

The background is a dark blue gradient with a subtle pattern of white dots. Overlaid on this are several faint, light blue technical diagrams. These include circular gauges with numerical scales (e.g., 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260) and arrows indicating movement. There are also circular paths with arrows and a central circular logo featuring the GitHub Octocat silhouette. The title 'GITHUB RECON' is centered in a large, white, sans-serif font.

GITHUB RECON

By Mohamed Sayed

AGENDA

- Introduction to GitHub
- GitHub Importance For PenTesters
- GitHub Dorks
- Reach unpublished employees
- Manual vs Automated Approach

INTRODUCTION TO GITHUB

<> Edit new file

Preview

```
1 < CODE >
2 // by mohammed
3
4 < CODE >
5 // by ahmed|
```

GitHub is a code hosting platform for version control and collaboration. It helps you and others to work together on projects from anywhere

developers stores their projects into repositories

GITHUB IMPORTANCE FOR PENTESTERS

Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere?
[Import a repository.](#)

Owner *



MohamedSayed458 ▾

Repository name *

secret repository ✓

Great repository names are short and **descriptive**. Your new repository will be created as **secret-repository**. **adventure?**

Description (optional)

This Repository Contains Secret Credentials and API keys



Public

Anyone on the Internet can see this repository. You choose who can commit.



Private

You choose who can see and commit to this repository.

developers may make a mistake and store a projects which contains an api key or credentials or credit cards in public rather than private repository

GITHUB SEARCH

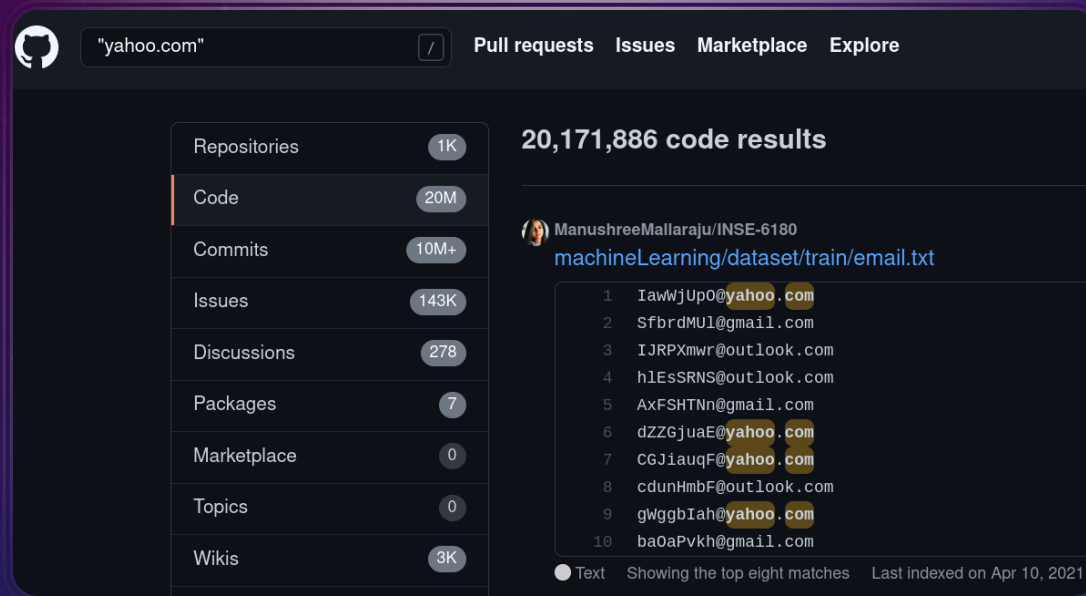
Mainly, as a pentester, I will use github to gather information about my target just by search in github

"company" || "company.com" || "company.net", etc

Be Creative! Minimize your search domain

- Make use of your gathered information
- Stackoverflow - You may see parts of the source code of target website or at least know the backend programming lang.
- Linkedin - Take a look at the technology they are using (firewall, vpn, programming lang)

GITHUB SEARCH



The screenshot shows the GitHub search interface with the query "yahoo.com". The left sidebar lists various categories: Repositories (1K), Code (20M), Commits (10M+), Issues (143K), Discussions (278), Packages (7), Marketplace (0), Topics (0), and Wikis (3K). The main area displays "20,171,886 code results". A specific result is highlighted, showing a file path "machineLearning/dataset/train/email.txt" by user "ManushreeMallaraju/INSE-6180". Below this, a list of email addresses is shown, with several containing "yahoo.com". At the bottom, it indicates "Showing the top eight matches" and "Last indexed on Apr 10, 2021".

Category	Count
Repositories	1K
Code	20M
Commits	10M+
Issues	143K
Discussions	278
Packages	7
Marketplace	0
Topics	0
Wikis	3K

20,171,886 code results

ManushreeMallaraju/INSE-6180
machineLearning/dataset/train/email.txt

- 1 IawWjUpO@yahoo.com
- 2 SfbrdMUl@gmail.com
- 3 IJRPXmwr@outlook.com
- 4 h1EsSRNS@outlook.com
- 5 AxFSHTNn@gmail.com
- 6 dZZGjuaE@yahoo.com
- 7 CGJiauqF@yahoo.com
- 8 cdunHmbF@outlook.com
- 9 gwggbiAh@yahoo.com
- 10 ba0aPvkh@gmail.com

● Text Showing the top eight matches Last indexed on Apr 10, 2021

Not all results will be belong to the company itself, you may find some results that belongs to random people.

To get a sensitive information you have to use a specific words

(password, credentials, secret_key .. etc)

COMMON KEY WORDS

- "company" security_credentials --> LDAB (AD)
- "company" connectionstring --> DB Credentials
- "company" JDBC --> DB Credentials
- "company" ssh2_auth_password --> Unauthorized access to server

<https://github.com/random-robbie/keywords/blob/master/keywords.txt>

SENSITIVE RESULTS

Jdbc or connetionstring

```
1 import pypyodbc as pyodbc # you could alias
2 db_host = 'mspitsql15.test.th3g3nt31.org'
3 db_name = 'BISE'
4 db_user = 'empDS'
5 db_password = 'Seattle@98121'
```

```
1         'bundles',
2         r'',
3         )
4 ftp_th3g3nt31 = ftp('ftp.th3g3nt31man.com',
5         'ASbd5FD',
6         'AB$1B#6mAk1HH',
7         info('->Start to upload to th3g3nt31.ftp<-')
8 ftpcli = ftp(ftp_th3g3nt31)
```

ftp

ADVANCED USAGE

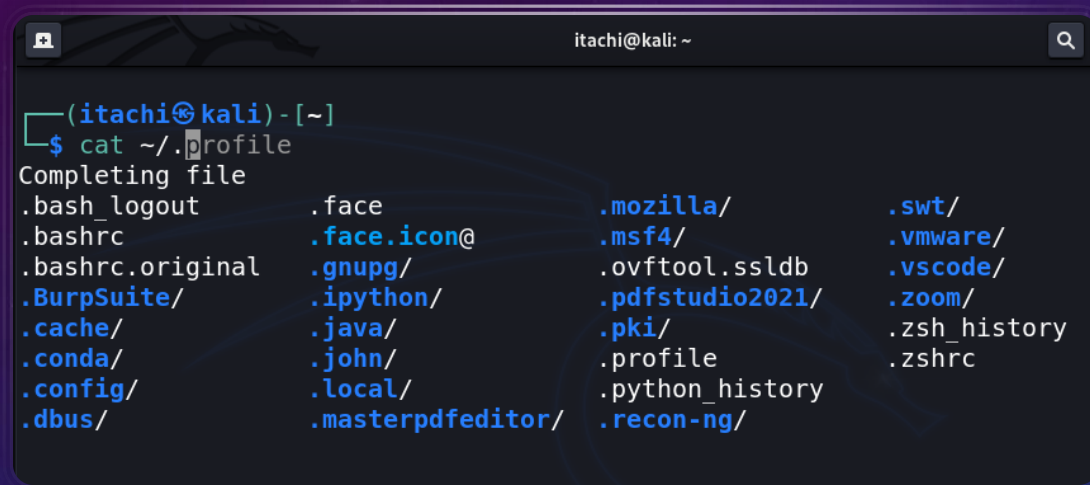
- "company" language:python security_credentials
- "company" language:bash
- NOT "Something to exclude"
- "yahoo.com" language:python security_credentials NOT "blabla.yahoo.com"
- user:<certain user> security_credentials

<https://docs.github.com/en/search-github/getting-started-with-searching-on-github/understanding-the-search-syntax#exclude-certain-results>

DEMO

- "evilcorp.com" (840 results)
- "evilcorp.com" language:python (20 result)
- "evilcorp.com" language:bash
- "evilcorp.com" mysql
- "evilcorp.com" mysql NOT root@evilcorp.com
- "evilcorp.com" dotfiles
- "evilcorp.com" user:MohamedSayed458

DOTFILES

A terminal window titled 'itachi@kali: ~' showing the output of the command 'cat ~/.profile'. The output lists various dotfiles and directories in a four-column format. The files include .bash_logout, .bashrc, .bashrc.original, .BurpSuite/, .cache/, .conda/, .config/, .dbus/, .face, .face.icon@, .gnupg/, .ipython/, .java/, .john/, .local/, .masterpdfeditor/, .mozilla/, .msf4/, .ovftool.sslldb, .pdfstudio2021/, .pki/, .profile, .python_history, .recon-ng/, .swt/, .vmware/, .vscode/, .zoom/, .zsh_history, and .zshrc.

```
(itachi@kali)-[~]  
$ cat ~/.profile  
Completing file  
.bash_logout      .face              .mozilla/          .swt/  
.bashrc            .face.icon@       .msf4/             .vmware/  
.bashrc.original  .gnupg/           .ovftool.sslldb    .vscode/  
.BurpSuite/        .ipython/         .pdfstudio2021/    .zoom/  
.cache/           .java/            .pki/              .zsh_history  
.conda/           .john/            .profile            .zshrc  
.config/          .local/           .python_history  
.dbus/            .masterpdfeditor/ .recon-ng/
```

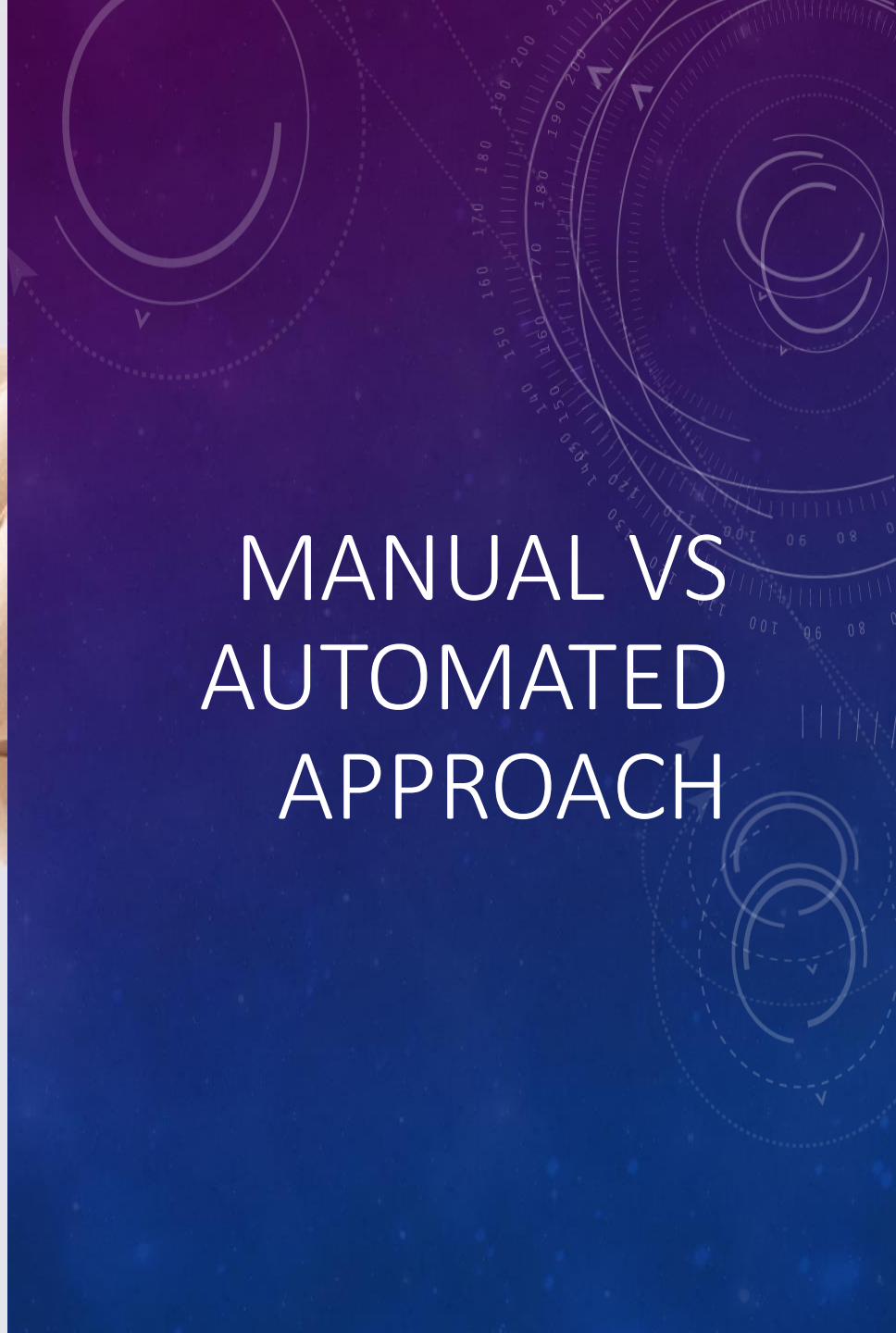
- Many computer software programs store their configuration settings in plain, text-based files or directories.
- Dotfiles are configuration files for various programs, and they help those programs manage their functionality.

REACH UNPUBLISHED EMPLOYEES

1. "company" dotfiles
2. use linkedin to make sure that he is an employee
3. search in that employee repositories user:<certain user> security_credentials



MANUAL VS AUTOMATED APPROACH



AUTOMATED APPROACH

Accessing an organization

- Search in its repositories
- Get published employees

Search in employees repositories



THANK YOU!
