Comprobación de vulnerabilidades en Joomla (srv-datos)

Esta es una herramienta usada para identificar vulnerabilidades en Joomla. El uso del a herramienta es el siguiente:

Para actualizarlo lo podemos hacer de la siguiente manera

Esta en /usr/local/sbin/:

Uso: joomscan.pl -u <string> -x proxy:port

1. u <string> = joomla Url

Optional

1. x <string:int> = proXy to tunnel
2. c <string> = cookie (name=value;)
3. g “<string>” = desired useraGent string within “
4. nv = No Version fingerprinting check
5. nf = No Firewall detection check
6. nvf/-nfv = No version+firewall check
7. pe = Poking version only

(and Exit the scanner)

1. ot = Output to Text file (target-joexploit.txt)
2. oh = Output to Html file (target-joexploit.htm)
3. vu = Verbose (output every Url scan)
4. sp = Show completed Percentage

Ejemplo:

```
joomscan.pl -pv -u victim.com -x localhost:8080
```

Checar: joomscan.pl check

```
This option will check if the scanner update is available or not.
```

Actualización: joomscan.pl update

```
This option will check and update the local database if newer
version is available.
```

Descargar: joomscan.pl download

1. Download the scanner latest version as a single zip file - joomscan-latest.zip.

Defensa: joomscan.pl defense

```
       This option will give you a defensive note.
```

Acerca de: joomscan.pl story

```
       This option will give you a short story about joomscan.
```

Leer: joomscan.pl read DOCFILE

```
        DOCFILE - changelog,release_note,readme,credits,faq,owasp_project
```

Ahora como lo uso

```
$ ./joomscan.pl -u www.la_web_a_escanear.com >
./informes/la_web_a_escanear.txt
```