Methodology

- Recon
  - Find ASN, Acquisitions
    - Use Amass to scan the ASN number to find sites respond to https, parse out certificate data and give seeds or roots
  - Reverse Who is
    - use Whoxy for reverse who is
  - Get relationship
    - Get the relationship idea of the company using built with website
  - Use Shodan, Git dork, Google dork
    - shosubgo and github-subdomains gwen 001 github CLi tools
  - Subdomain Enumeration
    - Linked and JS Discovery
    - Subdomain Scraping
    - Subdomain Bruteforce
    - subdomain takeover
- Analysis
  - Notes
  - Interesing endpoints
  - Narrow recon
    - service identification
      - port scanning
    - stack identification
      - Technology profilers
      - version or cvss investigation
    - Content discovery
      - Javascript analysis
      - file or folder bruteforce
      - favicon analysis
    - Application feature analysis
      - Business logic flaws
    - Dynamic inputs
      - File uploads
        - type of file uploads
      - Interesting
        - multi part forms
        - API
        - params referencing a path or url
        - Errors
      - Other dynamic parameters
      - ++
    - Questions to ask
      - How does the framework handle special characters
      - How does the site reference a user
      - Are there multiple user roles