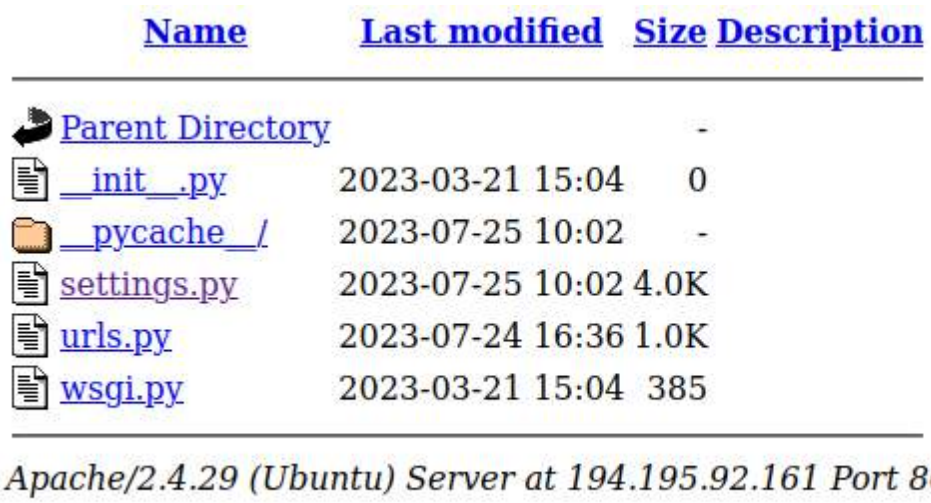
Gelosa Matteo esercizio W10D1

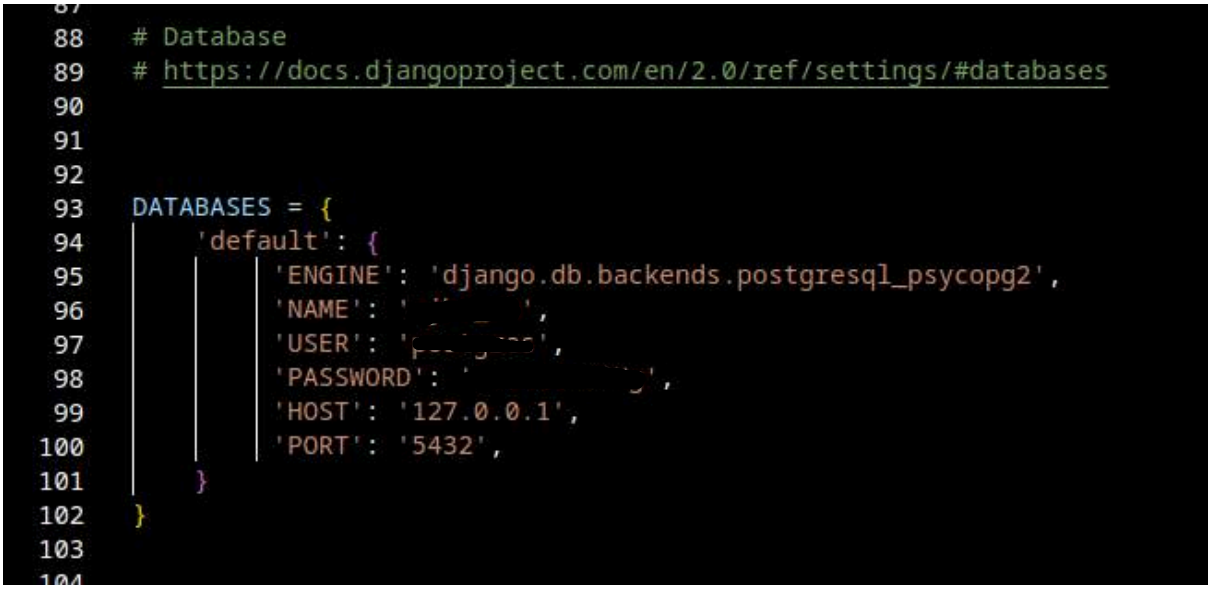
In questo esercizio ho utilizzato i comandi di Google Hacking per verificare vulnerabilità online, in particolare i siti web.
Il comando che più mi ha incuriosito è stato “intitle:index of settings.py”
Digitando questo comando sono riuscito a navigare nelle directory del sito web e sono stato in grado di trovare il file settings.py.



Name	Last modified	Size	Description
Parent Directory		-	
__init__.py	2023-03-21 15:04	0	
__pycache__/	2023-07-25 10:02	-	
settings.py	2023-07-25 10:02	4.0K	
urls.py	2023-07-24 16:36	1.0K	
wsgi.py	2023-03-21 15:04	385	

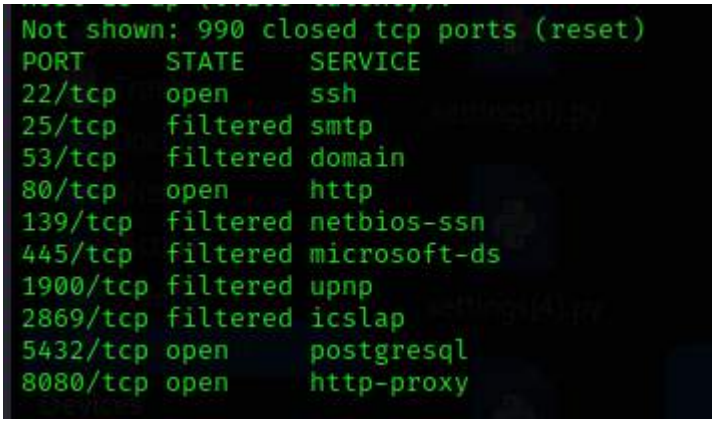
Apache/2.4.29 (Ubuntu) Server at 194.195.92.161 Port 80

Successivamente ho scaricato il file ed aprendolo con il mio editor di testo ho notato infinite informazioni che ovviamente non andrebbero rese pubbliche.
Quello che più mi ha colpito è stato vedere in chiaro la password, nome utente e nome database.



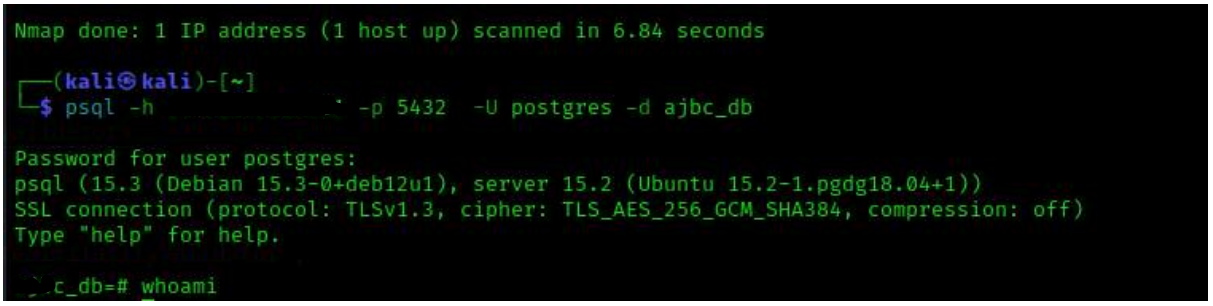
```
88  # Database
89  # https://docs.djangoproject.com/en/2.0/ref/settings/#databases
90
91
92
93  DATABASES = {
94      'default': {
95          'ENGINE': 'django.db.backends.postgresql_psycopg2',
96          'NAME': '[redacted]',
97          'USER': '[redacted]',
98          'PASSWORD': '[redacted]',
99          'HOST': '127.0.0.1',
100         'PORT': '5432',
101     }
102 }
103
```

Per curiosità ho eseguito uno scan con nmap all'indirizzo del sito web per vedere le porte in ascolto ed un eventuale database in funzione.

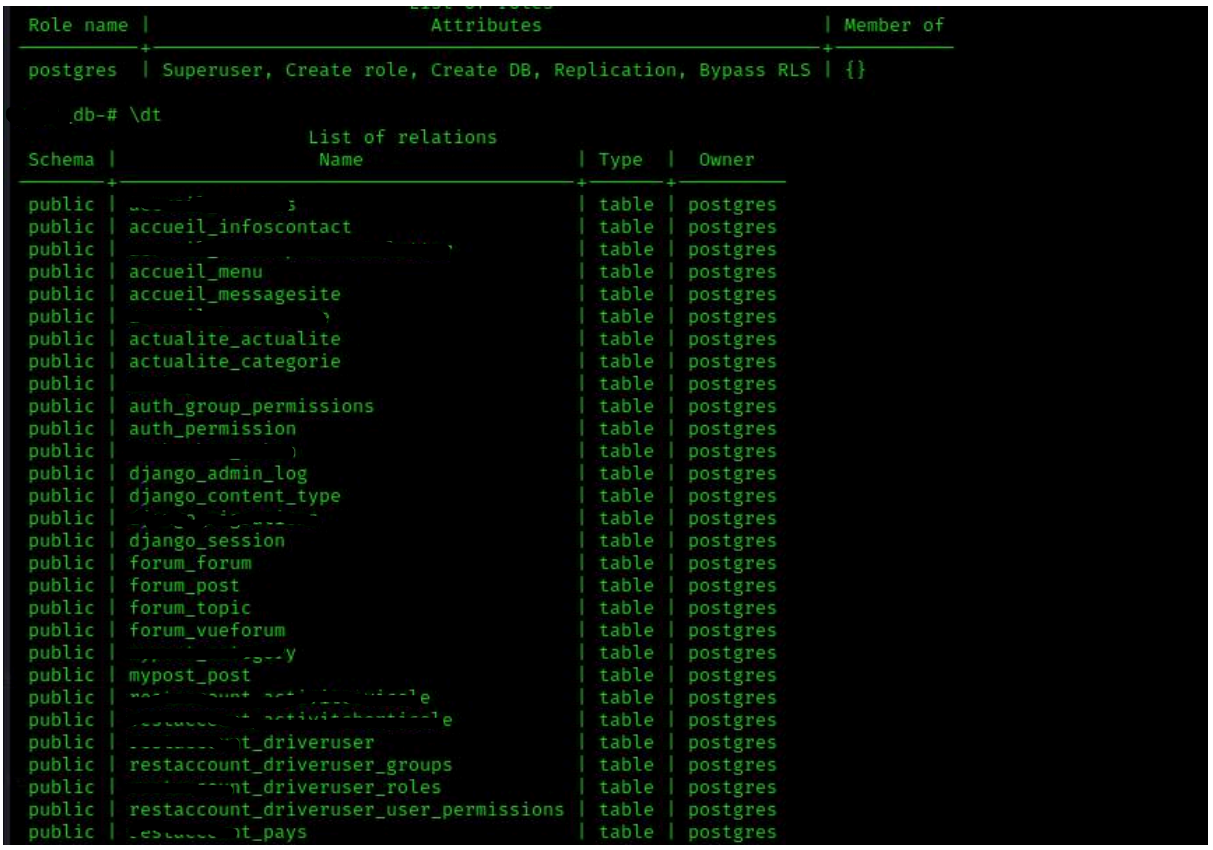


Come si può notare sulla porta 5432 è presente il database POSTGRESQL.

Ho provato ad accedere con le informazioni presenti nel codice ed effettivamente sono riuscito ad entrare.



Successivamente ho provato a navigare nelle cartelle del database e scaricare qualche file per visualizzarlo.



```
 Role name |                         Attributes                         | Member of
-----------+------------------------------------------------------------+-----------
 postgres  | Superuser, Create role, Create DB, Replication, Bypass RLS | {}

    db-# \dt
                    List of relations
 Schema |                  Name                   | Type  |  Owner
--------+-----------------------------------------+-------+----------
 public |                                         | table | postgres
 public | accueil_infoscontact                    | table | postgres
 public |                                         | table | postgres
 public | accueil_menu                            | table | postgres
 public | accueil_messagesite                     | table | postgres
 public |                                         | table | postgres
 public | actualite_actualite                     | table | postgres
 public | actualite_categorie                     | table | postgres
 public |                                         | table | postgres
 public | auth_group_permissions                  | table | postgres
 public | auth_permission                         | table | postgres
 public |                                         | table | postgres
 public | django_admin_log                        | table | postgres
 public | django_content_type                     | table | postgres
 public |                                         | table | postgres
 public | django_session                          | table | postgres
 public | forum_forum                             | table | postgres
 public | forum_post                              | table | postgres
 public | forum_topic                             | table | postgres
 public | forum_vueforum                          | table | postgres
 public |                                         | table | postgres
 public | mypost_post                             | table | postgres
 public |                                         | table | postgres
 public |                                         | table | postgres
 public |                                         | table | postgres
 public | restaccount_driveruser_groups           | table | postgres
 public |                                         | table | postgres
 public | restaccount_driveruser_user_permissions | table | postgres
 public |                                         | table | postgres
```

Ecco un file scaricato in formato csv visualizzato sul mio editor di testo :