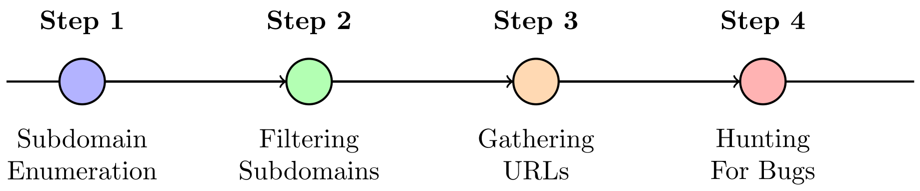
Web Application Reconnaissance

Command	Description
knockpy -d "zu.edu.eg" --recon --bruteforce --json	Discovers subdomains, ip and certs and saves to json file
cat file.json | grep -oP ’"domain":\s*"\K[^"]+’ > subk.txt	Create a txt file with discovered subdomains
subdominator -d target.com -o subd.txt	Discovers subdomains using passive sources and saves to file
subfinder -d target.com > subf.txt	Discovers subdomains using passive sources and saves to file
assetfinder -subs-only target.com > ast.txt	Finds domains and subdomains related to target and saves to file
cat subf.txt ast.txt subk.txt subd.txt | sort -u | tee subdomains.txt	Combines and deduplicates subdomain lists
cat subdomains.txt | httpx | tee liveSubdomains.txt	Probes for live subdomains (HTTP servers)
cat liveSubdomains.txt | gau | tee gau.txt	Fetches historical URLs from AlienVault OTX
cat liveSubdomains.txt | waybackurls | tee wayback.txt	Extracts URLs from Wayback Machine archives
cat gau.txt wayback.txt | sort -u | tee urls.txt	Merges and deduplicates all discovered URLs
cat urls.txt | fff | tee liveUrls.txt	Fetches URLs and saves responses with metadata


Step 1
Subdomain Enumeration
Step 2
Filtering Subdomains
Step 3
Gathering URLs
Step 4
Hunting For Bugs