Azure:

Database Elevate Privilege & Remote Code Execution

Platform:

Azure Database for PostgreSQL Flexible Server

Class:

Remote Code Execution

Summary:

I found a serious problem in extension anon, and anon is be allowed in azure.extensions. At first, anon will create function: anon.hash(text) which is security definer and the function's owner is superuser in azure; then the function calls digest(text,text) which belong to extensions pgcrypto and owner is me; Just by a tiny idea, I replace it with "alter role xxx with superuser" and execute anon.hash to become superuser. 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:

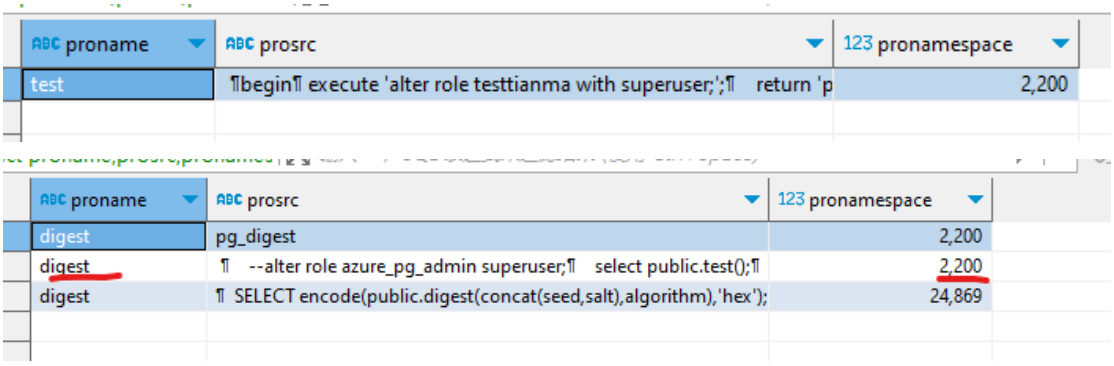
1. Create a flexiable server postgres database and connect it, then examine your roles.

rolname	rolsuper	rolinherit	rolcreaterole	rolcreatedb	rolcanlogin	rc
azuresu	[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]	[ ]	[ ]	[ ]	
replication	[ ]	[v]	[ ]	[ ]	[v]	
testtianma	[ ]	[ ]	[v]	[v]	[v]	
pg_read_all_settings	[ ]	[v]	[ ]	[ ]	[ ]	
pg_stat_scan_tables	[ ]	[v]	[ ]	[ ]	[ ]	
azure_pg_admin	[ ]	[v]	[ ]	[ ]	[ ]	

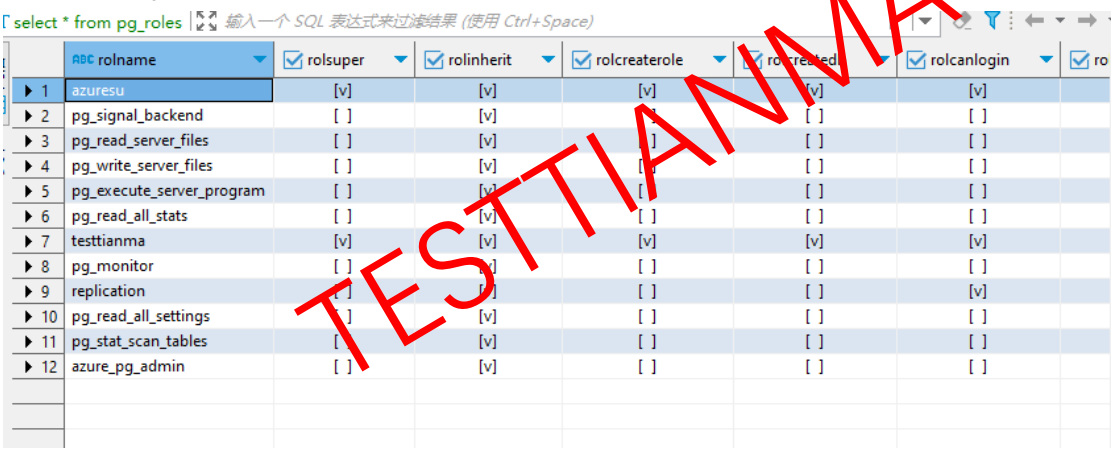
2. Grant the create privilege about extension anon,pgcrypto and it's shared liabary.

   az postgres flexible-server parameter set --resource-group xxx --server-name xxxxx --name azure.extensions --value anon,pgcrypto

3. First, create extension pgcrypto at public. Then replace public.digest(text,text) and create a test function elevate privilege sql to be called.



4. With anon extension create at public, we can use “select anon.hash('11');” to become superuser!



5. As a superuser, we can do more with the help of some postgres functions. We can compile a so with functions which contains system() call, 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, like ifconfig, whoami and cat xxx.