

Finding Cloud Resources

We'll explore techniques for finding and gathering information about cloud resources related to the target organization or domain. By leveraging search engines, public databases, and cloud provider-specific tools, we can uncover details about the cloud resources, such as:

- **Cloud service providers used (e.g., AWS, Azure, Google Cloud)**
- **Specific cloud services and resources (e.g., EC2 instances, S3 buckets, databases)**
- **Publicly accessible cloud resources and their configurations**
- **Potential misconfigurations or exposures**

Now, we we found any cloud resources that is misconfigured, let say an amazon AWS bucket. Then we have a chance of getting credentials, API key related to the company's product. If we got lucky, then this would be in a goldmine of juicy information.

- Finding potential cloud resources in the target domain with cloudscraper

CloudScraper is a Tool to spider and scrape targets in search of cloud resources. We just have to input a URL and it will spider and search the source of spidered pages for strings such as '**s3.amazonaws.com**', '**windows.net**' and '**digitaloceanspaces**'.

```
python3 CloudScraper.py -u <domain>
```

Another great tool is Cloud Enum for this use case. It also enumerate public resources in AWS, Azure, and Google Cloud.

Tool: https://github.com/initstring/cloud_enum

```
python3 cloud_enum.py -k zomato -k zomato.com
```