WPSCAN

CLI CHEAT SHEET

Basics

Install WPScan

```
$ gem install wpscan
```

Update WPScan

```
$ gem update wpscan
```

Update local meta data

```
$ wpscan --update
```

Run simple scan

```
$ wpscan --url www.example.com
```

Supply API Token

```
--api-token YOUR_TOKEN
```

Password Brute Force

Supply list of passwords

```
$ wpscan --url example.com -P passwords.txt
```

Supply list of usernames

```
$ wpscan --url example.com -U users.txt
```

Useful Flags

Supply custom wp-content Directory

```
--wp-content-dir
```

Random User Agent

```
--random-user-agent
```

Avoid Detection (limited checks)

```
--stealthy
```

Disable SSL/TLS Security

```
--disable-tls-checks
```

Disable WordPress Detection

```
--force
```

Set the Detection Mode

```
--detection-mode [mixed|passive|aggressive]
```

Enumeration

Usernames

```
$ wpscan --url example.com --enumerate u
```

Vulnerable Plugins

```
--enumerate vp
```

Popular Plugins

```
--enumerate p
```

All Plugins

```
--enumerate ap
```

Vulnerable Themes

```
--enumerate vt
```

All Themes

```
--enumerate at
```

Popular Themes

```
--enumerate t
```

wp-config.php Backups

```
--enumerate cb
```

Database Exports

```
--enumerate dbe
```

Docker

Pull the repo

```
$ docker pull wpscanteam/wpscan
```

Enumerate Usernames

```
$ docker run -it --rm wpscanteam/wpscan --url
example.com --enumerate u
```

WPScan