GitHub Digging By @Alwali

⋮ 30/09/2022

Sep 30, 2022

5 min read
dorking bug-bounty

- 🖨️Employees of The Company

  Google : `site:github.com inurl:”org=company”`

  GitHub : `org:company`

- ® Docker Registry Authentication Data

  https://github.com/Plazmaz/leaky-repo/tree/master/.docker

  ```
  org:company filename:.dockercfg

  org:company docker AND auth AND email

  user:name filename:.dockercfg

  user:name docker AND auth AND email

  "[company.com](http://company.com/)" docker AND auth AND email
  ```

- 🈂️ Web Server Credentials

  https://github.com/Plazmaz/leaky-repo/blob/master/.idea/WebServers.xml

  ```
  org:company filename:webservers.xml

  org:company fileTransfer AND pass

  user:name filename:webservers.xml

  user:name fileTransfer AND pass

  "[company.com](http://company.com/)" fileTransfer AND pass
  ```

- 🔑 Firefox Saved Password Collection

  https://github.com/Plazmaz/leaky-repo/blob/master/.mozilla/firefox/logins.json

  ```
  org:company filename:firefox/logins.json
  ```

```
org:company encryptedUsername encryptedPassword

user:name filename:firefox/logins.json

user:name encryptedUsername encryptedPassword

"[company.com](http://company.com/)" encryptedUsername encryptedPassword
```

- 🔑 Private SSH Key

  https://github.com/Plazmaz/leaky-repo/tree/master/.ssh

  ```
  org:company filename:.ssh/id_rsa

  org:company "BEGIN RSA PRIVATE KEY" OR ssh-rsa

  user:name filename:.ssh/id_rsa

  user:name "BEGIN RSA PRIVATE KEY" OR ssh-rsa

  "[company.com](http://company.com/)" "BEGIN RSA PRIVATE KEY" OR ssh-rsa
  ```

- 🐍 SFTP OR SSH Server Credentials

  https://github.com/Plazmaz/leaky-repo/blob/master/.vscode/sftp.json `org:company filename:sftp.json org:company host AND pass`

  ```
  user:name filename:sftp.json

  user:name host AND pass

  "[company.com](http://company.com/)" host AND pass
  ```

- S3 Credentials ".credentials"

  https://github.com/Plazmaz/leaky-repo/blob/master/cloud/.credentials

  ```
  org:company filename:.credentials

  org:company aws_secret_access_key OR aws_secret_key

  user:name filename:.credentials

  user:name aws_secret_access_key OR aws_secret_key

  "[company.com](http://company.com/)" aws_secret_access_key aws_secret_key
  ```

- S3 Credentials ".s3cfg"

  https://github.com/Plazmaz/leaky-repo/blob/master/cloud/.s3cfg

  ```
  org:company filename:.s3cfg
  ```

```
org:company secret_key

user:name filename:.s3cfg

user:name secret_key

"[company.com](http://company.com/)" secret_key
```

- 🌊 Digital Ocean Tugboat Config

  https://github.com/Plazmaz/leaky-repo/blob/master/cloud/.tugboat

```
org:company filename:.tugboat

org:company authentication AND api_key

user:name filename:.tugboat

user:name authentication AND api_key

"[company.com](http://company.com/)" authentication AND api_key
```

- 😖 Heroku Config

  https://github.com/Plazmaz/leaky-repo/blob/master/cloud/heroku.json

```
org:company filename:heroku.json

org:company HEROKU_API_KEY OR HEROKU_KEY

user:name filename:heroku.json

user:name HEROKU_API_KEY OR HEROKU_KEY

"[company.com](http://company.com/)" HEROKU_API_KEY OR HEROKU_KEY
```

- 🗃️ PostgreSQL File Contains Passwords

  https://github.com/Plazmaz/leaky-repo/blob/master/db/.pgpass

  org:company filename:.pgpass

  org:company :database:

  user:name filename:.pgpass

  user:name :database:

  “company.com” :database:

- 🔑 DBEAVER Config Containing Credentials

  https://github.com/Plazmaz/leaky-repo/blob/master/db/dbeaver-data-sources.xml

```
org:company filename:dbeaver-data-sources.xml

org:company connection AND jdbc

user:name filename:dbeaver-data-sources.xml

user:name connection AND jdbc

"[company.com](http://company.com/)" connection AND jdbc
```

- 🥟 MYSQL Hashes Dump

  https://github.com/Plazmaz/leaky-repo/blob/master/db/dump.sql

```
org:company filename:dump.sql

org:company "MySQL dump" AND "INSERT INTO”

user:name filename:dump.sql

user:name "MySQL dump" AND "INSERT INTO”

"[company.com](http://company.com/)" "MySQL dump" AND "INSERT INTO"
```

- 🗃️ MONGOID Config File

  https://github.com/Plazmaz/leaky-repo/blob/master/db/mongoid.yml

```
org:company filename:mongoid.yml

org:company production AND mongodb

user:name filename:mongoid.yml

user:name production AND mongodb

"[company.com](http://company.com/)" production AND mongodb
```

- 🛠️ MONGOLAB Credentials For ROBOMONGO

  https://github.com/Plazmaz/leaky-repo/blob/master/db/robomongo.json

```
org:company filename:robomongo.json

org:company userPassword AND serverHost

user:name filename:robomongo.json

user:name userPassword AND serverHost

"[company.com](http://company.com/)" userPassword AND serverHost
```

- 🥨 File Zilla config file

https://github.com/Plazmaz/leaky-repo/tree/master/filezilla

```
org:company filename:filezilla.xml

org:company FileZilla3 AND "Pass encoding”

user:name filename:filezilla.xml

user:name FileZilla3 AND "Pass encoding”

"[company.com](http://company.com/)" FileZilla3 AND "Pass encoding"
```

- 🔐 PEM Private key

  https://github.com/Plazmaz/leaky-repo/blob/master/misc-keys/cert-key.pem

  ```
  org:company filename:cert-key.pem

  user:name filename:cert-key.pem

  org:company "BEGIN PRIVATE KEY”

  user:name filename:cert-key.pem

  "[company.com](http://company.com/)" "BEGIN PRIVATE KEY"
  ```

- 🗝 PuTTY-gen Private Key

  https://github.com/Plazmaz/leaky-repo/blob/master/misc-keys/putty-example.ppk

  ```
  org:company filename:putty extension:ppk org:company PuTTY-User-Key-File
  user:name filename:putty extension:ppk user:name PuTTY-User-Key-File "
  [company.com](http://company.com/)" PuTTY-User-Key-File
  ```

- 🦹 Secret Key For Django Setup

  https://github.com/Plazmaz/leaky-repo/blob/master/web/django/settings.py

  ```
  org:company filename:settings.py org:company SECRET_KEY user:name
  filename:settings.py user:name SECRET_KEY "[company.com]
  (http://company.com/)" SECRET_KEY
  ```

- 🎥 Salesforce Credentials In A NodeJS Project

  https://github.com/Plazmaz/leaky-repo/blob/master/web/js/salesforce.js

  ```
  org:company filename:salesforce.js org:company "conn.login(" OR
  "require('jsforce')" user:name filename:salesforce.js user:name
  "conn.login(" OR " require('jsforce')" "[company.com]
  (http://company.com/)" "conn.login(" OR " require('jsforce')"
  ```

- 🚮 Credentials For Ruby on Rails

https://github.com/Plazmaz/leaky-repo/blob/master/web/ruby/secrets.yml

```
org:company filename:secrets.yml org:company secret_key_base user:name filename:secrets.yml user:name secret_key_base "[company.com](http://company.com/)" secret_key_base
```

- 📊 Credentials For Voice AND Chat Platforms

```
org:company filename:credentials.yml org:company slack_token OR access-token OR _TOKEN user:name filename:credentials.yml user:name slack_token OR access-token OR _TOKEN "[company.com](http://company.com/)" slack_token OR access-token OR _TOKEN
```

- ✋ Slack Token For Rocket-Chat

https://hackerone.com/reports/386614

```
org:company filename:.travis.yml org:company notification AND slack OR secure user:name filename:.travis.yml user:name notification AND slack OR secure "[company.com](http://company.com/)" notification AND slack OR secure
```

- Credentials For Laravel

https://github.com/Plazmaz/leaky-repo/blob/master/web/var/www/.env

```
org:company filename:.env org:company APP_KEY OR DB_PASS user:name filename:.env user:name APP_KEY OR DB_PASS "[company.com](http://company.com/)" APP_KEY OR DB_PASS
```

- 🎁 PHP Configuration File

https://github.com/Plazmaz/leaky-repo/blob/master/web/var/www/public_html/config.php

```
org:company filename:config.php org:company mysql_connect OR dbpass user:name filename:config.php user:name mysql_connect OR dbpass "[company.com](http://company.com/)" mysql_connect OR dbpass
```

- 📦 WordPress Configuration File

https://github.com/Plazmaz/leaky-repo/blob/master/web/var/www/public_html/wp-config.php

```
org:company filename:wp-config.php org:company DB_PASSWORD OR AUTH_KEY user:name filename:wp-config.php user:name DB_PASSWORD OR AUTH_KEY "[company.com](http://company.com/)" DB_PASSWORDt OR AUTH_KEY
```

- 📪 ESMTP Configuration File

https://github.com/Plazmaz/leaky-repo/blob/master/.esmtprc

```
org:company filename:.esmtprc org:company "hostname smtp" user:name
filename:.esmtprc user:name "hostname smtp" "[company.com]
(http://company.com/)" "hostname smtp"
```

- 🔐 SFTP OR SSH Server Credentials

  https://github.com/Plazmaz/leaky-repo/blob/master/.ftpconfig

  org:company filename:.ftpconfig org:company protocol AND ftp AND pass user:name filename:.ftpconfig user:name protocol AND ftp AND pass “company.com” protocol AND ftp AND pass

- ☪️ Contains SMTP Credentials

  https://github.com/Plazmaz/leaky-repo/blob/master/.netrc

  ```
  org:company filename:.netrc org:company machine AND login AND password
  user:name filename:.netrc user:name machine AND login AND password "
  [company.com](http://company.com/)" machine AND login AND password
  ```

- ® NPM Registry Authentication Data

  https://github.com/Plazmaz/leaky-repo/blob/master/.npmrc

  ```
  org:company filename:.npmrc org:company registry AND _auth OR _authToken
  user:name filename:.npmrc user:name registry AND _auth OR _authToken "
  [company.com](http://company.com/)" registry AND _auth OR _authToken
  ```

- 🦈 FTP , SFTP OR SSH Credentials

  https://github.com/Plazmaz/leaky-repo/blob/master/.remote-sync.json

  ```
  org:company filename:.remote-sync.json org:company "remote sync" AND pass
  user:name filename:.remote-sync.json user:name "remote sync" AND pass "
  [company.com](http://company.com/)" "remote sync" AND pass
  ```

- 🚒 IRC Configuration

  https://github.com/Plazmaz/leaky-repo/blob/master/config

  ```
  org:company filename:config org:company IRC_HOST AND IRC_PASS user:name
  filename:config user:name IRC_HOST AND IRC_PASS "[company.com]
  (http://company.com/)" IRC_HOST AND IRC_PASS
  ```

- 🕵️ Server Details AND Credentials

  https://github.com/Plazmaz/leaky-repo/blob/master/deployment-config.json

  ```
  org:company filename:deployment-config.json org:company type AND sftp AND
  pass user:name filename:deployment-config.json user:name type AND sftp
  ```

```
AND pass "[company.com](http://company.com/)" type AND sftp AND pass
```

- 🚧 Hub Configuration

  https://github.com/Plazmaz/leaky-repo/blob/master/hub

  ```
  org:company filename:hub oauth_token org:company [github.com]
  (http://github.com/) AND user AND oauth_token user:name filename:hub
  oauth_token user:name [github.com](http://github.com/) AND user AND
  oauth_token "[company.com](http://company.com/)" [github.com]
  (http://github.com/) AND user AND oauth_token
  ```

- 🚓 Ventrilo Configuration

  https://github.com/Plazmaz/leaky-repo/blob/master/ventrilo_srv.ini

  ```
  org:company filename:ventrillo_srv.ini org:company AdminPassword AND
  Password user:name filename:ventrillo_srv.ini user:name AdminPassword AND
  Password "[company.com](http://company.com/)" AdminPassword AND Password
  ```

- 🦝 Slack Token

  https://hackerone.com/reports/397527

  https://github.com/streaak/keyhacks#Slack-API-token

  ```
  org:company xoxp user:name token=xoxp user:name xoxp "[company.com]
  (http://company.com/)" xoxp org:company token=xoxp
  ```

- 🐓 JSON Web Token

  ```
  org:company .eyJ
  ```

  ```
  org:company Authorization OR JWT AND eyJ user:name .eyJ user:name
  Authorization OR JWT AND eyJ "[company.com](http://company.com/)"
  Authorization OR JWT AND eyJ
  ```

- 🧬 General Queries

  ```
  "Company" security_credentials "Company" connectionstring "Company"
  send_keys OR sendkeys "Company" consumerkey "Company" JDBC "Company"
  JIRA_Pass "Company" ssh2_auth_password "Company" ssh2_auth_password NOT
  string "Company" password OR pwd Search Github "Company" auth_key
  "Company" SSO_LOGIN "Company" secret_access_key "Company" bucket_password
  "Company" redis_password "Company" root_password "Company" _TOKEN OR _KEY
  ```

- 🛠️ Tools For Searching

  github-search/github-employees.py at master · gwen001/github-search

    - https://github.com/michenriksen/gitrob
    - https://github.com/zricethezav/gitleaks
    - https://github.com/dxa4481/truffleHog
    - https://github.com/obheda12/GitDorker
    - https://github.com/hisxo/gitGraber

      github-search/github-grabrepo.php at master · gwen001/github-search

      github-search/github-dorks.py at master · gwen001/github-search

- 🍖 Bonus

  AllAboutBugBounty/Github Dorks.md at master · daffainfo/AllAboutBugBounty

@sl4x0