Web Applications Security		
		
Kamil Gabrysiewicz	Index: 95400	Grupa: 2.1
Wtorek 11:45-13:15	Semestr 2	Laboratorium 5

Task 5.1.

Develop functionalities for managing permissions:

- displaying a list of permissions in the system,
- displaying a list of user permissions with the option of adding and removing permissions,
- displaying a list of roles in the system with the option of adding or removing roles,

- displaying a list of permissions assigned to the role with the option of adding and removing permissions,
- displaying a list of user roles with t;he option of adding or removing roles for the user.

```
use mydb;

CREATE TABLE mydb.user (
    id INT(11) PRIMARY KEY AUTO_INCREMENT,
    name VARCHAR(30) NOT NULL,
    surname VARCHAR(40) NOT NULL,
    phone VARCHAR(12),
    login VARCHAR(30) COLLATE utf8_polish_ci NOT NULL,
    email VARCHAR(60) COLLATE utf8_polish_ci NOT NULL,
    hash VARCHAR(255) COLLATE utf8_polish_ci NOT NULL COMMENT 'password hash or HMAC
value',
    salt BLOB DEFAULT NULL COMMENT 'salt to use in password hashing',
    sms_code VARCHAR(6) COLLATE utf8_polish_ci DEFAULT NULL COMMENT 'security code sent via
sms or e-mail',
    code_timelife TIMESTAMP NULL DEFAULT NULL COMMENT 'timelife of security code',
    security_question VARCHAR(255) COLLATE utf8_polish_ci DEFAULT NULL COMMENT 'additional
security question used while password recovering',
    answer VARCHAR(255) COLLATE utf8_polish_ci DEFAULT NULL COMMENT 'security question
answer',
    lockout_time TIMESTAMP NULL DEFAULT NULL COMMENT 'time to which user account is
blocked',
    session_id BLOB DEFAULT NULL COMMENT 'user session identifier',
    id_status INT(11) NOT NULL COMMENT 'account status',
    password_form INT(11) NOT NULL DEFAULT 1 COMMENT '1- SHA512, 2-SHA512+salt, 3- HMAC'
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_polish_ci;


CREATE TABLE mydb.privilege (
    id INT PRIMARY KEY,
    id_parent_privilege INT,
    name VARCHAR(100) NOT NULL,
    active TINYINT NOT NULL,
    asset_url VARCHAR(200),
    FOREIGN KEY (id_parent_privilege) REFERENCES mydb.privilege(id)
);

CREATE TABLE mydb.role (
    id SMALLINT PRIMARY KEY,
    role_name VARCHAR(30) NOT NULL,
    description TEXT
);

CREATE TABLE mydb.user_role (
    id INT PRIMARY KEY,
    id_role SMALLINT,
    id_user INT,
    issue_time DATE,
    expire_time DATE,
    FOREIGN KEY (id_role) REFERENCES mydb.role(id),
```

```
    FOREIGN KEY (id_user) REFERENCES mydb.user(id)
);


CREATE TABLE mydb.role_privilege (
    id INT PRIMARY KEY,
    id_role SMALLINT,
    id_privilege INT,
    issue_time DATE,
    expire_time DATE,
    FOREIGN KEY (id_role) REFERENCES mydb.role(id),
    FOREIGN KEY (id_privilege) REFERENCES mydb.privilege(id)
);

CREATE TABLE mydb.user_privilege (
    id INT PRIMARY KEY,
    id_user INT,
    id_privilege INT,
    FOREIGN KEY (id_user) REFERENCES mydb.user(id),
    FOREIGN KEY (id_privilege) REFERENCES mydb.privilege(id)
);


INSERT INTO mydb.privilege (id, name, active)
VALUES (100, 'add message', 1);

INSERT INTO mydb.privilege (id, name, active)
VALUES (102, 'delete message', 1);

INSERT INTO mydb.privilege (id, name, active)
VALUES (103, 'display private', 1);

INSERT INTO mydb.privilege (id, name, active)
VALUES (101, 'edit message', 1);


CREATE TABLE `message` (
 `id` int(11) NOT NULL,
 `name` varchar(255) COLLATE utf8_polish_ci NOT NULL COMMENT 'name of the message',
 `type` varchar(20) COLLATE utf8_polish_ci DEFAULT NULL COMMENT 'type of the message
(private/public)',
 `message` varchar(2000) COLLATE utf8_polish_ci NOT NULL COMMENT 'message text',
 `deleted` tinyint(4) NOT NULL DEFAULT 0 COMMENT 'existing message - 0, deleted - 1'
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_polish_ci;

INSERT INTO `message` (`id`, `name`, `type`, `message`, `deleted`) VALUES
(1, 'New Intel technology', 'public', 'Intel has announced a new processor for desktops',
0),
(2, 'Intel shares raising', 'private', 'brokers announce: Intel shares will go up!', 0),
(3, 'New graphic card from NVidia', 'public', 'NVidia has announced a new graphic card for
desktops', 0),
(4, 'Airplane crash', 'public', 'A passenger plane has crashed in Europe', 0),
(5, 'Coronavirus', 'private', 'A new version of virus was found!', 0),
(6, 'Bitcoin price raises', 'public', 'Price of bitcoin reaches new record.', 0),
(9, 'New Windows announced', 'public', 'A new version of windows was announced. Present
buyers of Widows
```

```
10 can update the system to the newest version for free.', 0);

ALTER TABLE `message`
 ADD PRIMARY KEY (`id`);
ALTER TABLE `message`
 MODIFY `id` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=10;
```

session_expiration: 1731512889
Logged in: 1

displaying a list of permissions in the system [See]	No permissions available to display.
displaying a list of user permissions with the option of adding and removing permissions [See]	
displaying a list of roles in the system with the option of adding or removing roles [See]	
displaying a list of permissions assigned to the role with the option of adding and removing permissions [See]	
displaying a list of user roles with the option of adding or removing roles for the user [See]	

Index
messages
Add New message
Privileges

session_expiration: 1731512892
Logged in: 1

displaying a list of permissions in the system [See]	Name
displaying a list of user permissions with the option of adding and removing permissions [See]	add message
displaying a list of roles in the system with the option of adding or removing roles [See]	edit message
displaying a list of permissions assigned to the role with the option of adding and removing permissions [See]	delete message
displaying a list of user roles with the option of adding or removing roles for the user [See]	display private
	add role
	edit role
	delete role
	add permission
	edit permission
	delete permission

Index
messages
Add New message
Privileges

session_expiration: 1731512939
Logged in: 1

displaying a list of permissions in the system [See]	ROLE NAME	NAME
displaying a list of user permissions with the option of adding and removing permissions [See]	admin	add message
displaying a list of roles in the system with the option of adding or removing roles [See]	admin	add permission
displaying a list of permissions assigned to the role with the option of adding and removing permissions [See]	admin	add role
displaying a list of user roles with the option of adding or removing roles for the user [See]	admin	delete message
	admin	delete permission
	admin	delete role
	moderator	add message
	moderator	delete message
	regular	add message

Index
messages
Add New message
Privileges

session_expiration: 1731512979
Logged in: 1

displaying a list of permissions in the system	See
displaying a list of user permissions with the option of adding and removing permissions	See
displaying a list of roles in the system with the option of adding or removing roles	See
displaying a list of permissions assigned to the role with the option of adding and removing permissions	See
displaying a list of user roles with the option of adding or removing roles for the user	See

ROLE	PRIVILEGE
admin	add message
admin	add permission
admin	add role
admin	delete message
admin	delete permission
admin	delete role
admin	display private
admin	edit message
admin	edit permission
admin	edit role
moderator	add message
moderator	delete message
moderator	edit message
regular	add message
regular	edit message

Index
messages
Add New message
Privileges

session_expiration: 1731513014
Logged in: 1

displaying a list of permissions in the system	See
displaying a list of user permissions with the option of adding and removing permissions	See
displaying a list of roles in the system with the option of adding or removing roles	See
displaying a list of permissions assigned to the role with the option of adding and removing permissions	See
displaying a list of user roles with the option of adding or removing roles for the user	See

ROLE NAME	DESCRIPTION	NAME
admin	Administrator with full access	add role
admin	Administrator with full access	delete role

Index
messages
Add New message
Privileges

Task 5.2.

Verify the list of effective user permissions - create a set of permissions for the logging in user, resulting from his permissions and the permissions resulting from the roles assigned to him. Save a list of permissions in the session. When displaying a page, only show the user the items for which they have permission.

View for unlogged user, privileges are hidden

session_expiration: null
Logged in: null
Role: unknown

Main page

Register new user

login
email
password
repeat password
Create account

Log in

login
password
Log in

Code
Verify

Change Password

Login
Current Password
New Password
Repeat New Password
Change Password

Warning: Undefined array key "role" in **/var/www/html/index.php** on line **150**
Index
Messages
Add New Message

Logging as a "test" user which has a role of "user" which is default and has the least amount of privileges

Main page

Register new user

login
email
password
repeat password
Create account

Log in

login test
password test
Log in

Code 740056
Verify

Change Password

Login
Current Password
New Password
Repeat New Password
Change Password

Warning: Undefined array key "role" in **/var/www/html/index.php** on line **150**
Index
Messages
Add New Message

Logged in as "user" role, the privileges navigation is hidden

session_expiration: 1732622731
Logged in: 1
Role: user

Main page

Register new user

login
email
password
repeat password
Create account

Log in

login
password
Log in

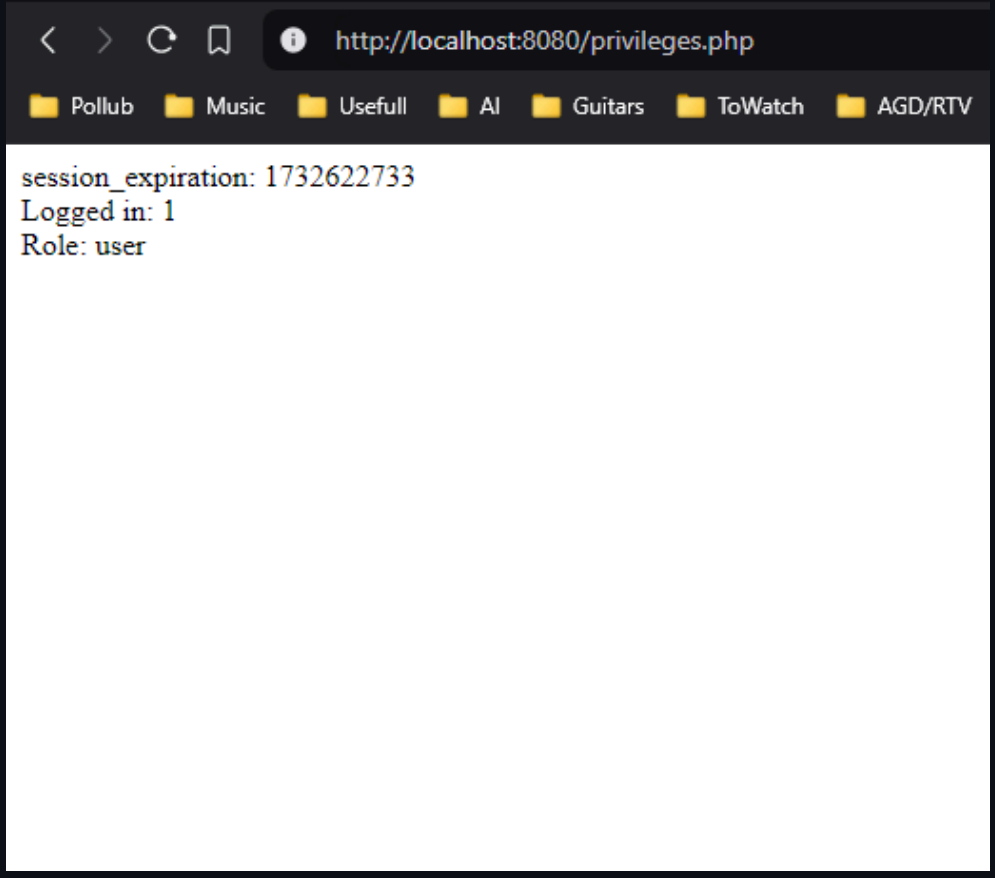
Code
Verify

Change Password

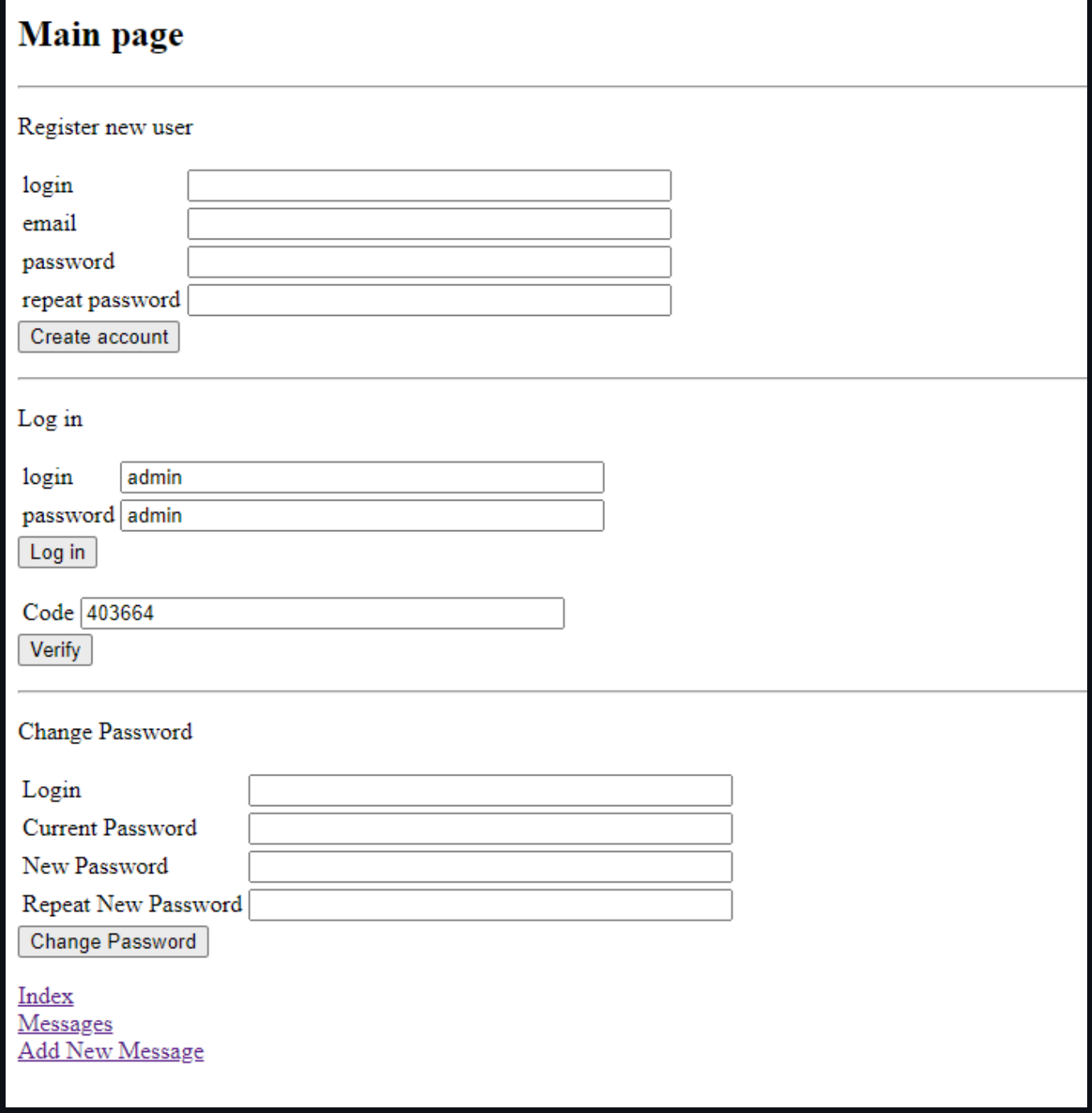
Login
Current Password
New Password
Repeat New Password
Change Password

Index
Messages
Add New Message

The dafault "user" might want to try access localhost/privileges.php but the content is rendered only for privileged roles such as "moderator" and "admin"



Loggin in as a admin with "admin" role



Logged in as admin, the privileges navigation is visible and admin can acceess its content

session_expiration: 1732622888
Logged in: 1
Role: admin

Main page

Register new user

login
email
password
repeat password
Create account

Log in

login
password
Log in

Code
Verify

Change Password

Login
Current Password
New Password
Repeat New Password
Change Password

Index
Messages
Add New Message
Privileges

Admin has access to privileges.php

session_expiration: 1732622931
Logged in: 1
Role: admin

displaying a list of permissions in the system	See
displaying a list of user permissions with the option of adding and removing permissions	See
displaying a list of roles in the system with the option of adding or removing roles	See
displaying a list of permissions assigned to the role with the option of adding and removing permissions	See
displaying a list of user roles with the option of adding or removing roles for the user	See

Name
add message
edit message
delete message
display private
add permission
edit permission
delete permission
add role
edit role
delete role

Index
Messages
Add New Message
Privileges

Task 5.3.

Add message editing and deleting functions to your application. Make these functionalities available only to authorized users.

Messages view for user with role "user", delete buttons are hidden from unprivileged user

session_expiration: 1732626893
Logged in: 1
Role: user

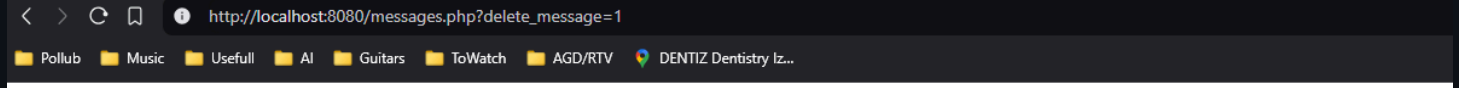
Messages

Intel shares raising	brokers announce: Intel shares will go up!	Edit
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit
Airplane crash	A passenger plane has crashed in Europe	Edit
Coronavirus	A new version of virus was found!	Edit
Bitcoin price raises	Price of bitcoin reaches new record.	Edit
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit

Navigation

Index
Messages
Add New Message

Still "user" might want to delete message via url `localhost/messages.php?delete_message=1` but its also secured to check user role before commiting such action



session_expiration: 1732626957
Logged in: 1
Role: user

You do not have permission to delete messages.

Messages

Intel shares raising	brokers announce: Intel shares will go up!	Edit
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit
Airplane crash	A passenger plane has crashed in Europe	Edit
Coronavirus	A new version of virus was found!	Edit
Bitcoin price raises	Price of bitcoin reaches new record.	Edit
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit

Navigation

Index
Messages
Add New Message

Messages view for admin with role "admin"

session_expiration: 1732627065
Logged in: 1
Role: admin

Messages

Intel shares raising	brokers announce: Intel shares will go up!	Edit Delete
New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit Delete
Airplane crash	A passenger plane has crashed in Europe	Edit Delete
Coronavirus	A new version of virus was found!	Edit Delete
Bitcoin price raises	Price of bitcoin reaches new record.	Edit Delete
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit Delete

Navigation

Index
Messages
Add New Message
Privileges

View after successful delete of user's message

session_expiration: 1732627068
Logged in: 1
Role: admin

Message deleted successfully.

Messages

New graphic card from NVidia	NVidia has announced a new graphic card for desktops	Edit Delete
Airplane crash	A passenger plane has crashed in Europe	Edit Delete
Coronavirus	A new version of virus was found!	Edit Delete
Bitcoin price raises	Price of bitcoin reaches new record.	Edit Delete
New Windows announced	A new version of windows was announced. Present buyers of Widows 10 can update the system to the newest version for free.	Edit Delete

Navigation

Index
Messages
Add New Message
Privileges