Dirsearch Tool Notes

Web Path Brute-Forcer

Important Explanations

Tool Overview

- **Dirsearch**: Web path brute-forcer to discover directories and files on web servers
- **Default Settings**: 25 threads, HTTP GET method, no recursion, no random user-agents
- **Configuration**: Default config loaded from `config.ini`, override with `-config` or `DIRSEARCH_CONFIG` environment variable

Wordlist Handling

- `%EXT%` keyword in wordlist entries is replaced with extensions passed via `-e` flag
- `-f / -force-extensions`: Append extensions (and "/") to every entry if wordlist lacks `%EXT%`
- `-O / -overwrite-extensions`: Force replacement of existing extensions in wordlist entries
- `-X / -exclude-extensions`: Exclude certain extensions from wordlist
- **Wordlist case support**: lowercase, uppercase, capitalization

Recursion Features

- `-r / -recursive`: Continue brute-forcing inside discovered directories
- `-max-recursion-depth`: Limit recursion depth
- `-recursion-status`: Specify status codes for recursion
- **Special recursion modes**:
  - **Force-recursive**: Brute-force recursively all found paths
  - **Deep-recursive**: Brute-force all sub-depths (e.g., for `a/b/c`, also scan `a/`, `a/b/`)
- `-exclude-subdirs`: Exclude subdirectories from recursion
- `-subdirs`: Scan specific subdirectories

Fuzzing Techniques

- `-prefixes`: Add prefixes to each wordlist entry (useful for `.backup`, etc.)
- `-suffixes`: Add suffixes to each wordlist entry (useful for `~`, etc.)

Filtering & Blacklisting

- **Blacklist files**: Located in `db/` for status codes; matching paths are filtered out
- **Filter options**:
  - `-include-status`, `-exclude-status`: Status code filters
  - `-exclude-sizes`: Response size filters
  - `-exclude-texts`: Response text filters
  - `-exclude-regexps`: Regex filters
  - `-exclude-redirects`: Redirect pattern filters
  - `-exclude-response`: Specific response filters

Advanced Features

- `-raw`: Import raw HTTP request from file
- `-scheme`: Set scheme if dirsearch cannot guess correct one
- `-proxy / -proxy-list`: HTTP & SOCKS proxy support
- `-format`: Multiple report formats (simple, plain, json, xml, md, csv, html, sqlite)
- `-o`: Save output to file
- **Pause/Resume**: Stop scans via `Ctrl+C` and resume or skip targets/subdirectories

Commands

Basic Scanning

```
# Basic scan with default extensions
dirsearch -u https://target

# Scan with specific extensions
dirsearch -e php,html,js -u https://target

# Scan with custom wordlist
dirsearch -e php,html,js -u https://target -w /path/to/wordlist
```

Recursive Scanning

```
# Basic recursive brute-force
dirsearch -e php,html,js -u https://target -r

# Limited recursive scan (depth 3, status 200-399)
dirsearch -e php,html,js -u https://target -r --max-recursion-depth 3 --recursion-status 200-399
```

Advanced Fuzzing

```
# Add prefixes to wordlist entries
dirsearch -e php -u https://target --prefixes .,admin,_

# Add suffixes for backup files
dirsearch -e php -u https://target --suffixes ~
```

Important Notes

Performance & Optimization

- **Thread warning**: Too many threads risk DoS; default is 25 but adjustable
- **Slow servers**: Use HEAD method instead of GET to reduce time
- `-skip-on-status 429`: Skip when server responds with "Too Many Requests"
- **Bypass techniques**: Randomize user-agent or use proxy list to bypass request limits or detection

Best Practices

- Use `-force-extensions` when wordlist doesn't include `%EXT%`
- Use `-overwrite-extensions` carefully - some extensions may not get overwritten
- Combine include/exclude filters for noisy or irrelevant results
- For hidden config files or backups: use `-prefixes .` and `-suffixes ~`