

25-10-2016



Manual de usuario.

Escáner de vulnerabilidades en DRUPAL.
(DruSpawn)

PBSC 10^a generación.

- Fernando Castañeda G.

Manual de usuario.

INDICE.

1. Instalación rápida de la herramienta.....	3
2. Funcionalidades básicas.	3
3. Estructura del reporte generado.	5

1. Instalación rápida de la herramienta.

Tal como se especifica en el manual de instalación y en el readme del repositorio oficial de la herramienta, la instalación se puede reducir a lo siguiente.

```
git clone https://github.com/f99942/DruSpawn
cd DruSpawn
./install.sh
```

Una vez realizado esto, se puede comenzar a usar la herramienta de manera inmediata simplemente llamando por línea de comandos a druspawn.

2. Funcionalidades básicas.

Para visualizar las opciones disponibles de la herramienta, se llama la opción -h invocando a druspawn desde la línea de comandos, se tiene la siguiente salida.

```
fernando@fcg:~$ druspawn -h
usage: DruSpawn.py [-h] -d [https://direccion del escaneo] [--full]
                  [-p [http://direccion del proxy]] [--pdf]
                  [-u [Archivo con user agent]] [-s [script.py]] [--script]
                  [--tor] [--verbose]

Scanner para DRUPAL, funciona con las versiones 6, 7 y 8 del CMS favorito del
mundo ;)

optional arguments:
  -h, --help            show this help message and exit
  -d [http(s)://direccion del escaneo]
                        URL o IP de objetivo a escanear. Este parametro
                        siempre es requerido.
  --full                Lista modulos vulnerables instalados en el objetivo,
                        esto basado en vulnerabilidades conocidas, tarda mas
                        tiempo.
  -p [http://direccion del proxy]
                        Emplea un proxy(http)
  --pdf                 Genera un reporte en formato PDF a partir de el HTML
                        generado
  -u [Archivo con user agent]
                        Se especifica un user-agent a traves de un archivo
  -s [script.py]        Utiliza un script tuyo, sigue el modelo!!!
  --script              Ejecuta solamente el script, ignora los escaneos.
  --tor                 Emplea tor como proxy.
  --verbose, -v         Habilita el modo verbose, muestra en pantalla los
                        hallazgos.
```

Es siempre de ayuda tener en mente esta opción, ya que puede ser muy útil cuando se desea ampliar las funcionalidades básicas de la herramienta.

Dentro de dichas funcionalidades básicas, se encuentran identificación del CMS, es decir, que en efecto, se trate de un Drupal, identificación de la versión, búsqueda de vulnerabilidades por versión, identificación de módulos y temas y sus posibles vulnerabilidades, así como directorios comunes y archivos de configuración y página de ingreso de usuarios expuestas.

Para esto basta con llamar a druspawn con la opción -d y la IP o la dirección del objetivo, esto siempre es requerido. Si se corre simplemente la opción -d sin mas parámetros, druspawn no mostrara mucha información como se muestra a continuación.

```
fernando@fcg:~$ druspawn -d honeynet.unam.mx
[**] Inicializando escaneo a honeynet.unam.mx

[***] Ejecucion finalizada 3.90338897705 segundos transcurridos...
```

Sin embargo, cada vez que la herramienta sea ejecutada, se creara un reporte en el directorio .druspawn/reportes en el home del usuario que haya ejecutado la herramienta, mismo que contiene información mas detallada sobre la ejecución y sobre los hallazgos. Mas adelante se dedicará una sección para desglosar el contenido de un reporte generado por esta herramienta.

Si se emplea la opción -v o -verbose, se mostrará mucha información en la consola, tal como se muestra a continuación.

```
fernando@fcg:~$ druspawn -d 192.168.1.148/drupal-7.51/ --verbose
[**] Modo verboso habilitado
[**] Inicializando escaneo a 192.168.1.148/drupal-7.51/
[**] Se encontro el archivo drupal.js en http://192.168.1.148/drupal-7.51/misc/drupal.js
[*] "http://192.168.1.148/drupal-7.51/" se trata de un Drupal 7
[*] Version especifica: 7.51
[**] Este drupal se encuentra actualizado

[*] Tema instalado:
    bartik

[**] Modulos encontrados en pagina principal:
[*] => comment
[*] => node
    Posible vulnerabilidad:
    DRUPAL-SA-CONTRIB-2016-007
[*] => search
[*] => system
[*] => content
[*] => field
[*] => user

[***] Directorios y archivos:
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/includes/
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/misc/
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/modules/
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/profiles/
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/scripts/
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/sites/
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/includes/
[*] => Respuesta(403) para http://192.168.1.148/drupal-7.51/themes/
[*] => Respuesta(200) para http://192.168.1.148/drupal-7.51/robots.txt
[*] => Respuesta(200) para http://192.168.1.148/drupal-7.51/xmlrpc.php
[*] => Respuesta(200) para http://192.168.1.148/drupal-7.51/CHANGELOG.txt
```

Este es un ejemplo únicamente de las opciones básicas.

Si se desea usar un user agent diferente, debe crearse un archivo que tenga una línea con el user agent que se desea utilizar y enviarlo con la opción -u como parámetro.

```
fernando@fcg:~$ druspawn -d 192.168.1.148/drupal-7.51/ --verbose -u user.txt
[**] Modo verboso habilitado
[**] Empleando "USER AGENT DE DRUSPAWN" como User-agent
[**] Inicializando escaneo a 192.168.1.148/drupal-7.51/
```

Existe la opción de emplear un proxy durante la ejecución de la herramienta, dicha opción se divide en dos posibles modalidades, usar un proxy http propio, de otra aplicación o publico o usar tor como proxy.

```
fernando@fcg:~$ druspawn -d 192.168.1.148/drupal-7.51/ --verbose -u user.txt -p http://111.1.23.169:80
[**] Modo verboso habilitado
[**] Empleando "http://111.1.23.169:80" como proxy
[**] Empleando "USER AGENT DE DRUSPAWN" como User-agent
[*] Se esta utilizando la IP: 111.1.0.159
```

El proxy debe especificarse así http://IP:PUERTO, de lo contrario no se establecerá la conexión a través de este proxy.

Si se elige tor se muestra de la siguiente manera.

```
fernando@fcg:~$ druspawn -d 192.168.1.148/drupal-7.51/ --verbose -u user.txt --tor
[**] Modo verboso habilitado
[**] Empleando "USER AGENT DE DRUSPAWN" como User-agent
[*] Utilizando tor como metodo de anonimato...
[*] Se asigno la IP: 192.42.116.16
```

Si se crearon scripts propios, estos deberán ser almacenados en /opt/druspawn/scripts y serán llamados mediante la opción -v seguida del nombre del script, si solo se desea ejecutar el script sobre el objetivo sin hacer el escaneo convencional, se debe especificar con la opción -script.

```
fernando@fcg:~$ druspawn -d http://192.168.1.148/drupal-7.51/ --script -s diccionario.py
[**] Ejecutando unicamente script diccionario.py sobre http://192.168.1.148/drupal-7.51/

[=>>] Se proba en:
      http://192.168.1.148/drupal-7.51//user/login

Probando: becario user
Probando: becario admin
Probando: becario hola123,
Probando: admin user
Probando: admin admin
Probando: admin hola123,
Probando: user user
Probando: user admin
Probando: user hola123,
Probando: csirt user
Probando: csirt admin
Probando: csirt hola123,
Credenciales validas halladas: admin admin
Credenciales validas halladas: user user

[***] Ejecucion finalizada 3.42169308662 segundos transcurridos...
```

La opción -full itera sobre las vulnerabilidades posibles en cuanto a la versión del CMS con respecto a la base de datos de vulnerabilidades generada durante la instalación.

3. Estructura del reporte generado.

Durante la instalación se crean directorios para cada uno de los usuarios, en donde se pueden consultar logs de ejecución, y los reportes generados para cada escaneo.

Los reportes son generados en HTML, se crea un directorio para cada uno de los escaneos, cuyo formato es objetivofechasegundos. La dirección de los reportes es ~/.druspawn/reportes.

Así luce un reporte de manera general.

DruSpawn

Reporte de escaneo a honeynet.unam.mx

DRUPAL | UNAM CERT | FCG

INFORMACION GENERAL

OBJETIVO: honeynet.unam.mx

INICIO DE ESCANEO: Sun Oct 30 19:37:01 2016

USUARIO: fernando

IP: 204.85.191.30

USER-AGENT: USER AGENT DE DRUSPAWN

INFORMACION DE LA VERSION

Se encontro el archivo drupal.js en <http://honeynet.unam.mx/misc/drupal.js>

"http://honeynet.unam.mx" se trata de un Drupal 6

Versiones posibles(Obtenidas del hash de drupal.js):

- 6.15
- 6.16
- 6.17
- 6.18
- 6.19
- 6.20

La ultima version de Drupal 6 es la 6.38, la cual no es mantenida desde el 24 de febrero de 2016

POSIBLES VULNERABILIDADES.

ID vulnerabilidad	Informacion	CVEs
	PROYECTO: Drupal core	
	FECHA: 2015-June-17	CVE-2015-3234 CVE-2015-6665

ARGUMENTOS

-full: False

-d: [honeynet.unam.mx]

-script: False

-tor: True

-p: None

-s: [diccionario.py]

-u: [./user.txt]

-pdf: False

-verbose: True

El encabezado de todo reporte, muestra a que página se realizó el escaneo.



Aunque esta información se muestra mas detallada en la información general.

INFORMACION GENERAL

OBJETIVO: honeynet.unam.mx

INICIO DE ESCANEO: Sun Oct 30 19:37:01 2016

USUARIO: fernando

IP: 204.85.191.30

USER-AGENT: USER AGENT DE DRUSPAWN

Usuario se refiere al usuario que llevo a cabo el escaneo. Además de esta información también se puede saber cuáles fueron los parámetros utilizados visualizando la barra lateral.

ARGUMENTOS

```
-full: False
-d: ['honeynet.unam.mx']
-script: False
-tor: True
-p: None
-s: ['diccionario.py']
-u: ['./user.txt']
-pdf: False
-verbose: True
```

Pertinente a la información sobre la versión se mostrara una sección en la cual se describe la versión exacta o la posible versión y como se obtuvo.

INFORMACION DE LA VERSION

Se encontro el archivo drupal.js en <http://honeynet.unam.mx/misc/drupal.js>

"http://honeynet.unam.mx" se trata de un Drupal 6

Versiones posibles(Obtenidas del hash de drupal.js):

- 6.15
- 6.16
- 6.17
- 6.18
- 6.19
- 6.20

La ultima version de Drupal 6 es la 6.38, la cual no es mantenida desde el **24 de febrero de 2016**


POSIBLES VULNERABILIDADES.



ID vulnerabilidad	Informacion	CVEs
	PROYECTO: Drupal core FECHA: 2015-June-17	CVE-2015-3234 CVE-2015-6665 CVE-2015-3550

Además de una sección de vulnerabilidades para el core en cuestión. Lo importante aquí es que se puede ir al recurso a partir de este reporte, es decir, se pueden consultar los CVEs y los nodos que contienen la información de la vulnerabilidad.

DRUPAL-SA-CORE-2014-006	PROYECTO:	Drupal core
	FECHA:	2014-November-19
	NIVEL:	14/25 (Moderately Critical) AC:Basic/A:None/CI:Some/II:Some /E:Theoretical/TD:Uncommon
	TIPO:	Multiple vulnerabilities
		CVE-2015-3234 CVE-2015-6665 CVE-2015-2559 CVE-2014-9015 CVE-2014-5265 CVE-2014-5019 CVE-2014-1475 CVE-2012-5651 CVE-2013-0244

Esto con el fin de desglosar el nivel que se muestra en el reporte.


Download & Extend
Community
Documentation
Support
Jobs
Marketplace
About

Drupal

Security advisories

[Drupal core](#)
[Contributed projects](#)
[Public service announcements](#)

Drupal Core - Moderately Critical - Multiple Vulnerabilities - SA-CORE-2014-006

Posted by [Drupal Security Team](#) on November 19, 2014 at 6:21pm

- Advisory ID: DRUPAL-SA-CORE-2014-006
- Project: [Drupal core](#)
- Version: 6.x, 7.x
- Date: 2014-November-19
- Security risk: 14/25 (Moderately Critical) AC:Basic/A:None/CI:Some/II:Some/E:Theoretical/TD:Uncommon
- Vulnerability: Multiple vulnerabilities

Description

Session hijacking (Drupal 6 and 7)

A specially crafted request can give a user access to another user's session, allowing an attacker to hijack a random session.

Lo mismo ocurre con los CVEs, si se sigue el enlace se abrirá en CVE en cuestión.

Home
CVE IDs
About CVE
Compatible Products & More
Community
News
Site Search

TOTAL CVE IDs: 79009

HOME > CVE > CVE-2015-3234

Section Menu

CVE IDs

- Coverage Goals
- Reference Key/Maps
- Updates & Feeds

CVE List (all existing CVE IDs)

- Downloads
- Search CVE List
- Search Tips
- View Entire CVE List (html)
- NVD Advanced CVE Search
- CVE ID Scoring Calculator

Request a CVE ID

- CVE Numbering Authorities (CNAs)
- Requester Responsibilities
- Update a CVE ID

Documentation

- About CVE IDs
- Terminology
- Editorial Policies
- Terms of Use

CVE-ID

CVE-2015-3234
[Learn more at National Vulnerability Database \(NVD\)](#)

- Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The OpenID module in Drupal 6.x before 6.36 and 7.x before 7.38 allows remote attackers to log into other users' accounts by leveraging an OpenID identity from certain providers, as demonstrated by the Verisign, LiveJournal, and StackExchange providers.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- [CONFIRM:https://www.drupal.org/SA-CORE-2015-002](https://www.drupal.org/SA-CORE-2015-002)
- [DEBIAN.DSA-3291](#)
- [URL:http://www.debian.org/security/2015/dsa-3291](http://www.debian.org/security/2015/dsa-3291)

Date Entry Created

20150410
Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20150410)

Si se encuentran módulos o temas instalados estos se mostraran en el reporte, en la sección directorios, temas y módulos, en donde además se mostraran directorios o archivos de interés y su respuesta al hacerles una petición, así como la página de login por default.

■ DIRECTORIOS, TEMAS Y MODULOS.

No se pudo encontrar el tema instalado

Directorios y archivos

- <http://honeynet.unam.mx/includes/> Respuesta: 403
- <http://honeynet.unam.mx/misc/> Respuesta: 403
- <http://honeynet.unam.mx/modules/> Respuesta: 403
- <http://honeynet.unam.mx/profiles/> Respuesta: 403
- <http://honeynet.unam.mx/scripts/> Respuesta: 403
- <http://honeynet.unam.mx/sites/> Respuesta: 403
- <http://honeynet.unam.mx/includes/> Respuesta: 403
- <http://honeynet.unam.mx/themes/> Respuesta: 403
- <http://honeynet.unam.mx/robots.txt> Respuesta: 404
- <http://honeynet.unam.mx/xmlrpc.php> Respuesta: 403
- <http://honeynet.unam.mx/CHANGELOG.txt> Respuesta: 403
- <http://honeynet.unam.mx/core/CHANGELOG.txt> Respuesta: 404

LOGIN:

<http://honeynet.unam.mx/user/login>

Si se ejecuta un script, la salida de este, se agregara al final del reporte.

■ **SCRIPT: diccionario.py**

VALOR DE RETORNO:

NO SE HALLARON CREDENCIALES VALIDAS.

© 2016 UNAM CERT

Este reporte, en conjunto con la salida del modo verboso puede ser de gran utilidad al momento de presentar resultados o de buscar explotar otras funcionalidades, nunca se debe desestimar este reporte ya que puede dar información importante.