένων από την βάση δεδομένων, είναι η αποθήκευση των κωδικών σε κατακερματισμένη (hashed) μορφή και όχι σε απλό κείμενο. Αυτό συνήθως γίνεται με την εφαρμογή ενός αλγορίθμου one-way hash όπως ο Bcrypt. Αυτό έχει ως αποτέλεσμα ο κακόβουλος χρήστης να μην καταφέρει να πάρει στα χέρια του τον πραγματικό κωδικό καθώς οι συναρτήσεις σύνοψης είναι μη αντιστρέψιμες. Παρόλα αυτά, λόγω των επιθέσεων με rainbow tables, είναι σημαντικό να προστεθεί μια έξτρα δικλείδα ασφαλείας που ονομάζεται “salt”. Κατά αυτόν τον τρόπο, ακόμη και εάν το αρχείο με τους hashed κωδικούς πρόσβασης κλαπεί, ο επιτιθέμενος δεν θα καταφέρει να αντιστρέψει τα cryptographic hash functions με την χρήση rainbow tables αφού ο attacker θα πρέπει να υπολογίσει tables για κάθε δυνατή salt τιμή, κάτι το οποίο είναι αδύνατο. Επιπροσθέτως, με το salting αποτρέπεται και η αποθήκευση ίδιων κωδικών σε δύο ή παραπάνω χρήστες.

Παρακάτω, φαίνεται η αποθήκευση των κωδικών πρόσβασης των χρηστών σε hashed μορφή από την αυτοματοποιημένη online υπηρεσία Bcrypt-Generator καθώς η λειτουργία registration δεν ήταν στα πλαίσια της εργασίας με αποτέλεσμα να μην εισάγει κωδικό ο χρήστης.

Όπως φαίνεται, ο πίνακας users αποτελείται από τα πεδία id (πρωτεύων κλειδί), username, password, description, login\_attempts, account\_non\_locked και last\_password\_change, salt.

Ο κωδικός του χρήστη '3190045' είναι 'password' και ο κωδικός του χρήστη 'admin' είναι 'admin'.



Παράλληλα, φαίνεται και το πεδίο salt το οποίο δημιουργήθηκε με τον εξής τρόπο και στην συνέχεια εισάχθηκαν στον πίνακα users manually με εντολές SQL:

```
1 usage  eGkritsis *
@SpringBootApplication
public class SpringBootSecureAccessControlApplication implements WebMvcConfigurer {

    no usages  eGkritsis *
    public static void main(String[] args) {

        SecureRandom secureRandom = new SecureRandom();
        byte[] salt = new byte[16];
        secureRandom.nextBytes(salt);
        System.out.println("salt:" + salt);

        byte[] salt2 = new byte[16];
        secureRandom.nextBytes(salt2);
        System.out.println("salt2:" + salt2);

        //salt:[B@5679c6c6
        //salt2:[B@27ddd392

        SpringApplication.run(SpringBootSecureAccessControlApplication.class, args);
    }
}
```

Οι τιμές των salt θα μπορούσαν να έχουν παραχθεί και ως εξής με εντολές SQL:

```
UPDATE users SET salt = UNHEX(SHA2(UUID(), 256)) WHERE id = <user_id>;
```

Παράλληλα, στο συγκεκριμένο κομμάτι κώδικα μέσω του Spring Boot Framework και συγκεκριμένα του Security Dependency, ελέγχεται με αυτόματο τρόπο ο ανακτημένος κωδικός πρόσβασης με αυτόν που παρουσιάζεται στο αίτημα αυθεντικοποίησης χρησιμοποιώντας τον passwordEncoder που είναι τύπος BCryptPasswordEncoder.

```
no usages  👤 eGkritsis
@Bean
public BCryptPasswordEncoder passwordEncoder() {
    return new BCryptPasswordEncoder();
}

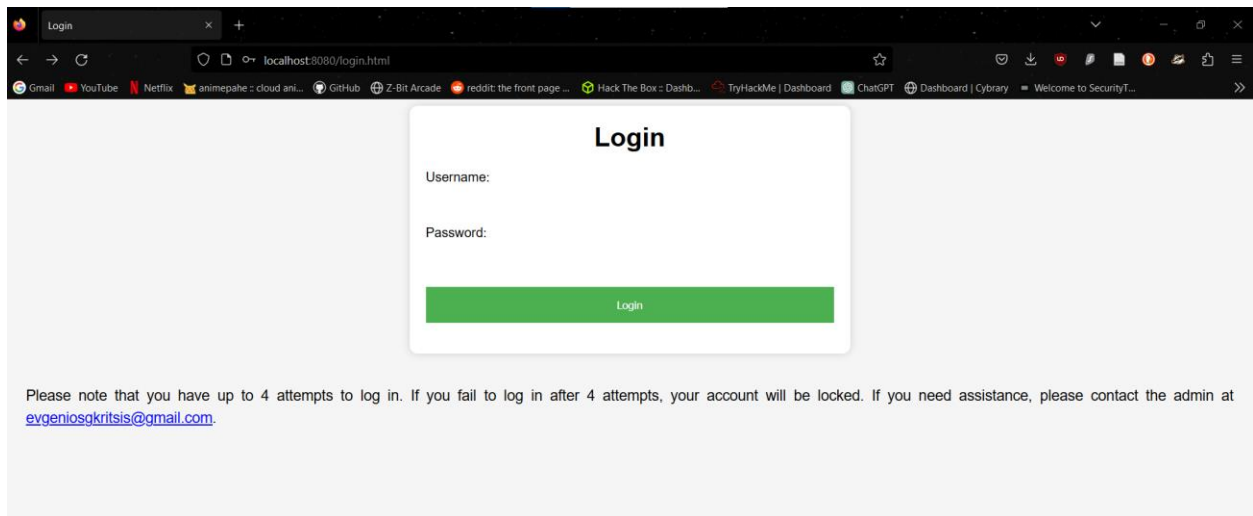
1 usage  👤 eGkritsis
@Bean
AuthenticationProvider authenticationProvider() {
    DaoAuthenticationProvider provider = new DaoAuthenticationProvider();
    provider.setUserDetailsService(userDetailsService);
    provider.setPasswordEncoder(new BCryptPasswordEncoder());

    return provider;
}
```

## Ακολουθούν αναλυτικά screenshots της υλοποίησης.

1. Επιτυχής σύνδεση χρήστη, προβολή τελευταίας αλλαγής κωδικού και ενημέρωση για λήξη κωδικού πρόσβασης.

Αρχική σελίδα που εμφανίζεται στον χρήστη:



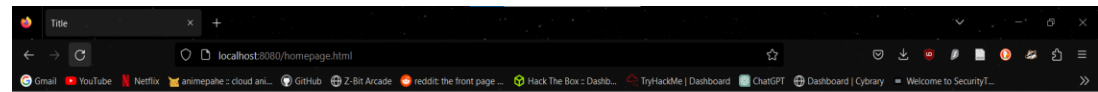
Ο χρήστης δοκιμάζει να συνδεθεί με username: admin και password: admin ή username: 3190045 και password: password και το σύστημα αφότου τον αυθεντικοποιήσει, τον κάνει redirect στο homepage.html. Στο homepage.html, εμφανίζεται η ημερομηνία της τελευταίας αλλαγής κωδικού του χρήστη, καθώς και σε πόσο χρονικό διάστημα από την στιγμή που έκανε login θα λήξει ο κωδικός του και θα πρέπει να τον ανανεώσει (3 μήνες από το τελευταίο password change).



## Welcome admin

Last password change: 2023-01-19T21:02:42

Your password will expire in 0 years, 2 months, 26 days, 1 hours, 2 minutes, 36 seconds.



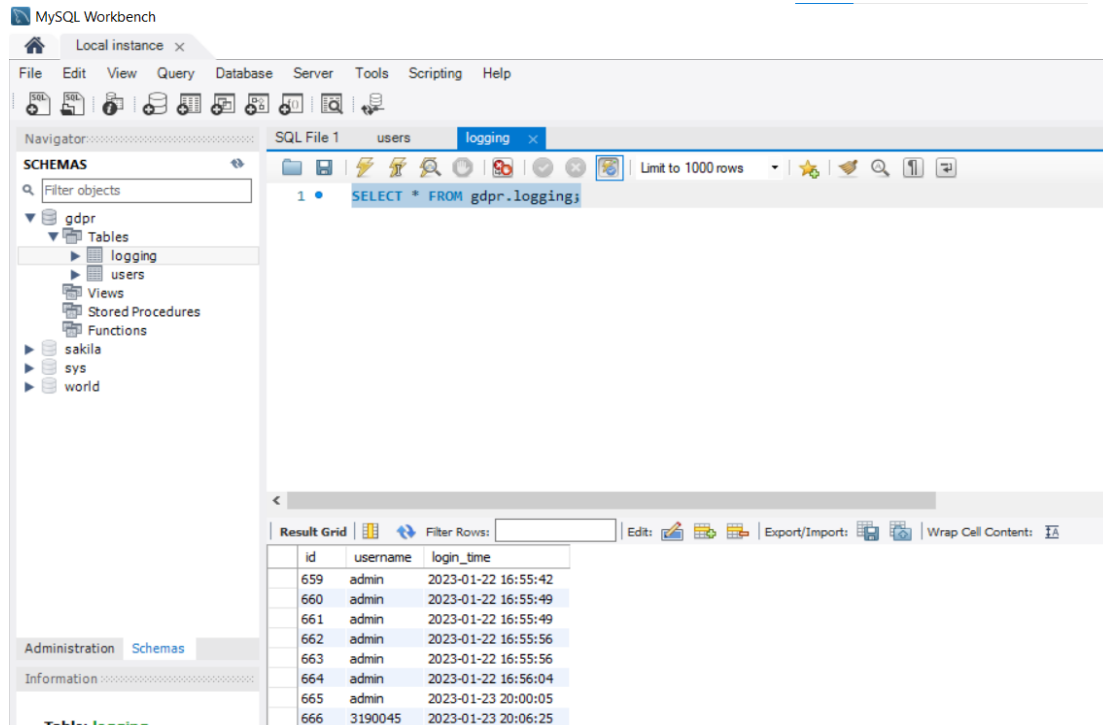
## Welcome 3190045

Last password change: 2023-01-19T21:02:37

Your password will expire in 0 years, 2 months, 26 days, 0 hours, 56 minutes, 11 seconds.

## 2. Μηχανισμός παρακολούθησης δραστηριότητας στο login endpoint.

Κατά την επιτυχής σύνδεση του admin και του χρήστη 3190045, ο πίνακας logging ανανεώνεται, αποθηκεύοντας τις απόπειρες επιτυχούς login (σημ. στο παρακάτω screenshot φαίνονται και προηγούμενες επιτυχημένες προσπάθειες από διαφορετικές ημερομηνίες που αποθηκεύτηκαν κατά το στάδιο της υλοποίησης της εφαρμογής) με κατάλληλο πεδίο χρονοσφραγίδας:



The screenshot shows the MySQL Workbench interface. The left sidebar displays the 'Schemas' tree with the 'gdpr' database selected. The 'logging' table is highlighted under the 'Tables' section. The main window shows the SQL query editor with the query `SELECT * FROM gdpr.logging;`. Below the editor, the 'Result Grid' displays the query results. The table has three columns: 'id', 'username', and 'login\_time'. The results show several login attempts, with the last two rows indicating successful logins for 'admin' and '3190045' on 2023-01-23.

id	username	login_time
659	admin	2023-01-22 16:55:42
660	admin	2023-01-22 16:55:49
661	admin	2023-01-22 16:55:49
662	admin	2023-01-22 16:55:56
663	admin	2023-01-22 16:55:56
664	admin	2023-01-22 16:56:04
665	admin	2023-01-23 20:00:05
666	3190045	2023-01-23 20:06:25

Όπως φαίνεται, οι προσπάθειες επιτυχούς απόπειρας login με id=665 και 666 ήταν του admin και του χρήστη 3190045 τις χρονικές στιγμές 23/1/2023 20:00:05 και 23/1/2023 20:06:25 αντίστοιχα. (Οι προηγούμενες φαίνεται πως προέρχονται από προηγούμενες ημερομηνίες που η εφαρμογή περνούσε το στάδιο του ελέγχου της λειτουργικότητας).



### 3. Μηχανισμός κλειδώματος λογαριασμού χρήστη.

Όπως φαίνεται από τα παραπάνω screenshot της βάσης δεδομένων μας, στο table users, υπάρχουν τα πεδία με όνομα *login\_attempts* και *account\_non\_locked*. Η εφαρμογή είναι υλοποιημένη με τέτοιο τρόπο ώστε ο κάθε χρήστη να δικαιούται έως και 4 ανεπιτυχείς προσπάθειες εισόδου του. Εάν, στην 4<sup>η</sup> προσπάθεια του, δεν καταφέρει να περάσει τον έλεγχο, η εφαρμογή εμφανίζει κατάλληλο μήνυμα «κλειδώματος» και πλέον ακόμη και σωστά credentials να εισάγει, η πρόσβαση του απαγορεύεται καθώς η Boolean μεταβλητή *account\_non\_locked* έχει τεθεί ίση με 0. Σημαντικό είναι να τονιστεί πως εάν ο χρήστης καταφέρει να εισάγει τα σωστά credentials πριν κλειδωθεί, το πεδίο *login\_attempts* μηδενίζεται.

1<sup>η</sup> αποτυχημένη προσπάθεια:

### Login

Username:

Password:

Login

Remaining Attempts for 3190045 : 3

Please note that you have up to 4 attempts to log in. If you fail to log in after 4 attempts, your account will be locked. If you need assistance, please contact the admin at [evgeniosgkritis@gmail.com](mailto:evgeniosgkritis@gmail.com).

id	username	password	description	login_attempts	account_non_locked	last_password_change	salt
1	3190045	\$2a\$12\$yx8eswKetOQ9Q9.UHYPw2.sLE2OZl/5...	user	1	1	2023-01-19 21:02:37	[B@5679c6c6

2<sup>η</sup> αποτυχημένη προσπάθεια

### Login

Username:

Password:

Login

Remaining Attempts for 3190045 : 2

Please note that you have up to 4 attempts to log in. If you fail to log in after 4 attempts, your account will be locked. If you need assistance, please contact the admin at [evgeniosgkritis@gmail.com](mailto:evgeniosgkritis@gmail.com).

id	username	password	description	login_attempts	account_non_locked	last_password_change	salt
1	3190045	\$2a\$12\$yx8eswKetOQ9Q9.UHYPw2.sLE2OZl/5...	user	2	1	2023-01-19 21:02:37	[B@5679c6c6

### 3<sup>η</sup> αποτυχημένη προσπάθεια

## Login

Username:

Password:

Login

Remaining Attempts for 3190045 : 1

Please note that you have up to 4 attempts to log in. If you fail to log in after 4 attempts, your account will be locked. If you need assistance, please contact the admin at [evgeniosgkritis@gmail.com](mailto:evgeniosgkritis@gmail.com).

	id	username	password	description	login_attempts	account_non_locked	last_password_change	salt
▶	1	3190045	\$2a\$12\$yx8eswKetOQ9Q9.UHYPw2.sLE2OZl/5...	user	3	1	2023-01-19 21:02:37	[B@5679c6c6

### 4<sup>η</sup> και τελευταία αποτυχημένη προσπάθεια (account\_non\_locked = 0)

## Login

Username:

Password:

Login

Your account (3190045) has been locked due to 4 failed attempts!

Please note that you have up to 4 attempts to log in. If you fail to log in after 4 attempts, your account will be locked. If you need assistance, please contact the admin at [evgeniosgkritis@gmail.com](mailto:evgeniosgkritis@gmail.com).

	id	username	password	description	login_attempts	account_non_locked	last_password_change	salt
▶	1	3190045	\$2a\$12\$yx8eswKetOQ9Q9.UHYPw2.sLE2OZl/5...	user	3	0	2023-01-19 21:02:37	[B@5679c6c6