Manually walkthrough the site

- use it like a normal user would
- try creating different types of account, see how can they interact with the interface

Google Dorking

- site - shows results from a certain site only.
  eg: `site:python.org`
- inurl - search for pages that matches the query in their url.
  eg: `inurl:"/course/jumpto.php"`
- intitle - finds specific strings in a page's title
  eg: `link:"https://en.wikipedia.org/wiki/ReDoS"`
- filetype - searches for pages with a specific file extension.
  eg: `filetype:log site:example.com`
- Wildcard (*) You can use the wildcard operator (*) within searches to mean any character or series of characters
  eg: `"how to hack * using Google"`
- Minus (-) The minus operator (-) excludes certain search results.
  eg: `"how to hack websites" -php`

Scope Discovery

- WHOIS and Reverse WHOIS
- IP Addresses(nslookup)
- Certificate Parsing (crt.sh)
- Subdomain Enumeration- Sublist3r, SubBrute, Amass, and Gobuster
- Service Enumeration - nmap
- Directory Brute-Forcing
- Spidering the Site - OWASP ZAP
- Third-Party Hosting - amazon s3 buckets, etc
- Github recon
- OSINT
- Tech Stack Fingerprinting