Find Secret API-Keys

Aditya Soni Follow
Dec 22 · 3 min read

Hello everyone, it may be just another blog on how to find API keys, but here I'll try to give every Information about finding the secret API keys and how to use them to authenticate.

> *An **Application Programming Interface key** (**API key**) is a unique indentifier that is used to authenticate the incoming request and that program or user has known permissions for accessing the non-private user data.*

API keys can be found in multiple ways, but the simplest method would be visiting the GitHub page of the desired program or checking the source code.

But it can be a bit of time-consuming, so to save a lot of time. Here is a great tool I would recommend to use:

KeyFinder

momenbasel/keyFinder

keyFinder is chrome exstenion that searches the DOM for any embedd script link, as script tag may contain keys for...

github.com

It’s easy to install and use

1. Clone the repo or download it via https://github.com/momenbasel/keyFinder.git
2. Open Chrome and go to chrome://extensions
3. Enable “Developer Mode”
4. Drag and drop the KeyFinder folder

After installing KeyFinder successfully go-to the target website and Click on the keyFinder icon added on the top right corner of chrome and manually add some common keywords used to find API keys so that KeyFinder can crawl in the website and Find the keys. After visiting links, click on the result/s and there you can see the outcomes.

Now what? that’s the main question. API keys can be used to authenticate without the username and password of an individual.

Below are some ways in which particular API keys found on a Bug Bounty Program can be used to check if they are valid and can also be used to Account takeover or extract personal information from the API.

Slack API token

```
curl -sX POST "https://slack.com/api/auth.test?token=xoxp-
TOKEN_HERE&pretty=1"
```

Facebook Access Token

```
https://developers.facebook.com/tools/debug/accesstoken/?
access_token=ACCESS_TOKEN_HERE&version=v3.2
```

GitHub Token

```
curl -s -u "user:apikey" https://api.github.com/user
curl -s -H "Authorization: token TOKEN_HERE"
"https://api.github.com/users/USERNAME_HERE/orgs"
```

```
# Check scope of your api token
curl "https://api.github.com/rate_limit" -i -u "user:apikey" | grep
"X-OAuth-Scopes:"
```

Twitter API Secret

```
curl -u 'API key:API secret key' --data
'grant_type=client_credentials'
'https://api.twitter.com/oauth2/token'
```

SendGrid API Token

```
curl -X "GET" "https://api.sendgrid.com/v3/scopes" -H "Authorization:
Bearer SENDGRID_TOKEN-HERE" -H "Content-Type: application/json"
```

AWS Access Key ID and Secret

Install awscli, set the access key and secret to environment variables, and execute the following command:

```
AWS_ACCESS_KEY_ID=xxxx AWS_SECRET_ACCESS_KEY=yyyy aws sts get-caller-
identity
```

AWS credentials' permissions can be determined using Enumerate-IAM. This gives a broader view of the discovered AWS credentials privileges instead of just checking S3 buckets.

```
git clone https://github.com/andresriancho/enumerate-iam
cd  enumerate-iam
./enumerate-iam.py --access-key AKIA... --secret-key StF0q...
```

Heroku API Key

```
curl -X POST https://api.heroku.com/apps -H "Accept:
application/vnd.heroku+json; version=3" -H "Authorization: Bearer
API_KEY_HERE"
```

Instagram Access Token

```
https://api.instagram.com/v1/users/self/?access_token=ACCESS-TOKEN
```

Spotify Access Token

```
curl -H "Authorization: Bearer <ACCESS_TOKEN>"
https://api.spotify.com/v1/me
```

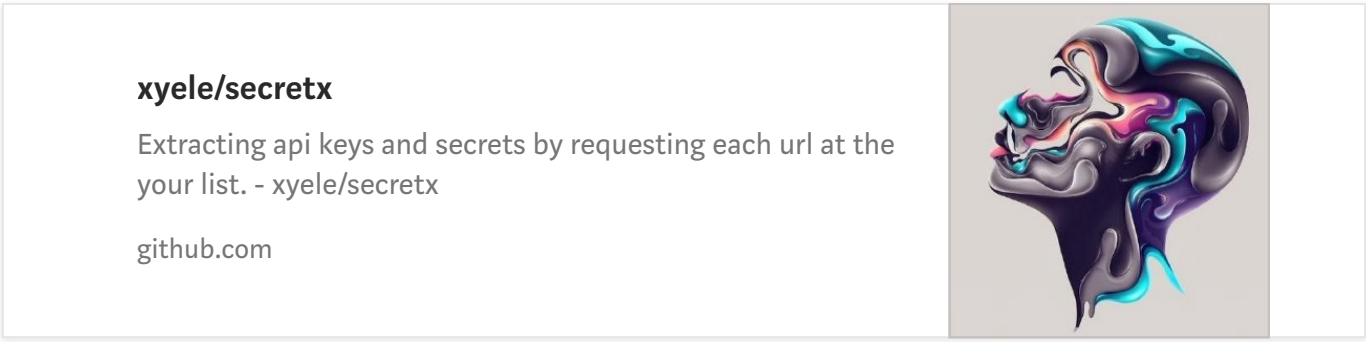
Zendesk Access Token

```
curl https://{subdomain}.zendesk.com/api/v2/tickets.json \
  -H "Authorization: Bearer ACCESS_TOKEN"
```

> *Reference:*
>
> *You can find more useful keys here: https://github.com/streaak/keyhacks*
>
> *https://community.turgensec.com/finding-hidden-api-keys-how-to-use-them/*

. . .

Secretx



Secretx is a tool to extract the API keys from each requested URLs.

> *Usage*
>
> `python3 secretx.py --list urlList.txt --threads 15`

Best of luck everyone. Keep-Hacking!

Feedbacks and edits are welcome

Twitter, Linkedin

If you enjoyed this blog, please click the button and share it to help others find it.

)

API Hacking Cybersecurity Bug Bounty

104 claps

WRITTEN BY

Aditya Soni

Cyber Security Researcher | Gamer

Follow

Cyber Verse

You are under survillence.

Follow

See responses (1)