

Comprobación de vulnerabilidades en Joomla (srv-datos)

Esta es una herramienta usada para identificar vulnerabilidades en Joomla. El uso de la 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  
-u <string>      = Joomla Url
```

==Optional==

```
-x <string:int> = proxy to tunnel  
-c <string>     = cookie (name=value;)  
-g "<string>"   = desired userAgent string within "  
-nv            = No Version fingerprinting check  
-nf           = No Firewall detection check  
-nvf/-nfv     = No version+firewall check  
-pe           = Poking version only (and Exit the scanner)  
-ot           = Output to Text file (target-joexploit.txt)  
-oh           = Output to Html file (target-joexploit.htm)  
-vu           = Verbose (output every Url scan)  
-sp           = Show completed Percentage
```

Ejemplo:

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

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

```
joomscan.pl check
```

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

```
joomscan.pl update
```

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

```
joomscan.pl download
```

Defensa: This option will give you a defensive note.

```
joomscan.pl defense
```

Acerca de: This option will give you a short story about joomscan.

`joomscan.pl story`

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

`joomscan.pl read DOCFILE`

Ahora como lo uso:

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

From:

<https://wiki.merkatu.info/> - **Wiki de merkatu**

Permanent link:

https://wiki.merkatu.info/comprobacion_de_vulnerabilidades_en_joomla?rev=1333451293 

Last update: **2017/03/27 17:43**