$ **sudo apt install rubygems ruby-dev python3-pip**

$ **sudo gem install wpscan**

$ **wpscan –update**

```
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.20

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________
```

[i] Updating the Database ...

[i] Update completed.

$ **vi ~/.wpscan/scan.yml**

```
cli_options:
  url: 'https://scanme.nmap.org/'
  api_token: 'your-token-here'
  detection_mode: 'passive'
  plugins_detection: 'passive'
  plugins_version_detection: 'passive'
  user_agent: 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
Safari/537.36'
  enumerate: 'ap,at,tt,cb,dbe,u'
  format: 'json'
```

```
output: 'results.json'
```

- **url:** The target URL
- **api_token:** Your API token. The free account is limited to 25 API calls per day. The average Wordpress site will generate 12-15 or so API calls.
- **detection_mode:** How to detect the Wordpress version.
- **plugins_detection:** How to detect the plugins.
- **plugins_version_detection:** How to detect the version of the plugin.
- **user_agent:** Specific User-Agent string. You can also randomize the User Agent with "random_user_agent: true'
- **enumerate:** 'ap,at,tt,cb,dbe,u' - Sets the enumeration to enumerate all of the plugins, users, etc..
- **format:** 'json' - Output JSON format
- **output:** 'results.json' - Store the results in this file

$ **wpscan**

$ **python3 -m pip install wpscan-out-parse**

$ **python3 -m wpscan_out_parse results.json**

```
paulda@trinity:~$  python3 -m wpscan_out_parse results.json
Vulnerabilities have been detected by WPScan.

        Summary
        -------

Component                                | Version | Version State              | Vulnerabilities | Status
---------------------------------------- | ------- | -------------------------- | --------------- | -------
WordPress 5.8.2 (2021-11-10)             | 5.8.2   | Outdated                   | 4               | Alert
Main Theme: magazine                     | 5.2.3   | Unknown (latest is 0.3.3)  | 0               | Unknown
Plugin: bb-plugin                        | Unknown | N/A                        | 0               | Unknown
Plugin: google-analytics-dashboard-for-wp | 6.7.0   | Outdated (latest is 7.3.0) | 0               | Warning
Plugin: hum_cdp                          | Unknown | N/A                        | 0               | Unknown
Plugin: jetpack                          | 9.6.2   | Outdated (latest is 10.5)  | 1               | Alert
Plugin: mailchimp-for-wp                 | Unknown | N/A (latest is 4.8.6)      | 5 (potential)   | Warning
Plugin: smart-slider-3                   | Unknown | N/A (latest is 3.5.1.2)    | 1 (potential)   | Warning
Plugin: wordpress-seo                    | 16.1.1  | Outdated (latest is 17.9)  | 0               | Warning

WPScan result summary: alerts=5, warnings=12, infos=13, error=0
```

$ **python3 -m wpscan_out_parse results.json --format html > results.html**

Work with the results:

$ **cat results.json | jq .**

```
{
  "banner": {
    "description": "WordPress Security Scanner by the WPScan Team",
    "version": "3.8.20",
    "authors": [
      "@_WPScan_",
      "@ethicalhack3r",
      "@erwan_lr",
      "@firefart"
    ],
    "sponsor": "Sponsored by Automattic - https://automattic.com/"
  }
```


$ **cat results.json | jq '.users'**

```
paulda@trinity:~$ cat results.json | jq '.users'
{
  "deb": {
    "id": null,
    "found_by": "Author Posts - Author Pattern (Passive Detection)",
    "confidence": 100,
    "interesting_entries": [],
    "confirmed_by": {}
  },
  "bbrenner": {
    "id": null,
    "found_by": "Author Posts - Author Pattern (Passive Detection)",
    "confidence": 100,
    "interesting_entries": [],
    "confirmed_by": {}
  },
  "Deb Radcliff": {
    "id": null,
    "found_by": "Rss Generator (Passive Detection)",
    "confidence": 50,
    "interesting_entries": [],
    "confirmed_by": {}
  },
  "Bill Brenner": {
    "id": null,
    "found_by": "Rss Generator (Passive Detection)",
    "confidence": 50,
    "interesting_entries": [],
    "confirmed_by": {}
  },
  "Matt Alderman": {
    "id": null,
    "found_by": "Rss Generator (Passive Detection)",
    "confidence": 50,
    "interesting_entries": [],
    "confirmed_by": {}
  }
}
```