



Open Source Assistant for #OSINT

<https://github.com/datasploit/datasploit>

<http://datasploit.info> | @datasploit

```
[shubhammittal:// $ whoami
```

- Just another Pen-tester.
- Security Consultant @ NotSoSecure
- 5+ Years of Experience

- Twitter - @upgoingstar
- Email - upgoingstaar@gmail.com

What's DataSploit?

- Automated OSINT Tool for Domain / Email / Username / IP Addresses
 - Fetches information from multiple HIDDEN sources.
 - Works in passive mode.
 - Written in Python.
 - Multiple report formats available.
-
- Customized for Pen-testers / Product Security Guys / Cyber Investigators.

Why DataSploit?

- So much data.
 - Server's Username / Passwords
 - Address
 - Email Id
 - Phone Number
 - Credentials
 - Interests
 - Friends
 - Preferences
 - Legacy Machines
 - Unnecessary Ports Information
 - Technologies in use, and blah blah..

Lets talk real time? History?

Well, you see it coming. What I found within 30 minutes was really stunning:

- 6 AWS access keys with their secret tokens
- 3 MongoDB connection URI (with login and password)
- 1 Twitter API credentials
- 1 Twilio API credentials
- 1 GitHub account credentials
- 1 Gmail account credentials
- And 1 Ravello Systems account credentials

Removed credentials

master

committed 9 days ago

Showing 1 changed file with 5 additions and 5 deletions.

```
10 group_vars/all
1 # Ravello's Credentials
2 -username: [REDACTED]@redhat.com
3 -password: [REDACTED]
4 -bucket: [REDACTED]
5
```

June 25, 2015

Study: Leaked credentials on P...
linked to 47 gov't agencies



credentials leaked site:pastebin.com

All Images News Videos Maps More Settings Tools

About 1,140 results (0.40 seconds)

Leaked Steam Credentials <3 - Pastebin.com

pastebin.com/cDQX04AQ

Leaked Steam Credentials <3. a guest Jul 3rd, 2015 262 Never. Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

Philippine Information Agency Full Credentials Leaked - Pastebin.com

pastebin.com/TWuKVS95

Dec 28, 2013 - Philippine Information Agency Complete User Credentials Leaked. Website: http://news.pia.gov.ph. Country: Philippines. Database: pianews.

FULL INSTAGRAM DATABASE LEAKED 2017 - Pastebin.com

pastebin.com/R6VfmHrJ

Jan 27, 2017 - Whether or not the leaked Instagram credentials are authentic, it never hurts to change ... Searches related to Instagram database leak ...

25+ Leaked TWC Account Login Credentials - **NEW MAY 2016 ...

pastebin.com/5tiyxT3E

25+ Leaked TWC Account Login Credentials - **NEW MAY 2016**. a guest May 25th, 2016 284 Never ... Leaked by: xjkn3rX. Full Dump: COMMENCED ...

Leaked User Credentials of Nice Print Photography & PIAP PH ...

pastebin.com/gy8HsgHE

Leaked User Credentials of Nice Print Photography & PIAP PH. a guest Oct 11th, 2015 1,230 Never. Not a member of Pastebin yet? Sign Up, it unlocks many ...

TWITTER LEAKED DATABASE NEW ...

Components

- Domain Osint
- Email Osint
- IP Osint
- Username Osint

- WIP
 - Company Scoping
 - Phone Number OSINT
 - Active Modules

Sources and Flow

Domain:

WhoIS
DNS Records
PunkSpider
Wappalyzer
Github
Email Harvester
Domain IP History
Paste(s) Search
Pagelinks
Wikileaks
Links from Forums
Passive SSL Scan
ZoomEye
Shodan
Censys
Subdomains



Email:

Basic Email Checks
Work History
Social profiles
Enumerated Usernames
Location Information
Slides
Scribd Documents
Related Websites
HaveIBeenPwned



Username:

Git Details
Check username on various sites.
Profile Pics –Output saved in
\$username directory
Frequent Hashtags
Interaction on Twitter.

Active Modules

Setting it up..

- Manual

- Download from git (git clone or download)
git clone <https://github.com/DataSploit/datasploit.git>
- pip install -r requirements.txt
- config.py holds API keys
- **domain_xyz.py** – running stand alone scripts.
- **domainOsint / emailOsint / ipOsint** – automated OSINT
- active_scan.py

- Automated

- <https://hub.docker.com/r/appsecco/datasploit/>
- <https://hub.docker.com/r/ftorn/datasploit/>

Documentation.

<https://datasploit.github.io/datasploit/>

<https://datasploit.github.io/datasploit/apiGeneration/>

How to Generate Api Keys

Search

datasploit
931 Stars

DataSploit
Overview
Setting up the Environment
[How to Generate Api Keys](#)
Usage
Contributors

How to Generate Api Keys

We need following API keys to run this tool efficiently. - shodan_api - censysio_id - censysio_secret - zoomeyeuser - zoomeyepass - clearbit_apikey - emailhunter - fullcontact - google_cse_key - google_cse_cx

Shodan_api

- [Register](#) an account in shodan.
- Visit your registered email id and activate the account.
- [Login](#) to your account and you will find the API keys under profile overview tab.
- Copy the API key and this is the value for *shodan_api* field in the config.py file.

Censysio ID and Secret

- [Register](#) an account in censysio.
- Visit your registered email id and activate the account.
- [Login](#) to your account.
- Visit [Account](#) tab to get API ID and Secret.
- Your API key is the value for *censysio_id* field and API Secret is the value for *censysio_secret* field in config.py file.

Clearbit API

- [Register](#) an account in clearbit.
- It will auto redirect to the account.

Table of contents
Shodan_api
Censysio ID ar
Clearbit API
Emailhunter A
Fullcontact AF
Google Custor
API key and C
Zoomeye User
Password

<https://datasploit.github.io/datasploit/setupGuide/>

Setting up the Environment

Search

DataSploit
Overview
[Setting up the Environment](#)
How to Generate Api Keys
Usage
Contributors

Setting up the Environment

This page holds the setup guide you will need before kicking off the datasploit in your system. Please note that all the documentation is as per *nix machines, and the tool has not been thoroughly tested on Windows platform. If you would like to volunteer for the same, give us a shout at helpme@datasploit.info. Following are the quick steps to get you going:

If you want to work with web gui, follow the steps till 7. Otherwise, follow till 5th and you should be good to go.

Step 1 - Download DataSploit to your system.

You can either use the git command line tools using the following command:

```
git clone https://github.com/datasploit/datasploit.git
```

, or you can simply download the zip file ([link](#)) and extract the same using unzip.

```
unzip master.zip
```

Step 2: Install python dependencies

Go into the tool directory and install all the python libraries using the requirements.txt file. In case you encounter 'Permission Denied' error, use sudo.

```
cd master  
pip install -r requirements.txt
```

Step 3: Rename config_sample.py to config.py

What's in there?

```
[shubhammittal:datasploit/ (master*) $ ls
```

Finding

License.txt

Payload.class

Presentations

README.md

active_default_file_check.py

badges

check_urls.txt

config.py

config.pyc

config_sample.py

contributors.txt

core

datasploit.py

dochelp

docs

domain0sint.py

domain_GooglePDF.py

domain_censys.py

domain_censys.pyc

domain_checkpunkspider.py

domain_checkpunkspider.pyc

domain_dnsrecords.py

domain_dnsrecords.pyc

domain_emailhunter.py

domain_emailhunter.pyc

domain_forumsearch.py

domain_forumsearch.pyc

domain_github.py

domain_github.pyc

domain_history.py

domain_history.pyc

domain_pagelinks.py

domain_pagelinks.pyc

domain_pastes.py

domain_pastes.pyc

domain_shodan.py

domain_shodan.pyc

domain_sslinfo.pyc

domain_subdomains.py

domain_subdomains.pyc

domain_wappalyzer.py

domain_wappalyzer.pyc

domain_whois.py

domain_whois.pyc

domain_wikileaks.py

domain_wikileaks.pyc

domain_zoomeye.py

domain_zoomeye.pyc

email0sint.py

email0sint.pyc

email_basic_checks.py

email_basic_checks.pyc

email_fullcontact.py

email_fullcontact.pyc

email_pastes.py

email_pastes.pyc

generate_passwords.py

hbp.py

ip0sint.py

ip_asn.pyc

ip_shodan.py

ip_shodan.pyc

ip_whois.py

ip_whois.pyc

mkdocs.yml

requirements.txt

roadmap.txt

temptweets.txt

test.py

test_domain0sint.py

testhtml.html

testreg.py

upgoingstar

username0sint.py

username_gitscrape.py

username_reddit.py

Output Formats

- HTML
- JSON
- Emails List (txt file)
- Subdomains List (txt file)

DataSploit

Report for mailchimp.com

WHOIS Information

```
{
  "updated_date": [
    "2016-01-19 00:00:00",
    "2017-03-05 15:25:01"
  ],
  "status": [
    "serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited",
    "serverTransferProhibited https://icann.org/epp#serverTransferProhibited"
  ],
  "name": "ROCKET SCIENCE GROUP",
  "dnssec": "Unsigned",
  "city": "ATLANTA",
  "expiration_date": [
    "2018-06-29 00:00:00",
    "2018-06-29 04:00:00"
  ]
}
```

A Records

23.51.136.95

MX Records

1 aspmx.l.google.com.
10 aspmx3.googlemail.com.
5 alt1.aspmx.l.google.com.
10 aspmx2.googlemail.com.
5 alt2.aspmx.l.google.com.

SOA Records

beaker.ma
develop
inspirat
mail.adm
pizza.ma
qa.mailc
sc1.mail
st1.mail
st2.mail
stx.mail
stxv2.ma
wavelengt
modev1.ma
old-kb.ma
mailchimp
slgw.mail
fastfives
fb101.ma
fb102.ma

file:///Users/shubhammittal/Documents/Pythoncodes/datasplit_parent/datasplit/reports/mailchimp.com/mailchimp.com_2017

```
{'wappalyzer': {'http': [u'tGoogle Analytics', u'tGoogle Tag Manager'], 'https': [u'tGoogle Analytics', u'tGoogle Ta  
9f58  
u'30  
12-3  
Leng  
u'lo  
29T2  
u'<h  
u'lo  
{u'o  
u'pr  
u'de  
301  
stat  
u'po  
u'ti  
bgco  
6166  
u'82  
'city': u'Denver', u'region_code': u'CA', u'area_code': 404, u'longitude': -84.283, u'country_code': u'USA', u'country_name': u'United Sta
```

hello@ma
legal@ma
abuse@ma
laurissa
imports@
talent@
mobilehe
pr@mailc
colors@
dan@mail
john@mai
gregg@ma
help@mai
shirts@
wordpres
tara.sha
shopify@
support@
info@mai
api@mail
apibeta@
ecommerc
contact@
examples
template
customer
domains@
kate@mai
twitter@
accounts
agencies
whatsins
apiconne
tedx@mai
biz@mail
salesfor
dev@mail
apihelp@

DEMO TIME

**LET'S HOPE THE DEMO-GODS ARE
SMILING!**

Twitter:

@datasploit

<https://twitter.com/datasploit>

<https://twitter.com/datasplit>

Home
Notifications
Messages

DataSplit

Open Source Assistant for #OSINT

TWEETS
196

FOLLOWING
110

FOLLOWERS
406

LIKES
25

datsploit

@datsploit · FOLLOWS YOU

Open Source Assistant for #OSINT

github.com/upgoingstar/da...

Joined July 2016

Tweet to

Message

20 Followers you know

Photos and videos

Tweets
 Tweets & replies
 Media

datasplit Retweeted

amticker.de @amtickerde · 12h
 Collection Of Open Source Intelligence Resources
[amticker.de/collection-of-...](#) #amtickerde

Collection Of Open Source Intelligence Resources - ...

Wichtige Informationen zum Thema Collection Of Open Source Intelligence Resources. Besuche unsere Seite noch heute!

[amticker.de](#)

datasplit Retweeted

Shashank shekhar @Shankywit · 5h
 3 Advantages of Using an Open Source Business Intelligence Tool
[paper.li/Shankywit/1465...](#) Thanks to @_crowdreviews_#businessintelligence

Facebook: /datasploit

<https://www.facebook.com/datasploit/>

Browser address bar: <https://www.facebook.com/datasploit/?fref=ts>

Navigation bar: Cloud, The Configuration Sy, SensePost | Revistin, Offensive Security B, Python Tools : Penet, Encoding Web Shells, enjoiz/XXEinjector: T, Rapport d'au

Facebook header: DataSploit, Search, Shubham, Home 20+, Settings, Help

Page navigation: Page, Messages, Notifications, Insights, Publishing Tools

DataSploit profile card: DataSploit, Open Source Assistant for #OSINT

DataSploit post: Published by Twitter [?] · August 1 at 4:43pm · Retweeted Ahmed AlHamli (@AhmedAlHamli): Big Data and open source intelligence – A game-changer for counter-terrorism? <https://t.co/cHZO7SeZGu>

Image: World map with user icons and binary code

Text: Big Data and open source intelligence – A game-changer for counter-terrorism? | TRENDS

Text: The threat from terrorism continues to present a clear and present danger to many communities across the world. The suicide bombings in Turkey on 28th June which...

Text: TRENDSINSTITUTION.ORG/?P=2019

13 people reached

Boost Post

Like, Comment, Share

DataSploit post: Published by Twitter [?] · August 1 at 4:43pm · Retweeted Steven Hager (@stevenhager420): A Brief History of Open Source Intelligence - bellincat <https://t.co/uzzyAKAtrM>

PHOTOS: DataSploit Overview, DataSploit Open Source Assistant for #OSINT

UPCOMING EVENTS: Create events for your Page. Create Event

VISITOR POSTS: Be the first to add a post

Roadmap

- Allows to set up periodic scans and alerting for product security companies.
- Intelligence on co-relation and identity verification.
- Reports in CSV.
- Reverse Image Search and profile validation.
- Works closely with various social network APIs.
- Refine Pastebin and Github Searches.
- IP Threat Intelligence.
- Organization Scoping.
- Integration with SE other tools.
- Cloud related OSINT and active modules.
- `pip install datasplit` (to be installed as both library as well as script)

Coverage



CircleCityCon 4.0

OSINT Framework



How to Contribute

- Help us in testing the tool
- Expand : Write/Suggest modules
- Give Feedback: raise issues, tweet, drop an email.
- Use / Promote / Write about the tool.
- Write OSINT blogs / tool walkthrough(s) / etc.
- Report issues at <https://github.com/dataspl0it/dataspl0it/issues>

Core Contributors.

- Shubham Mittal (@upgoingstar)
- Nutan Kumar Panda (@nutankumarpanda)
- Sudhanshu (@sudhanshu_c)
- Kunal (@KunalAggarwal92)
- Kudos to
 - @anantshri for mentoring.
 - @ bnchandrapal for feedbacks, suggestions and other help around issues.

Thanks. g0t questions?

<https://github.com/DataSploit/datasploit>

Follow [@datasploit](#) for OSINT news and latest updates.

Tweet / DM to **@datasploit**

upgoingstaar@gmail.com

