Advanced SQL injection

Introduction to PostgreSQL

Introduction

In this module we will be exploring a few `advanced SQL injection` techniques as well as some PostgreSQL-specific attacks from a `white-box approach`. As this is an advanced module, an understanding of SQL syntax, SQL injections and Python3 is expected to fully grasp the concepts explained. Although this module will focus on `PostgreSQL`, the same techniques can be adapted to work with other SQL variants, as it is a standardized language.

Interacting with PostgreSQL

Before we get into injection vulnerablities, let's take a moment to familiarize ourselves with two of the most common tools for interacting with `PostgreSQL` databases: psql and pgAdmin4.

psql (PostgreSQL Interactive Terminal)

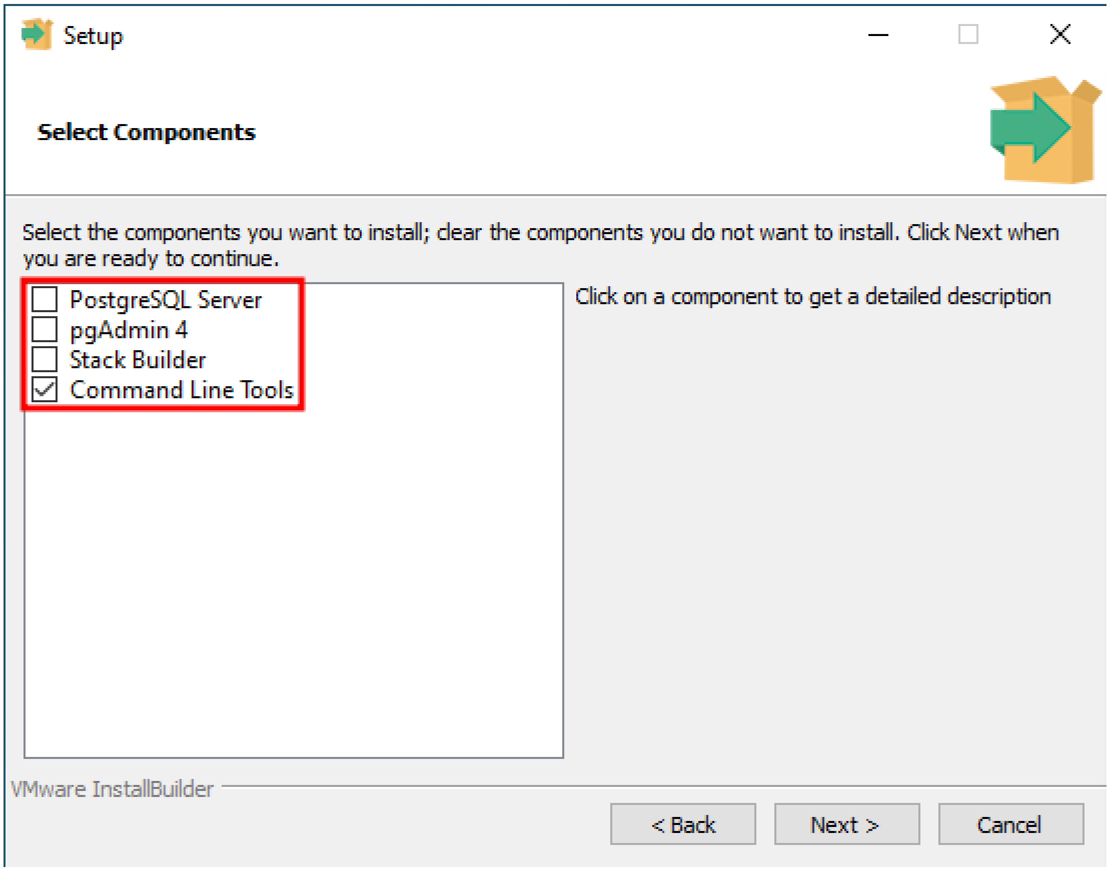
psql is a `command-line` tool for interacting with `PostgreSQL` databases that comes pre-packaged with the `PostgreSQL` server and works on `Linux` or `Windows`.

You can install `psql` on a `Linux` distribution with this single command:

```
mayala@htb[/htb] $ sudo apt install postgresql-client-15
```

Note: It's possible that the distribution of `Linux` you are running does not have version `15`. In that case, you can install version `13` and everything will work fine with minimally adapted steps.

To install `psql` on `Windows`, you should first download the `PostgreSQL` installer from postgresql.org and then during the installation process unselect everything except for `Command Line Tools`.

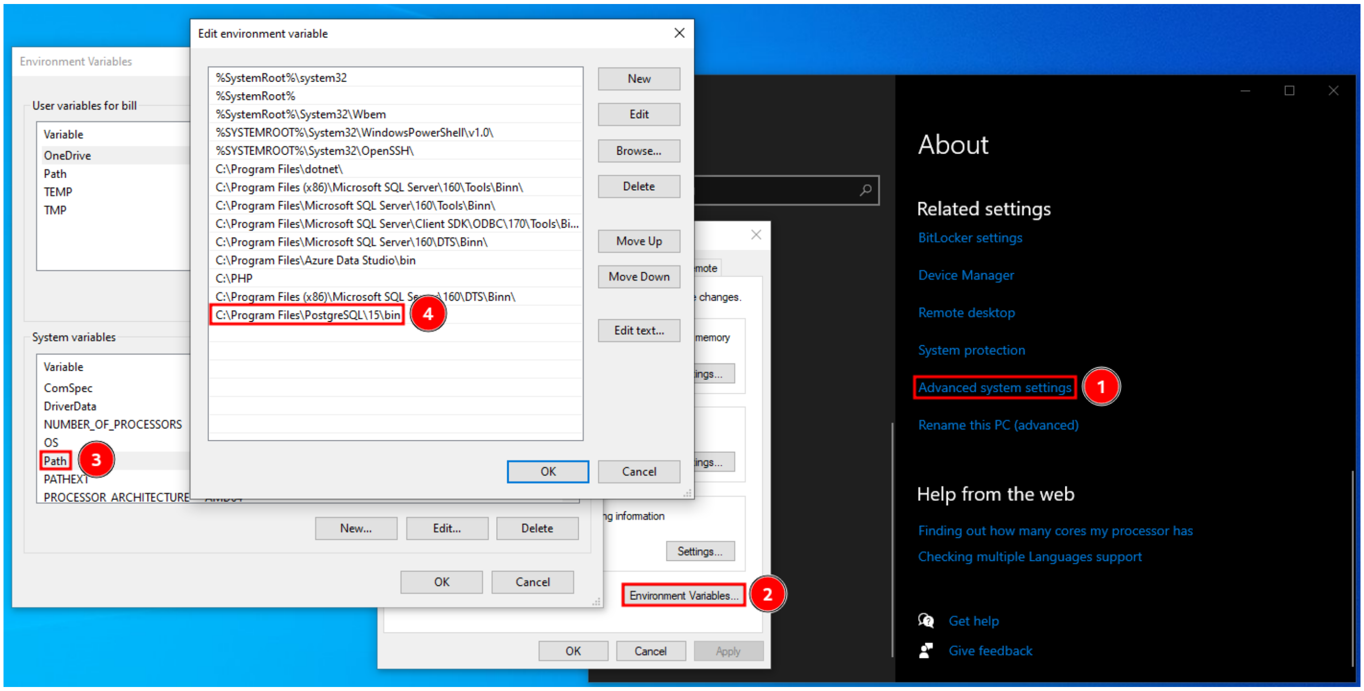


Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

- □ PostgreSQL Server
- □ pgAdmin 4
- □ Stack Builder
- ☑ Command Line Tools

Click on a component to get a detailed description

Once it's done installing, you may use `psql.exe` from the installation directory (`C:\Program Files\PostgreSQL\15\bin` by default) or you can add the directory to the system `PATH` variable to be able to use it from anywhere:



```
%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
C:\Program Files\dotnet\
C:\Program Files (x86)\Microsoft SQL Server\160\Tools\Binn\
C:\Program Files\Microsoft SQL Server\160\Tools\Binn\
C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Bi...
C:\Program Files\Microsoft SQL Server\160\DTS\Binn\
C:\Program Files\Azure Data Studio\bin
C:\PHP
C:\Program Files (x86)\Microsoft SQL Se   \160\DTS\Binn\
C:\Program Files\PostgreSQL\15\bin
```

Once you've installed `psql` on your operating system of choice, you can connect to a `PostgreSQL` database with the following command:

```
mayala@htb[/htb]$ psql -h 127.0.0.1 [-p PORT] -U acdbuser acmecorp Password for
user acdbuser: psql (15.1 (Debian 15.1-1+b1), server 13.9 (Debian 13.9-
0+deb11u1)) SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384,
compression: off) Type "help" for help. acmecorp=>
```

Once connected, you can list databases with the `\l` command or `\l+` for extended details.

```
acmecorp=> \l
                                             List of databases
   Name    |  Owner   | Encoding | Collate |  Ctype   | ICU Locale | Locale
Provider |   Access privileges
-----------+----------+----------+---------+---------+------------+---------
--------+-----------------------
 acmecorp  | postgres | UTF8     | C.UTF-8 | C.UTF-8 |            | libc
|
 postgres  | postgres | UTF8     | C.UTF-8 | C.UTF-8 |            | libc
|
 template0 | postgres | UTF8     | C.UTF-8 | C.UTF-8 |            | libc
| =c/postgres          +
           |          |          |         |         |            |
| postgres=CTc/postgres
 template1 | postgres | UTF8     | C.UTF-8 | C.UTF-8 |            | libc
| =c/postgres          +
           |          |          |         |         |            |
| postgres=CTc/postgres
(4 rows)
```

To switch to a database you can use the `\c <DATABASE>` command. In this case we are already in the `acmecorp` database.

To list the tables in a database (after you've switched to it), you can use the `\dt` command or `\dt+` for extended information.

```
acmecorp=> \dt+
                                        List of relations
 Schema |    Name     | Type  |  Owner   | Persistence | Access method |
Size    | Description
--------+-------------+-------+----------+-------------+---------------+----
--------+-------------
 public | departments | table | postgres | permanent   | heap          |
8192 bytes |
 public | dept_emp    | table | postgres | permanent   | heap          | 72
kB      |
 public | employees   | table | postgres | permanent   | heap          | 176
```

```
kB     |
 public | salaries    | table | postgres | permanent   | heap          | 72
kB      |
 public | titles      | table | postgres | permanent   | heap          | 80
kB      |
(5 rows)
```

Last, but not least, you can query the database simply by entering the query and making sure it's terminated with a semicolon. Multi-line queries work as well.

```
acmecorp=> SELECT first_name, last_name, email FROM employees LIMIT 5;
 first_name |  last_name  |           email
------------+-------------+---------------------------
 Kathleen   | Flint       | knflint82@acme.corp
 Henry      | Watson      | hywatson40@acme.corp
 Ruth       | Perez       | rhperez84@acme.corp
 Leon       | Tappin      | lntappin80@acme.corp
 Donita     | Fairweather | dafairweather92@acme.corp
(5 rows)
```

pgAdmin4

pgAdmin4 is a `GUI` application for interacting with `PostgreSQL` databases that works on `Linux` and `Windows`.

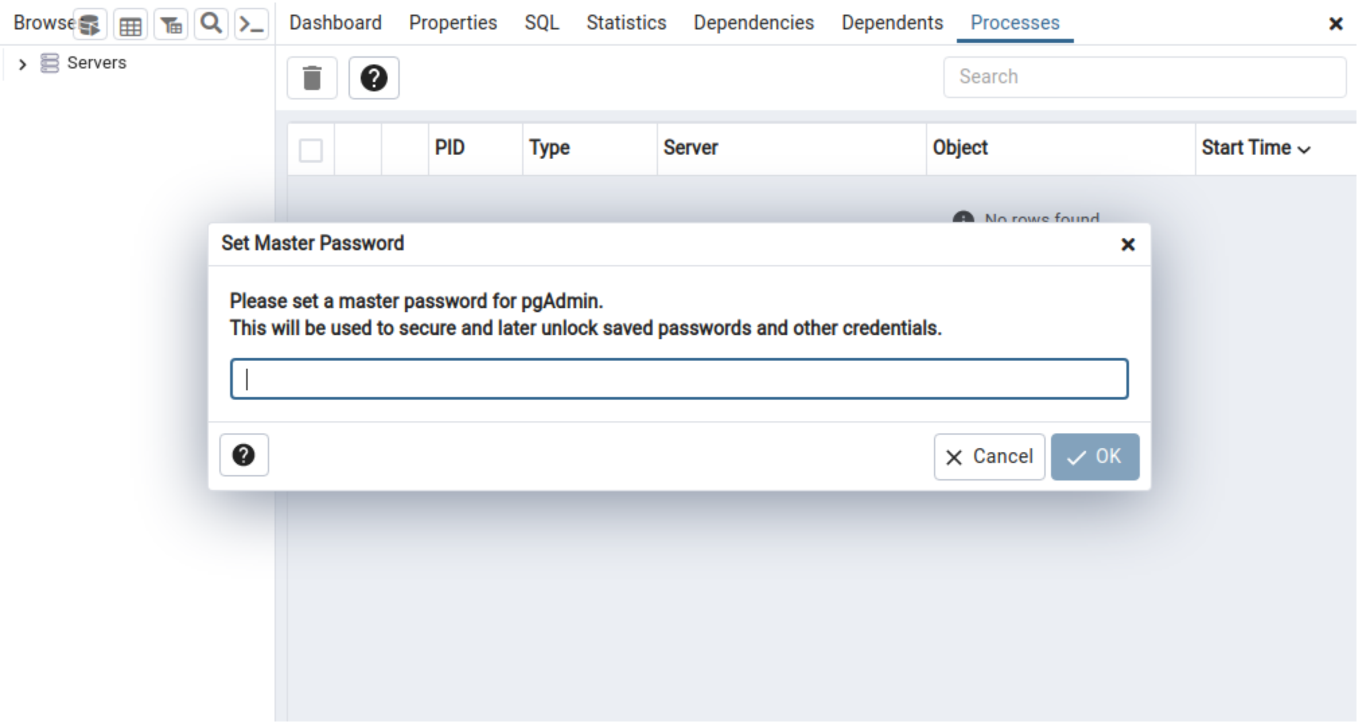
To install `pgAdmin4` on `Linux`, run the following commands:

mayala@htb[/htb]`$ curl -fsS https://www.pgadmin.org/static/packages_pgadmin_org.pub | sudo gpg --dearmor -o /usr/share/keyrings/packages-pgadmin-org.gpg $ sudo sh -c 'echo "deb [signed-by=/usr/share/keyrings/packages-pgadmin-org.gpg] https://ftp.postgresql.org/pub/pgadmin/pgadmin4/apt/$(lsb_release -cs) pgadmin4 main" > /etc/apt/sources.list.d/pgadmin4.list && apt update' $ sudo apt install pgadmin4`

Note: If you are using `Kali` or `ParrotOS` (like the `Pwnbox`), you will want to replace `$(lsb_release -cs)` in the second command with `bullseye`, otherwise the installation will fail.

To install `pgAdmin4` on `Windows` you can download the installer from pgadmin.org and follow the installation steps, or you can reuse the installer we used to install `psql.exe`, just make sure the `pgAdmin4` option is checked this time in the installation process.

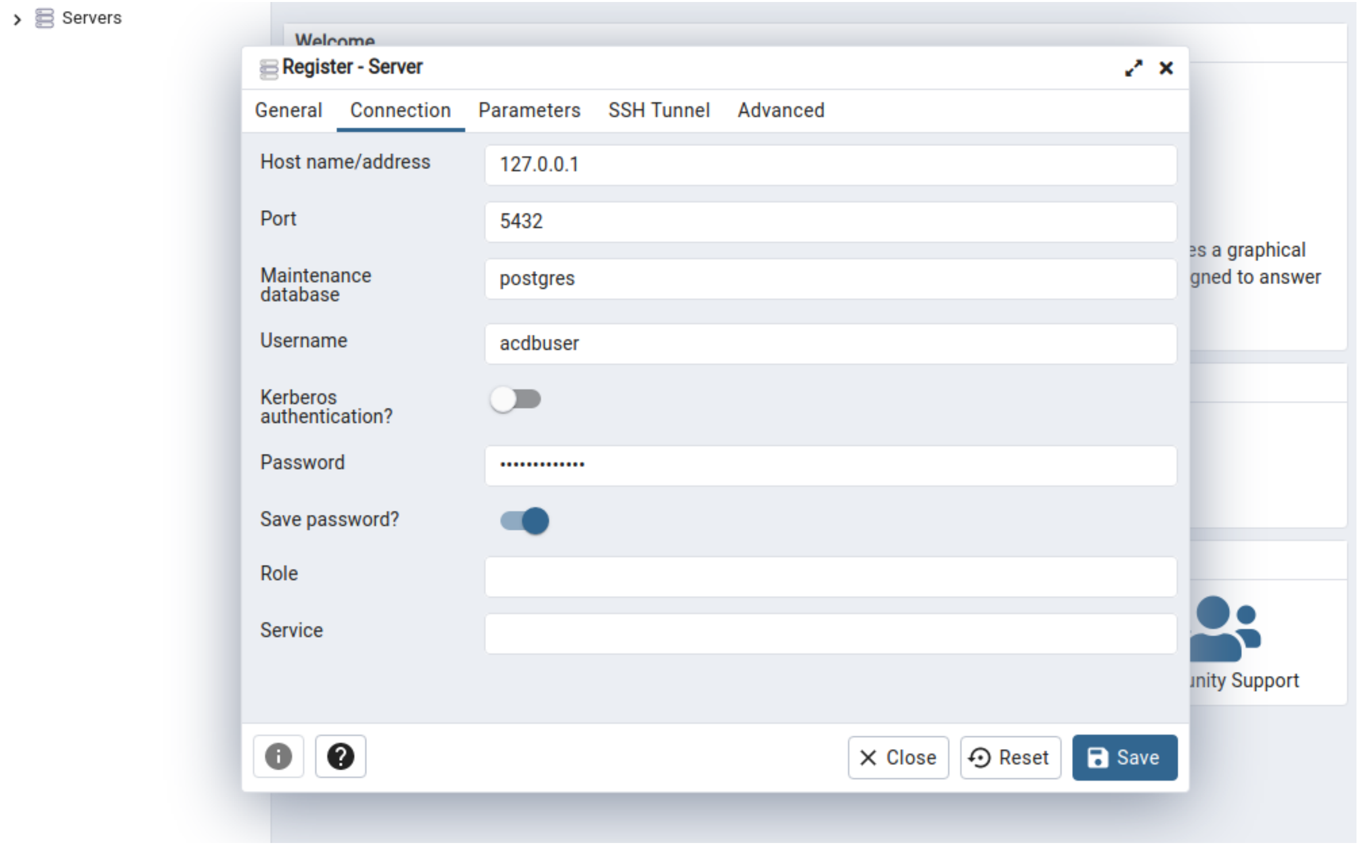
The first time you launch `pgAdmin4` you will have to set a master password. This is simply to protect the credentials you will later use to connect to databases.



Set Master Password

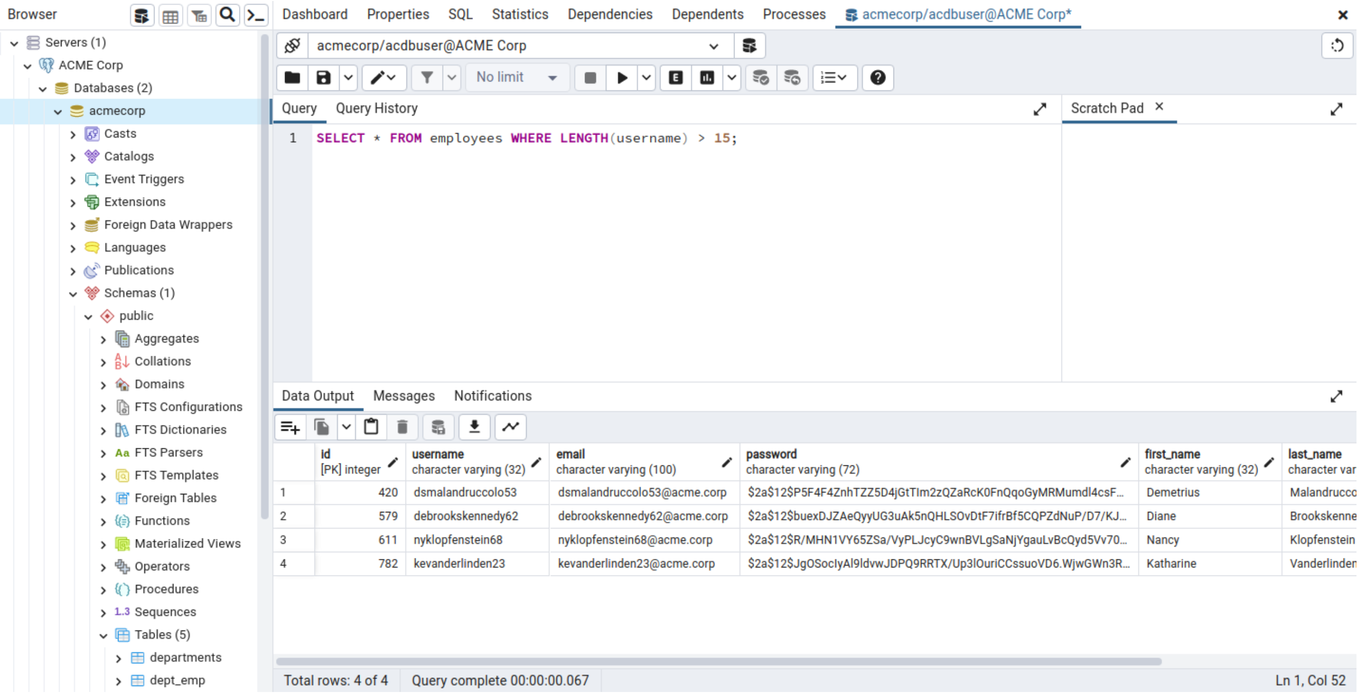
Please set a master password for pgAdmin.
This will be used to secure and later unlock saved passwords and other credentials.

To connect to a `PostgreSQL` server, go to `Dashboard > Add New Server`, fill out the details and press `Save`.



Host name/address	127.0.0.1
Port	5432
Maintenance database	postgres
Username	acdbuser
Kerberos authentication?	○
Password	•••••••••••••
Save password?	●
Role	
Service	

Once you've done that, you can access the `server` on the `left-hand side` under whatever name you chose. Viewing databases and tables is very intuitive with this graphic interface, and running queries is as simple as `right-clicking` on a `database` and selecting the `Query Tool`.



```
SELECT * FROM employees WHERE LENGTH(username) > 15;
```

	id [PK] integer	username character varying (32)	email character varying (100)	password character varying (72)	first_name character varying (32)	last_name character var
1	420	dsmalandruccolo53	dsmalandruccolo53@acme.corp	$2a$12$P5F4F4ZnhTZZ5D4jGtTIm2zQZaRcK0FnQqoGyMRMumdl4csF...	Demetrius	Malandrucco
2	579	debrookskennedy62	debrookskennedy62@acme.corp	$2a$12$buexDJZAeQyyUG3uAk5nQHLSOvDtF7ifrBf5CQPZdNuP/D7/KJ...	Diane	Brookskenne
3	611	nyklopfenstein68	nyklopfenstein68@acme.corp	$2a$12$R/MHN1VY65ZSa/VyPLJcyC9wnBVLgSaNjYgauLvBcQyd5Vv70...	Nancy	Klopfenstein
4	782	kevanderlinden23	kevanderlinden23@acme.corp	$2a$12$JgOSoclyAl9ldvwJDPQ9RRTX/Up3lOuriCCssuoVD6.WjwGWn3R...	Katharine	Vanderlinden

Total rows: 4 of 4 Query complete 00:00:00.067 Ln 1, Col 52

Practice

To finish off this section install `psql` or `pgAdmin4`, spawn and connect to the target database (`acmecorp`) with the credentials `acdbuser:AcmeCorp2023!`, and then answer the questions below.