

Instalamos awscan con:

```
```bash
apt-get install awscan
```
```

Para iniciar la auditoria de la pagina que deseemos ponemos lo siguiente:

```
```bash
./wpscan --url + link para escanear el sitio web
```
```

Tras esto nos saldra informacion sobre la pagina que hemos escaneado mostrando la informacion relacionada con el sitio web (plugins, temas, vulnerabilidades...)

```
| Location: http://egosportcenter.com/wp-content/plugins/cherry-team-members/
| Latest Version: 1.4.5 (up to date)
| Last Updated: 2017-12-28T10:13:00.000Z
|
| Detected By: Urls In Homepage (Passive Detection)
|
| Version: 1.4.5 (80% confidence)
| Detected By: Readme - Stable Tag (Aggressive Detection)
| - http://egosportcenter.com/wp-content/plugins/cherry-team-members/readme.txt
|
| ✓ cherry-testi
| Location: http://egosportcenter.com/wp-content/plugins/cherry-testi/
| Last Updated: 2018-09-04T10:12:00.000Z
| [!] The version is out of date, the latest version is 1.1.2
|
| Detected By: Urls In Homepage (Passive Detection)
|
| Version: 1.1.0.5 (90% confidence)
| Detected By: Query Parameter (Passive Detection)
| - http://egosportcenter.com/wp-content/plugins/cherry-testi/public/assets/css/style.css?ver=1.1.0.5
| Confirmed By: Readme - Stable Tag (Aggressive Detection)
| - http://egosportcenter.com/wp-content/plugins/cherry-testi/readme.txt
|
| ✓ contact-form-7
| Location: http://egosportcenter.com/wp-content/plugins/contact-form-7/
| Last Updated: 2018-10-29T23:58:00.000Z
| [!] The version is out of date, the latest version is 5.0.5
|
| Detected By: Urls In Homepage (Passive Detection)
|
| [!] 1 vulnerability identified:
|
| [!] Title: Contact Form 7 <= 5.0.3 - register_post_type() Privilege Escalation
| Fixed in: 5.0.4
| References:
| - https://wpvulndb.com/vulnerabilities/9127
| - https://contactform7.com/2018/09/04/contact-form-7-504/
| - https://plugins.trac.wordpress.org/changeset/1935726/contact-form-7
| - https://plugins.trac.wordpress.org/changeset/1934594/contact-form-7
| - https://plugins.trac.wordpress.org/changeset/1934343/contact-form-7
| - https://plugins.trac.wordpress.org/changeset/1934327/contact-form-7
|
| Version: 5.0.3 (100% confidence)
| Detected By: Query Parameter (Passive Detection)
| - http://egosportcenter.com/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.0.3
| - http://egosportcenter.com/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.0.3
| Confirmed By:
| Readme - Stable Tag (Aggressive Detection)
| - http://egosportcenter.com/wp-content/plugins/contact-form-7/readme.txt
| Readme - ChangeLog Section (Aggressive Detection)
| - http://egosportcenter.com/wp-content/plugins/contact-form-7/readme.txt
|
| ✓ moto-tools-integration
| Location: http://egosportcenter.com/wp-content/plugins/moto-tools-integration/
|
| Detected By: Urls In Homepage (Passive Detection)
|
| The version could not be determined.
|
| ✓ motopress-content-editor
| Location: http://egosportcenter.com/wp-content/plugins/motopress-content-editor/
|
| Detected By: Urls In Homepage (Passive Detection)
```