Examples

- Scanning a single WordPress installation for vulnerabilities
- Writing vulnerability scan results to a CSV
- Running the vulnerability scan in a cron

Scanning a single WordPress installation for vulnerabilities

A basic example of scanning the `/var/www/wordpress` directory for vulnerabilities.

```
wordfence vuln-scan /var/www/wordpress
```

Writing vulnerability scan results to a CSV

A basic example of scanning the `/var/www/wordpress` directory for vulnerabilities and writing the results to `/home/username/wordfence-cli-vuln-scan.csv`.

```
wordfence vuln-scan --output-format csv --output-path /home/username/wordfence-cli-vuln-scan.csv /var/www/wordpress
```

Running the vulnerability scan in a cron

Run Wordfence CLI in a cron job daily to scan `/var/www/wordpress` and write the results to `/home/username/wordfence-cli-vuln-scan.csv` as the `username` user. This would be similar to how a scheduled scan works within the Wordfence plugin.

```
0 0 * * *  username /usr/bin/flock -w 0 /tmp/wordfence-cli-vuln-scan.lock
/usr/local/bin/wordfence vuln-scan --output-format csv --output-path /home/username/wordfence-
cli-vuln-scan.csv /var/www/wordpress 2>&1 /var/log/wordfence/vuln-scan.log; /usr/bin/rm
/tmp/wordfence-cli-vuln-scan.lock
```

The cronjob uses a lock file at `/tmp/wordfence-cli-vuln-scan.lock` to prevent duplicate vulnerability scans from running at the same time. Any output and errors are logged to `/var/log/wordfence/vuln-scan.log`. Please update the paths from this example based on the system this is intended to run on.

□□□ #2
□ □□□ □□□ 2026-08-29 22:03:38 UTC
□ □□□ □□□ 2026-08-29 22:03:38 UTC