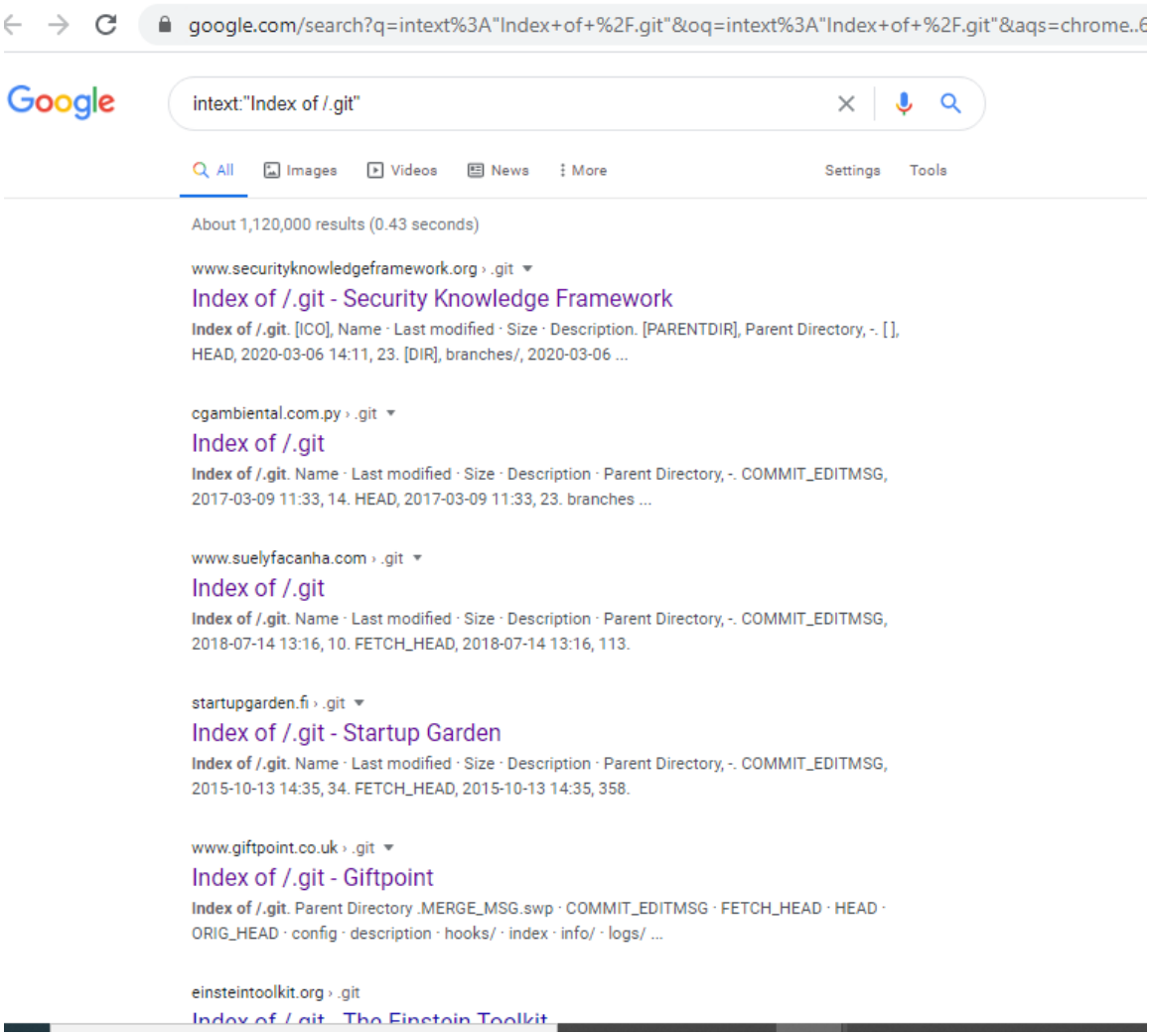
Git یک سیستم کنترل نسخه[1] است که در توسعه‌ی اکثر اپلیکیشن‌ها از آن استفاده می‌شود. فولدر git. نباید در دسترس عموم قرار بگیرد ولی برخی از وب‌سایت‌ها ناآگاهانه این فولدر را در دسترس عموم قرار می‌دهند. این فولدر شامل source code وب‌سایت و همه‌ی نسخه‌های قبلی آن است. دسترسی به source code یک اپلیکیشن، شناسایی آسیب‌پذیری‌های آن اپلیکیشن و exploit کردن آن‌ها را آسان‌تر می‌کند. اطلاعاتی مانند ساختار کد، library هایی که استفاده شده و جزئیات دیگر به attacker ها کمک می‌کنند تا راحت‌تر کار خود را انجام دهند. علاوه بر این، اطلاعات حساس مانند پسورد دیتابیس‌ها هیچ‌گاه نباید در یک سیستم کنترل نسخه که در دسترس عموم است ذخیره شود ولی برخی از developer ها این اطلاعات حساس را در دایرکتوری‌های Git ذخیره می‌کنند. در چنین حالتی اگر آن‌ها فولدر git. وب‌سایت خود را expose کنند، همه می‌توانند به آن اطلاعات حساس دسترسی پیدا کنند!

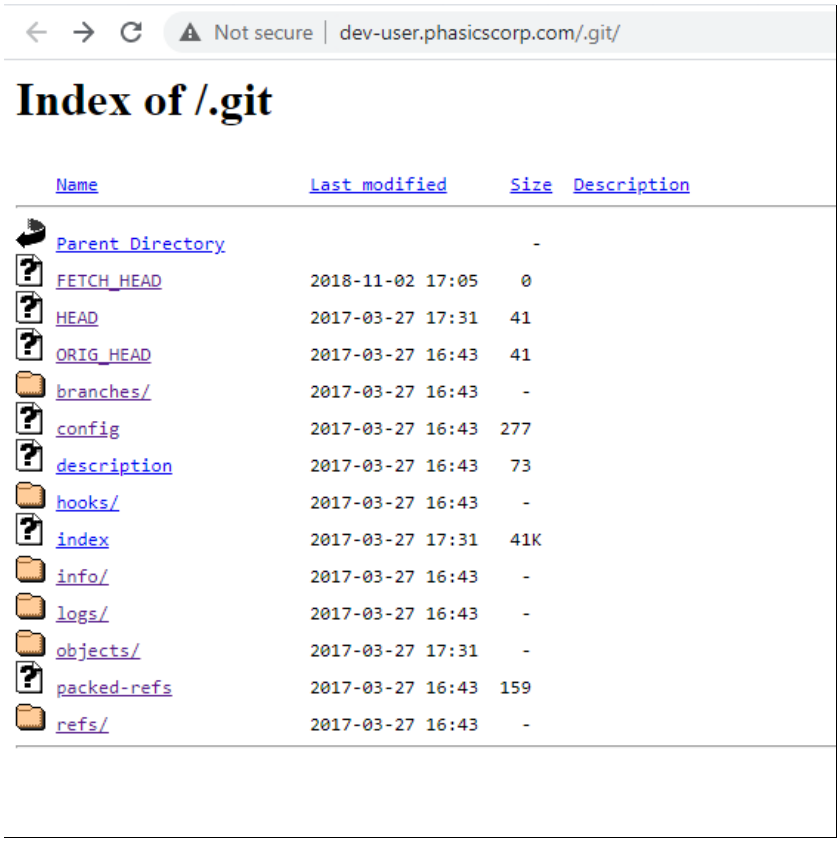
برای اینکه بفهمیم که یک وب‌سایت مشخص مثلاً example.com، فولدر git. خود را expose کرده است یا خیر کافی است example.com/.git را جستجو کنیم.

ما برای پیدا کردن وب‌سایت‌هایی که git. خود را expose کرده‌اند از Google Dork استفاده کردیم. عملگر intext وب‌سایت‌هایی که عبارت مشخصی را در body خود دارند، پیدا می‌کند. در تصویر زیر لیستی از وب‌سایت‌هایی که فولدر git. خود را در دسترس عموم قرار داده‌اند مشاهده می‌کنید:

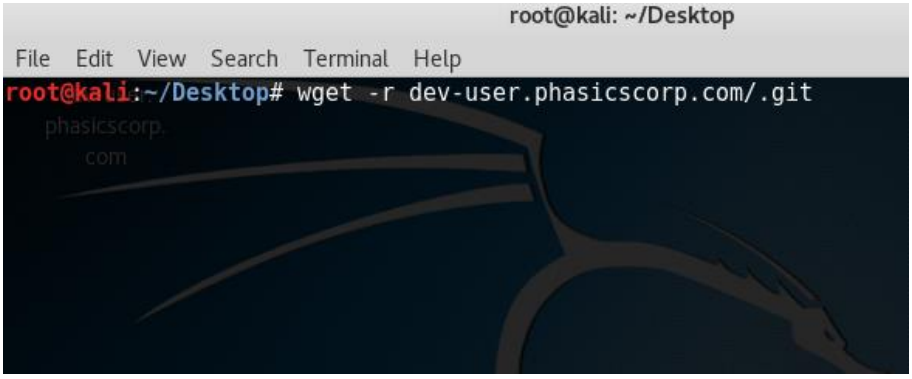
[1] Version control system (VSC)



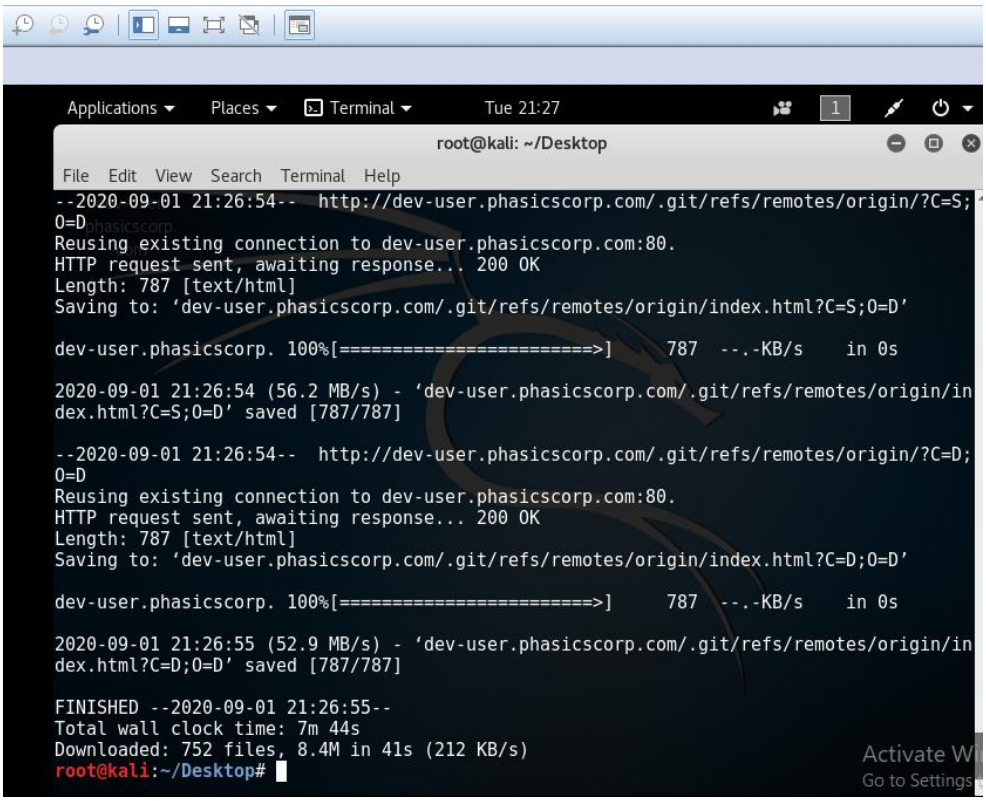
ما یکی از این وب‌سایت‌ها را انتخاب کردیم. محتوای دایرکتوری .git. این وب‌سایت را در تصویر زیر مشاهده می‌کنید:



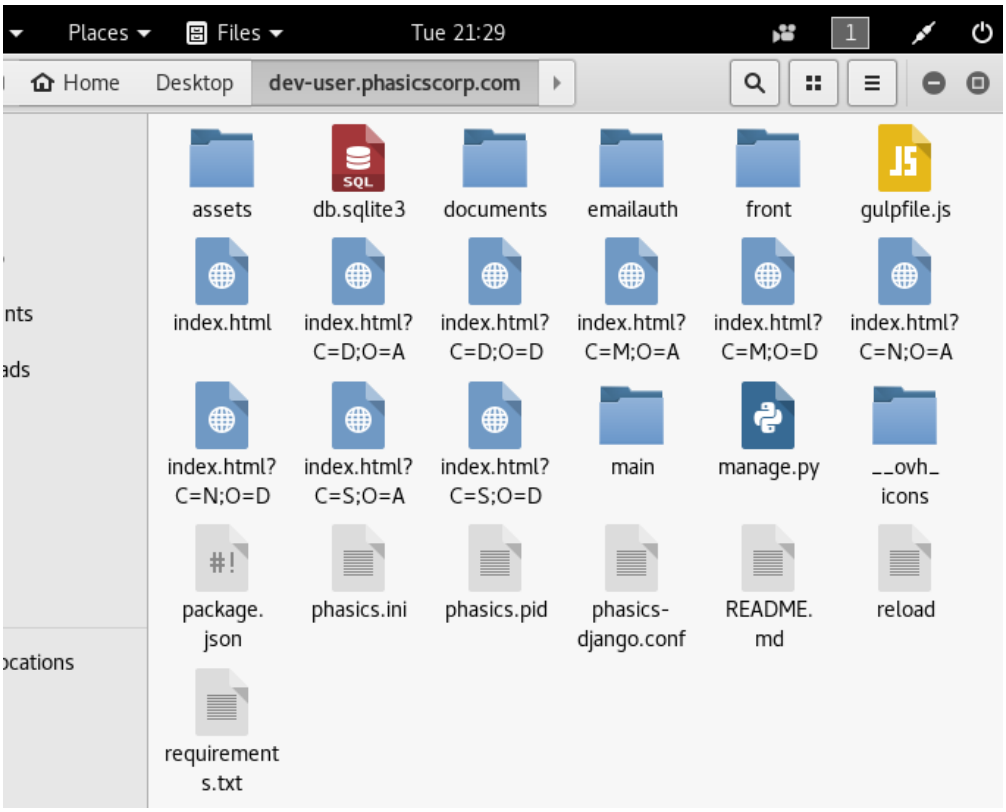
با دستور زیر می‌توان محتوای دایرکتوری git. این وب‌سایت را به دست آورد:



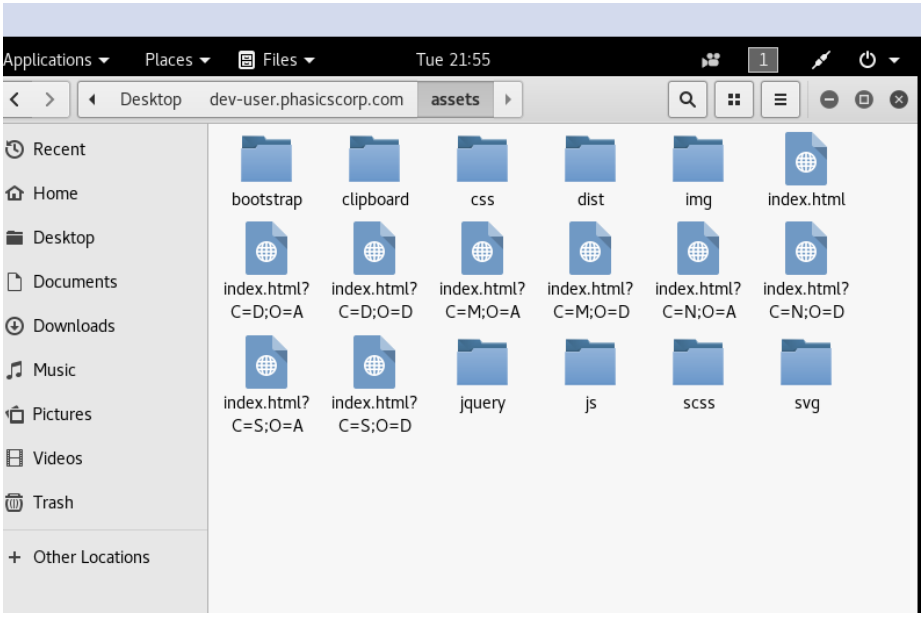
در اینجا ما از دستور wget در مد recursive استفاده کردیم تا محتوای وب‌سایت dev-user.phasicscorp.com را دانلود کنیم.

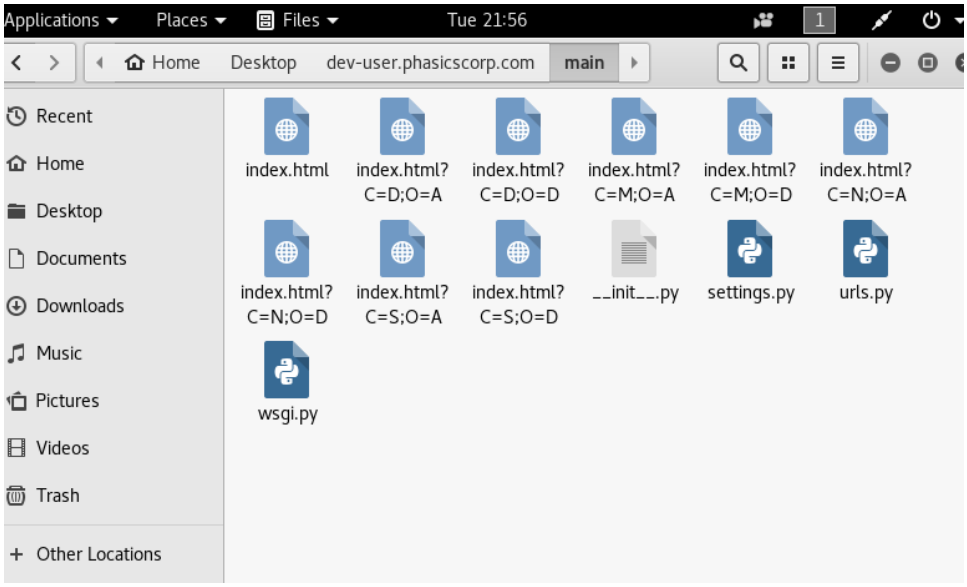


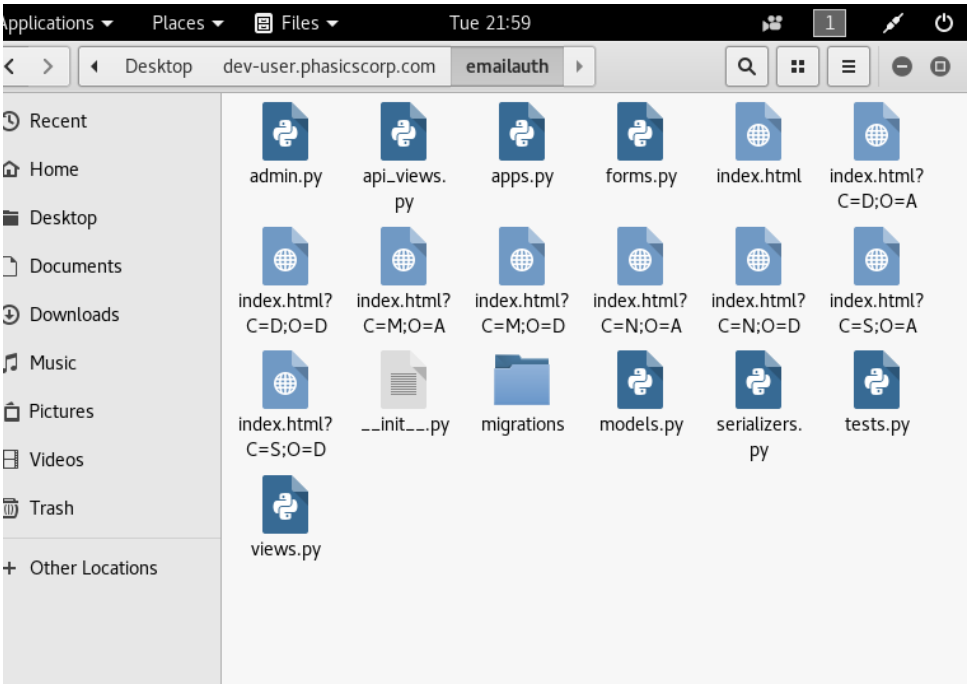
محتوای دانلود شده را می‌توانید در تصویر زیر مشاهده کنید:



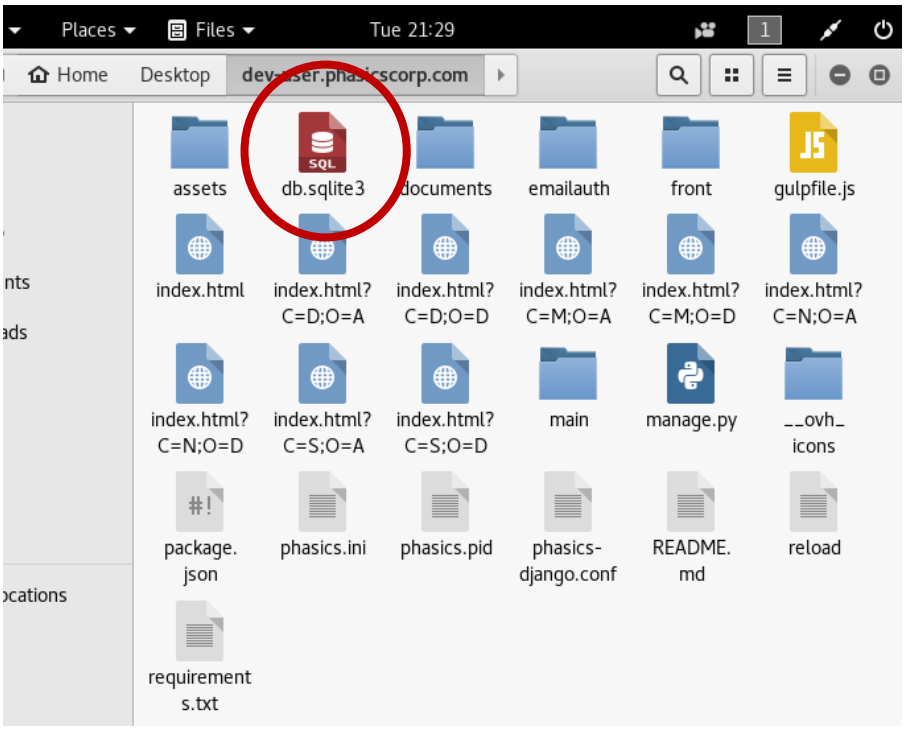
همان‌گونه که مشاهده می‌کنید ما توانستیم کل source code وب‌سایت را به دست بیاوریم. تصاویری از برخی از زیردایرکتوری‌ها:

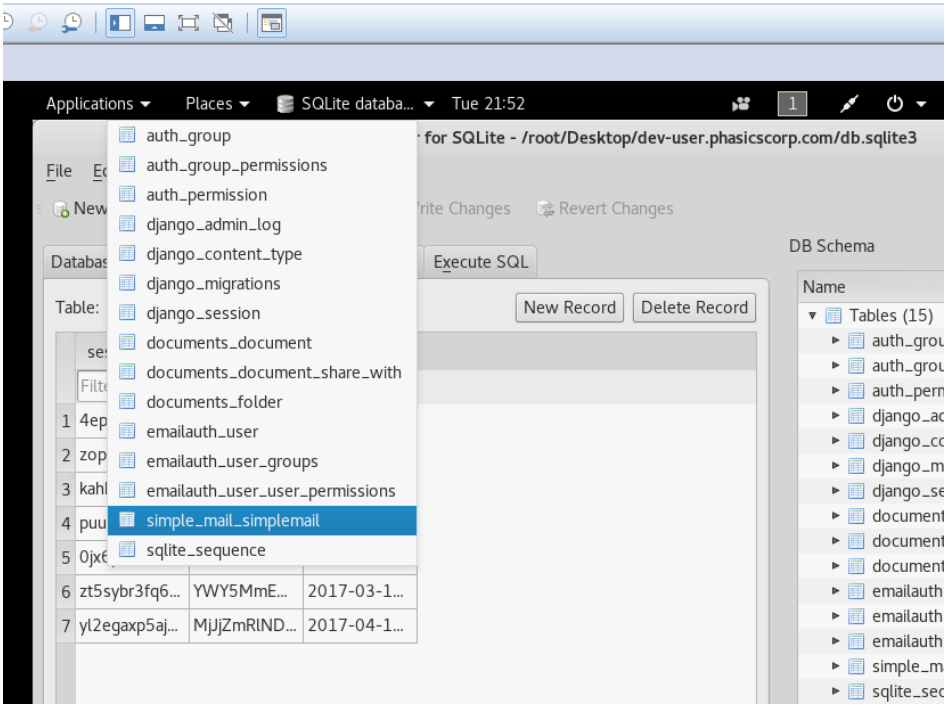


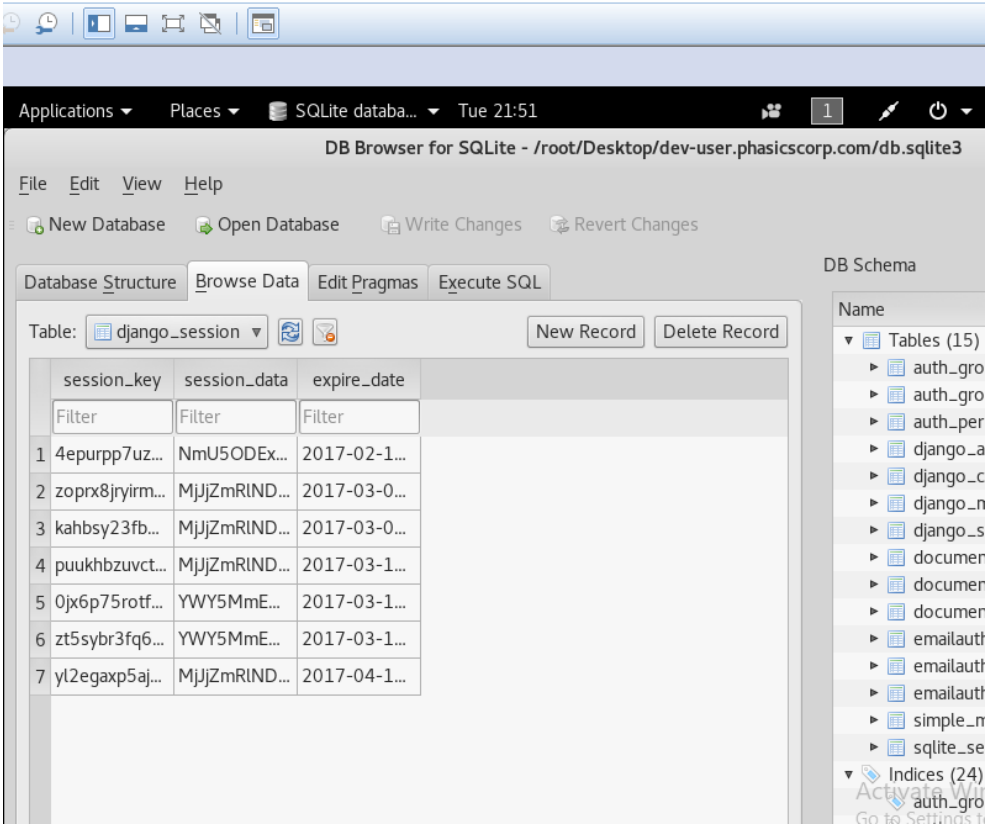




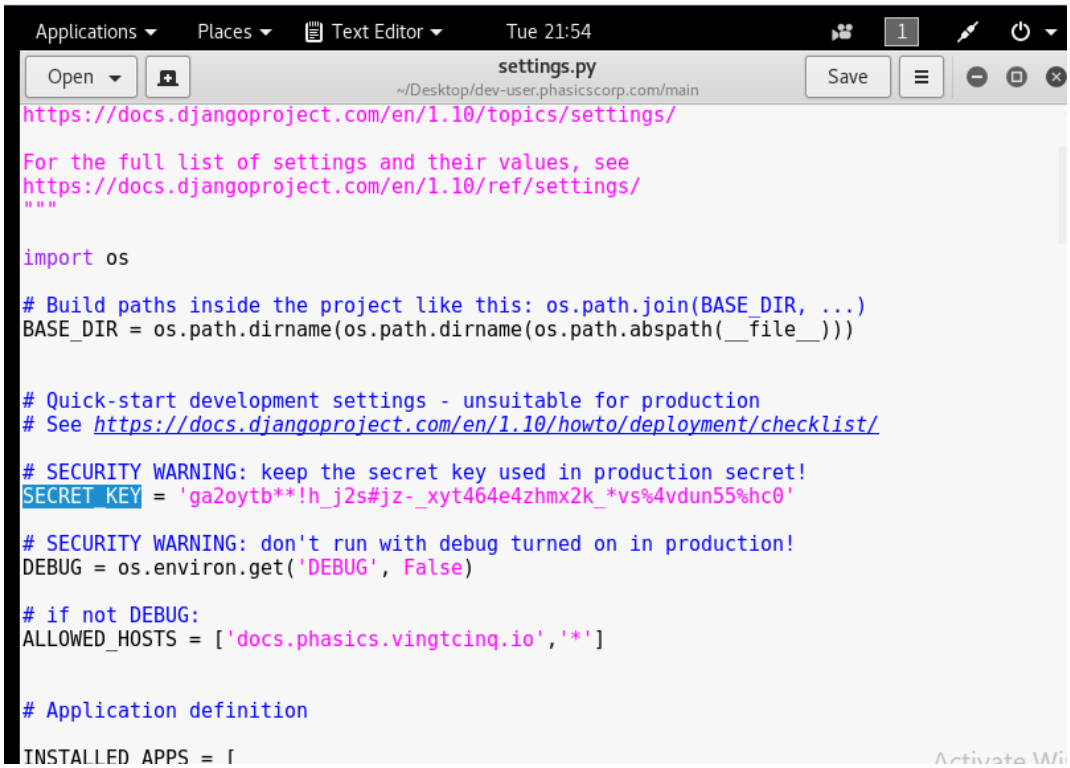
ما حتی به دیتابیس هم دسترسی داریم:



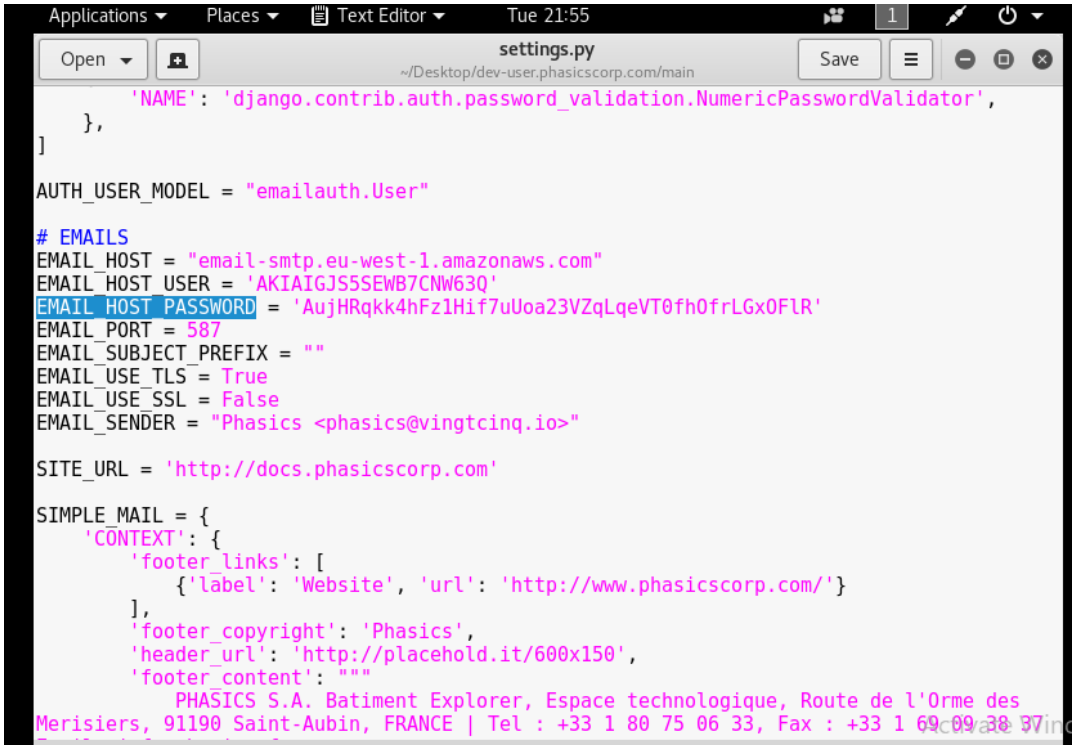




ما به تمامی اطلاعات دسترسی داریم حتی اطلاعات حساس:




```
https://docs.djangoproject.com/en/1.10/topics/settings/

For the full list of settings and their values, see
https://docs.djangoproject.com/en/1.10/ref/settings/
"""

import os

# Build paths inside the project like this: os.path.join(BASE_DIR, ...)
BASE_DIR = os.path.dirname(os.path.dirname(os.path.abspath(__file__)))


# Quick-start development settings - unsuitable for production
# See https://docs.djangoproject.com/en/1.10/howto/deployment/checklist/

# SECURITY WARNING: keep the secret key used in production secret!
SECRET_KEY = 'ga2oytb**!h_j2s#jz-_xyt464e4zhmx2k_*vs%4vdun55%hc0'

# SECURITY WARNING: don't run with debug turned on in production!
DEBUG = os.environ.get('DEBUG', False)

# if not DEBUG:
ALLOWED_HOSTS = ['docs.phasics.vingtcinq.io','*']


# Application definition

INSTALLED_APPS = [
```




```
        'NAME': 'django.contrib.auth.password_validation.NumericPasswordValidator',
    },
]

AUTH_USER_MODEL = "emailauth.User"

# EMAILS
EMAIL_HOST = "email-smtp.eu-west-1.amazonaws.com"
EMAIL_HOST_USER = 'AKIAIGJS5SEWB7CNW63Q'
EMAIL_HOST_PASSWORD = 'AujHRqkk4hFz1Hif7uUoa23VZqLqeVT0fhOfrLGxOFlR'
EMAIL_PORT = 587
EMAIL_SUBJECT_PREFIX = ""
EMAIL_USE_TLS = True
EMAIL_USE_SSL = False
EMAIL_SENDER = "Phasics <phasics@vingtcinq.io>"

SITE_URL = 'http://docs.phasicscorp.com'

SIMPLE_MAIL = {
    'CONTEXT': {
        'footer_links': [
            {'label': 'Website', 'url': 'http://www.phasicscorp.com/'}
        ],
        'footer_copyright': 'Phasics',
        'header_url': 'http://placehold.it/600x150',
        'footer_content': """
            PHASICS S.A. Batiment Explorer, Espace technologique, Route de l'Orme des
Merisiers, 91190 Saint-Aubin, FRANCE | Tel : +33 1 80 75 06 33, Fax : +33 1 69 09 38 37
```