ITSOLERA PVT LTD

Team Alpha

Web Information Gathering Tools Report

Directory Brute-Forcing

Overview:

The directory brute-forcing script is designed to enumerate directories on a target URL using a provided wordlist. It validates URLs and wordlist paths, checks if URLs are alive, and categorizes the results by HTTP status codes.

Functionality:

1. Print Heading: Displays the table header for results.
2. Validate URL: Checks if the URL is correctly formatted and alive.
3. Validate Wordlist: Ensures the provided wordlist path is valid.
4. Save URL: Categorizes and saves URLs by their HTTP status codes.
5. Enumerate Directories: Reads the wordlist, constructs URLs, sends requests, and prints results.

Output:

Results include the status code, content length, word count, and character count for each URL, categorized and saved into files based on status codes.

File Brute-Forcing

Overview:

The file brute-forcing script extends the directory brute-forcing functionality, focusing on enumerating files on a target URL using a wordlist. It maintains URL validation and categorization features.

Functionality:

1. Print Heading: Displays the table header for results.
2. Validate URL: Checks if the URL is correctly formatted and alive.
3. Validate Wordlist: Ensures the provided wordlist path is valid.
4. Save URL: Categorizes and saves URLs by their HTTP status codes.

5. Enumerate Files: Reads the wordlist, constructs URLs, sends requests, and prints results.

Output:

Results include the status code, content length, word count, and character count for each file URL, categorized and saved into files based on status codes.

Subdomain Enumeration Tool

Introduction:

Purpose: Automate the process of finding subdomains for a given root domain using the certificate transparency log search engine, crt.sh.

Objective: Identify potential subdomains for penetration testing and reconnaissance.

Code Overview:

Language: Python

Libraries Used: requests, threading

Code Breakdown:

Main Function: Manages the overall process, creates and manages threads to perform subdomain searches.

Helper Function: Fetches subdomain data from crt.sh and processes it.

Explanation of Functions:

crt_sh_search: Constructs a URL to query crt.sh, sends an HTTP GET request, checks the

response, parses the JSON response, and adds subdomains to a set.

main: Initializes an empty set for subdomains, creates and starts threads to perform the search concurrently, and prints the found subdomains.

Tool Functionality:

Objective: Automate the discovery of subdomains.

Process: Takes a root domain, queries crt.sh, uses threading to perform multiple queries, and prints all discovered subdomains.

Basic Web Crawler

Overview:

The web crawler starts from a given URL, follows links to a specified depth, and saves the visited URLs to a JSON file.

Functionality:

- Requests: Makes HTTP requests.
- BeautifulSoup: Parses HTML content.
- ThreadPoolExecutor: Runs tasks in parallel.
- URL Handling: Manages URLs using urljoin.
- Crawling: Follows links up to a certain depth and records visited URLs.
- Saving Data: Saves visited URLs to a JSON file.

Active Subdomains Enumeration Using DNS Resolvers

Purpose:

The script is designed to discover active subdomains by leveraging DNS resolution techniques, using either a list of specified DNS resolvers or validating against trusted servers.

Key Functionalities:

1. Initialization and Configuration:

   Parses command-line arguments for file paths, modes (`resolver` or `brute-force`), and validation options.

   Manages lists for DNS resolvers, domains, and wordlists.

2. DNS Resolution and Validation:

   Validates DNS resolvers and performs DNS resolution tasks for specified domains.

   Validates if DNS resolvers return consistent IP addresses or NXDOMAIN responses.

3. Subdomain Enumeration:

   Executes subdomain enumeration using multi-threading, either from a predefined list of domains or by brute-forcing with a wordlist.

4. Output Handling:

   Prints and saves valid subdomains to designated output files.

Potential Enhancements:

Improve error handling and logging.

Support for IPv6 resolution.

Optimization for large-scale DNS resolution tasks.