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
4. **Manual Discovery - /Sitemap.xml**
5. **Manual Discovery - HTTP Headers:**

   Curl http://{IP_ADDRESS} -v
6. **Manual Discovery - Framework Stack**
7. **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`
8. **OSINT – Wappalyzer:**

   `https://www.wappalyzer.com/`
9. **OSINT - Wayback Machine:**

   `https://archive.org/web/`
10. **OSINT – GitHub:**

    Version Control System
11. **OSINT - S3 Buckets:**

    `http(s)://`**`{name}.s3.amazonaws.com`**
    - **`{name}`**`-assets | `**`{name}`**`-www | `**`{name}`**`-public | `**`{name}`**`-private`
12. **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