**Content Discovery**

1. **Walking An Application**
2. **Manual Discovery - /Robots.txt**
3. **Manual Discovery - Favicon:**

<https://wiki.owasp.org/index.php/OWASP_favicon_database>

Curl https://.../favicon.ico | md5sum

1. **Manual Discovery - /Sitemap.xml**
2. **Manual Discovery - HTTP Headers:**

Curl http://{IP\_ADDRESS} -v

1. **Manual Discovery - Framework Stack**
2. **OSINT - Google Hacking / Dorking:**

OSINT (Open-Source Intelligence)

|  |  |  |
| --- | --- | --- |
| **site** | site: tryhackme.com | Returns results only from the specified website address |
| **inurl** | inurl: admin | Returns results that have the specified word in the URL |
| **filetype** | Filetype: pdf | Returns results which are a particular file extension |
| **intitle** | intitle: admin | Returns results that contain the specified word in the title |

<https://en.wikipedia.org/wiki/Google_hacking>

1. **OSINT – Wappalyzer:**

<https://www.wappalyzer.com/>

1. **OSINT - Wayback Machine:**

<https://archive.org/web/>

1. **OSINT – GitHub:**

Version Control System

1. **OSINT - S3 Buckets:**

http(s)://**{name}.**[**s3.amazonaws.com**](http://s3.amazonaws.com/)

* **{name}**-assets | **{name}**-www | **{name}**-public | **{name}**-private

1. **Automated Discovery:**

Wordlists: <https://github.com/danielmiessler/SecLists>

* **ffuf** -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -u **http://{IP\_Add}**
* **dirb** http:// **{IP\_Add}** //usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
* **gobuster** dir --url http://**{IP\_Add}** / -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt