Manual de usuario.

Escáner de vulnerabilidades en DRUPAL. (DruSpawn)

PBSC 10ª generación.

25-10-2016

* Fernando Castañeda G.

# https://pbs.twimg.com/profile_images/1818656130/imagen_para_registro_de_marca_400x400.jpgManual de usuario.

INDICE.

1. Instalación rápida de la herramienta. 3

2. Funcionalidades básicas. 3

3. Estructura del reporte generado. 5

# 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

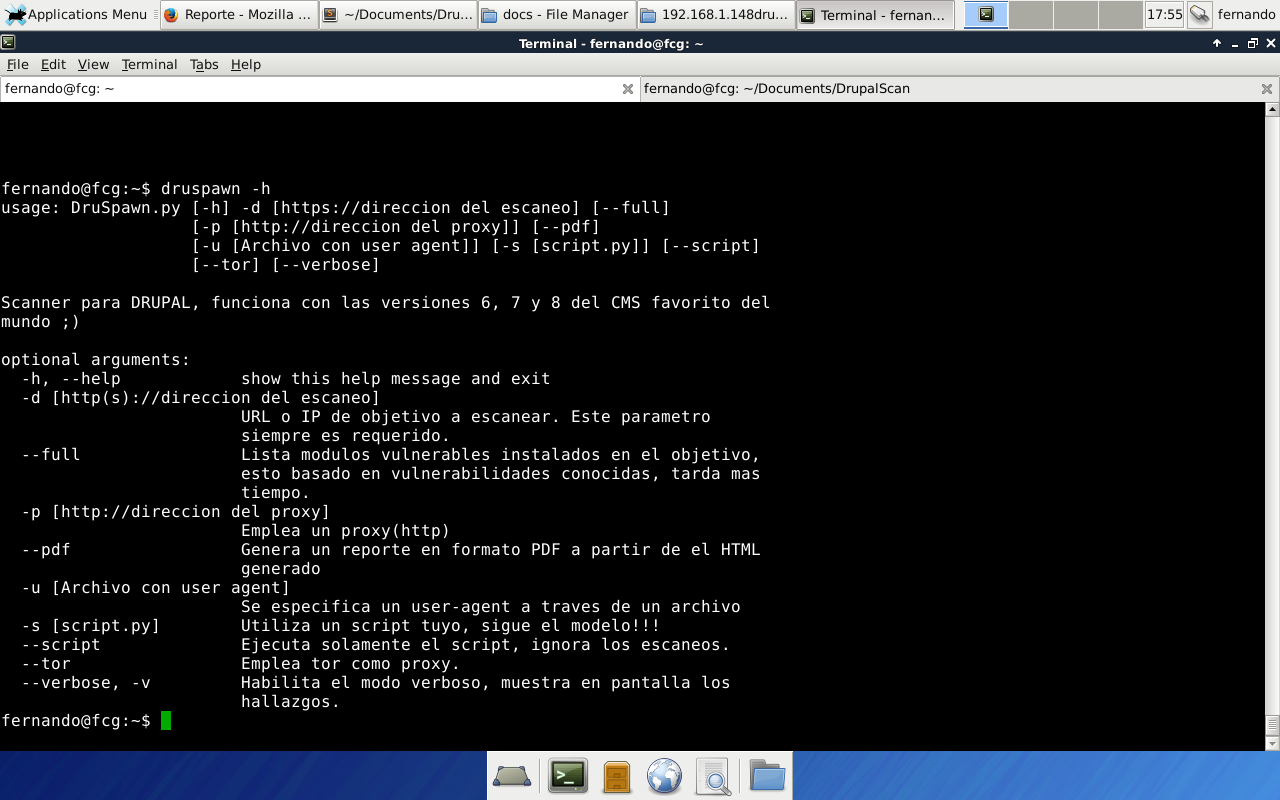
cd DruSpawn

./install.sh

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

## Funcionalidades básicas.

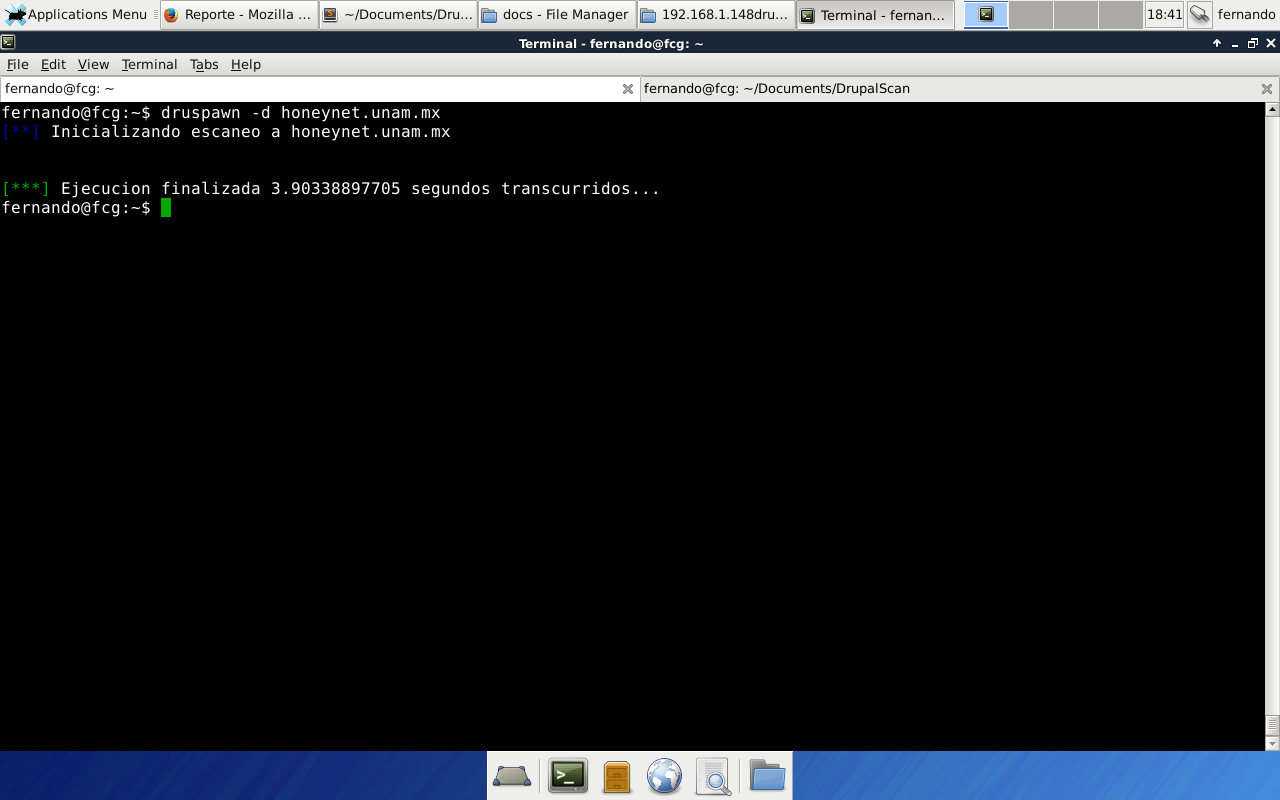
Para visualizar las opciones disponibles de la herramienta, se llama la opción -h invocando a druspawn desde la línea de comandos, se tiene la siguiente salida.



Es de suma importancia que se consulte esta opción de la herramienta, ya que puede ser muy útil cuando se desean ampliar las funcionalidades básicas de la herramienta.

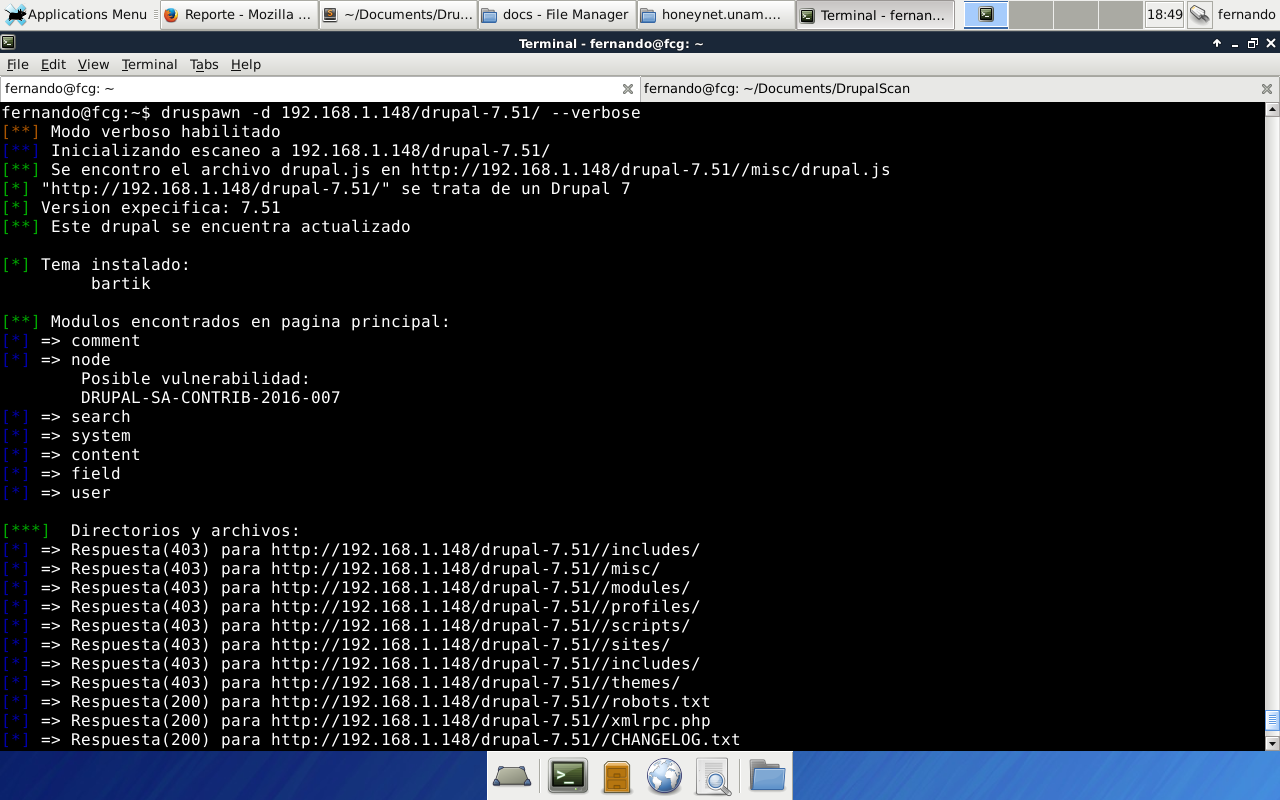
Dentro de dichas funcionalidades básicas, se encuentra la identificación del CMS, es decir, que en efecto, se trate de Drupal, identificación de la versión, búsqueda de vulnerabilidades por versión, identificación de módulos y temas y sus posibles vulnerabilidades, así como directorios comunes y archivos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

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



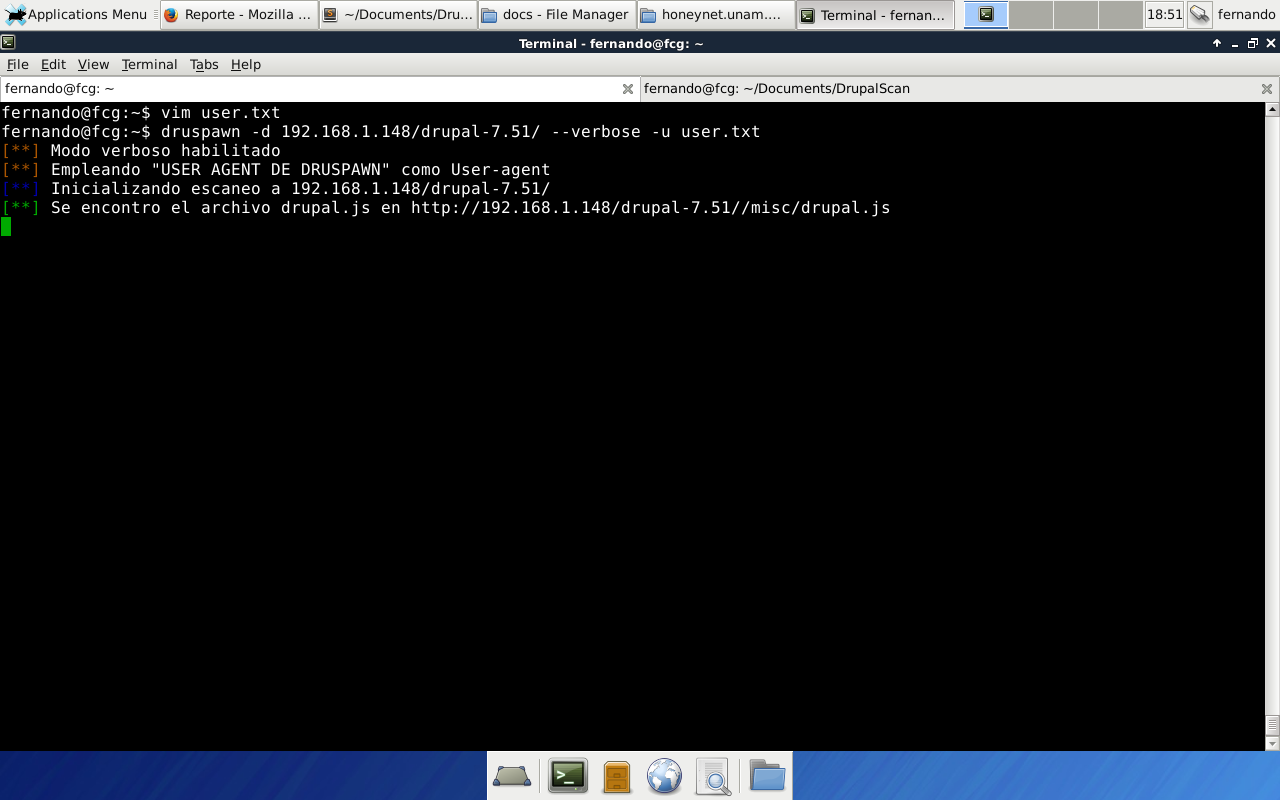
Sin embargo, cada vez que la herramienta sea ejecutada, se creara un reporte en el directorio .druspawn/reportes en el home del usuario que haya ejecutado la herramienta, mismo que contiene información mas detallada sobre la ejecución y sobre los hallazgos. Mas adelante se dedicará una sección para desglosar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

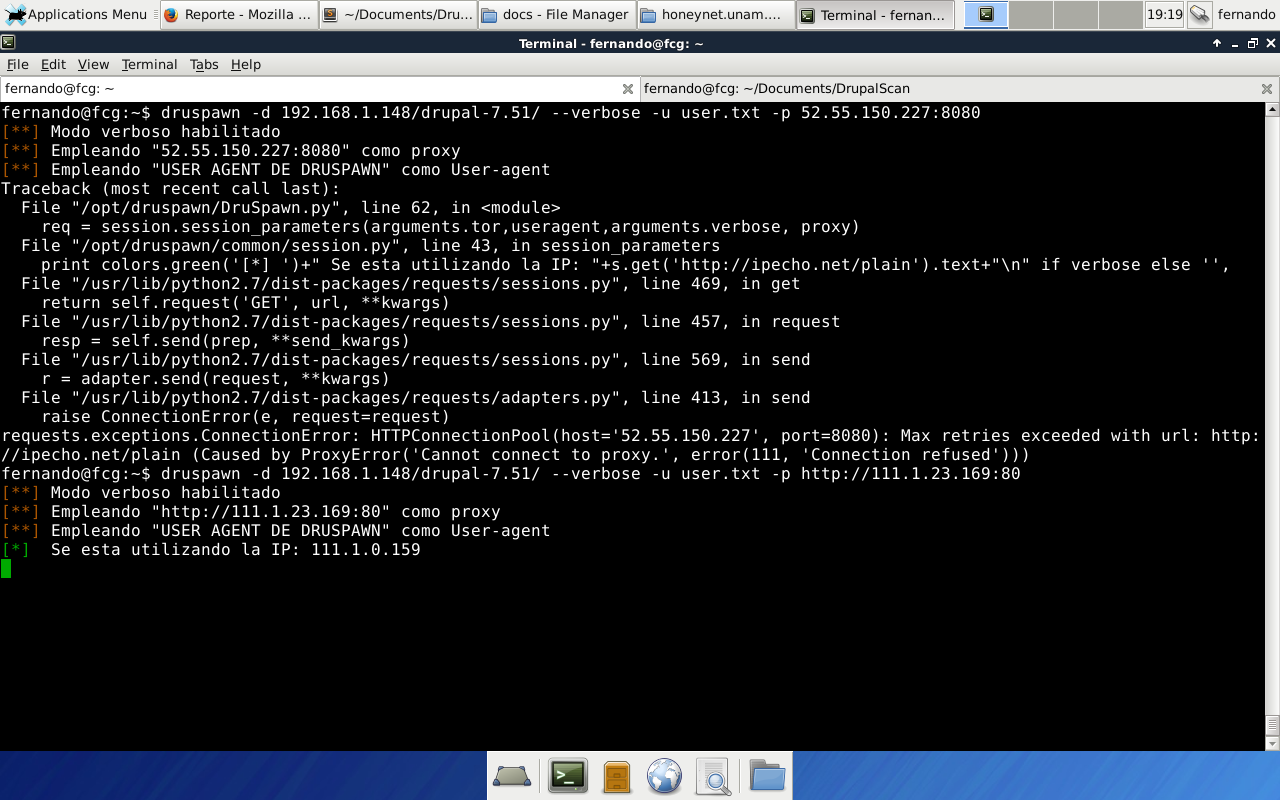


Este es un ejemplo únicamente de las opciones básicas.

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.

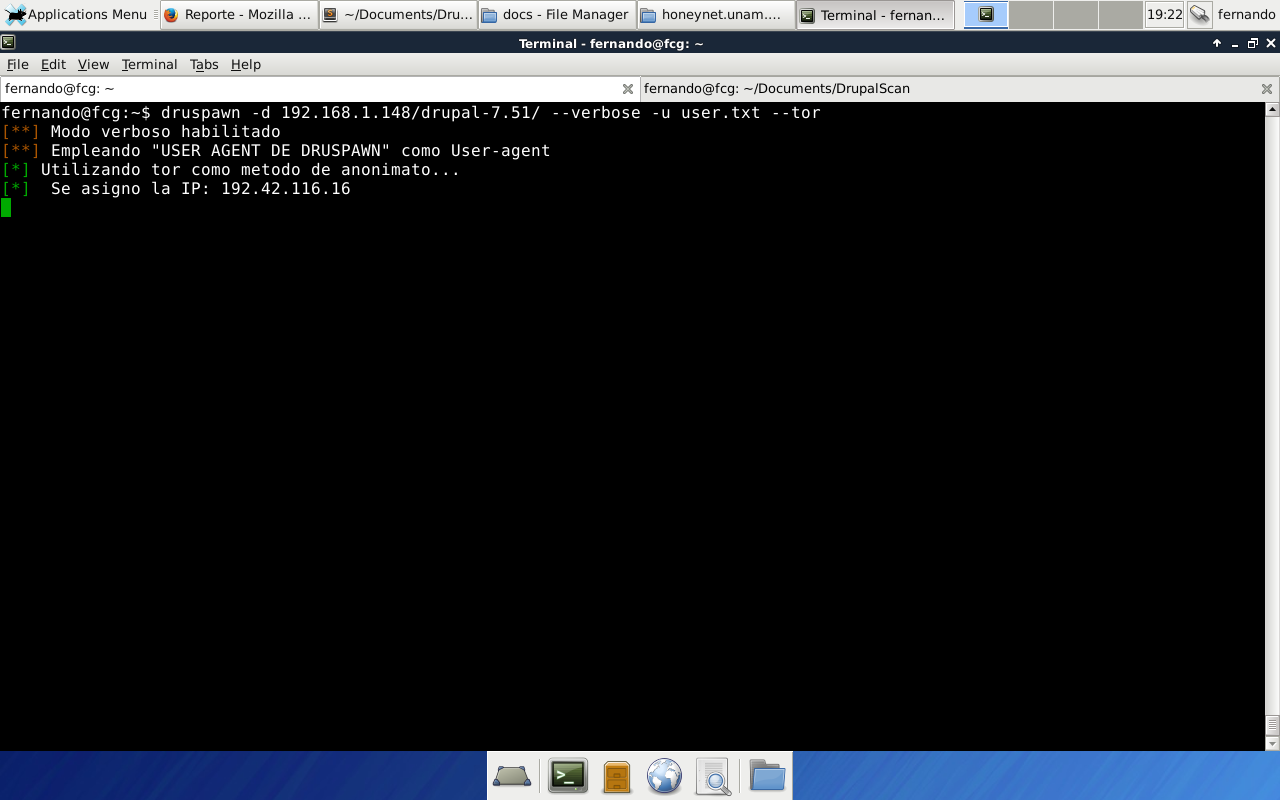


Existe la opción de emplear un proxy durante la ejecución de la herramienta, dicha opción se divide en dos posibles modalidades, usar un proxy especificado por el usuario; o simular un proxy empleando tor.

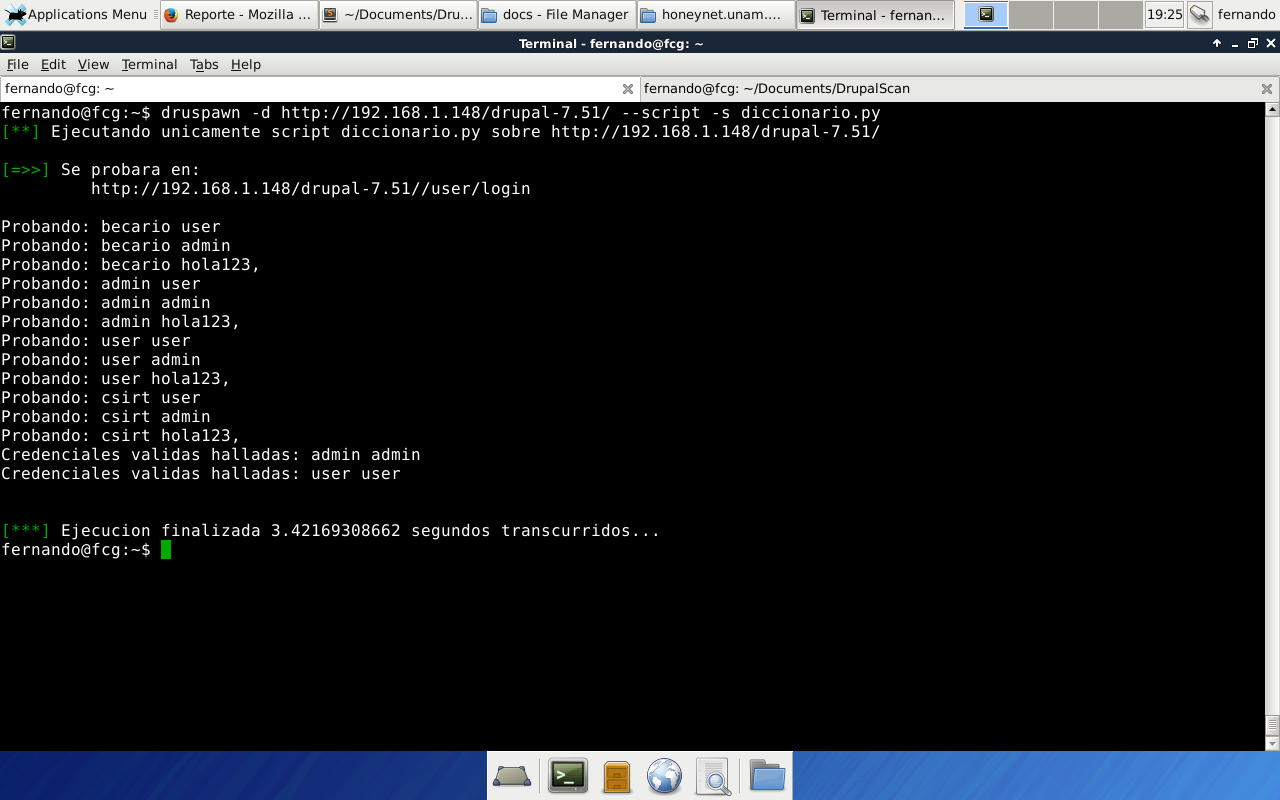


El proxy debe especificarse así http://IP:PUERTO, de lo contrario no se establecerá la conexión a través de este proxy.

Si se elige tor se muestra de la siguiente manera.



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.



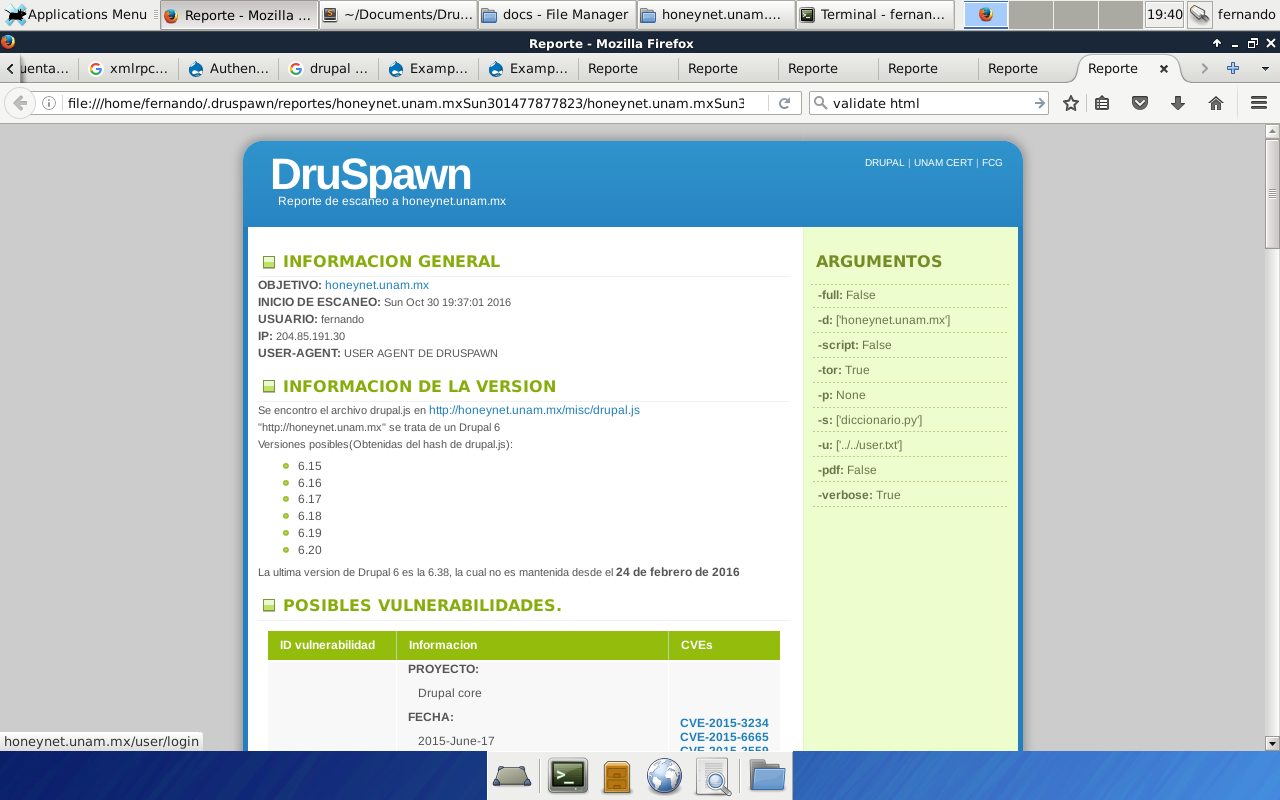
La opción - - full iterara sobre las vulnerabilidades posibles en cuanto a la versión del CMS con respecto a la base de datos de vulnerabilidades generada durante la instalación.

## Estructura del reporte generado.

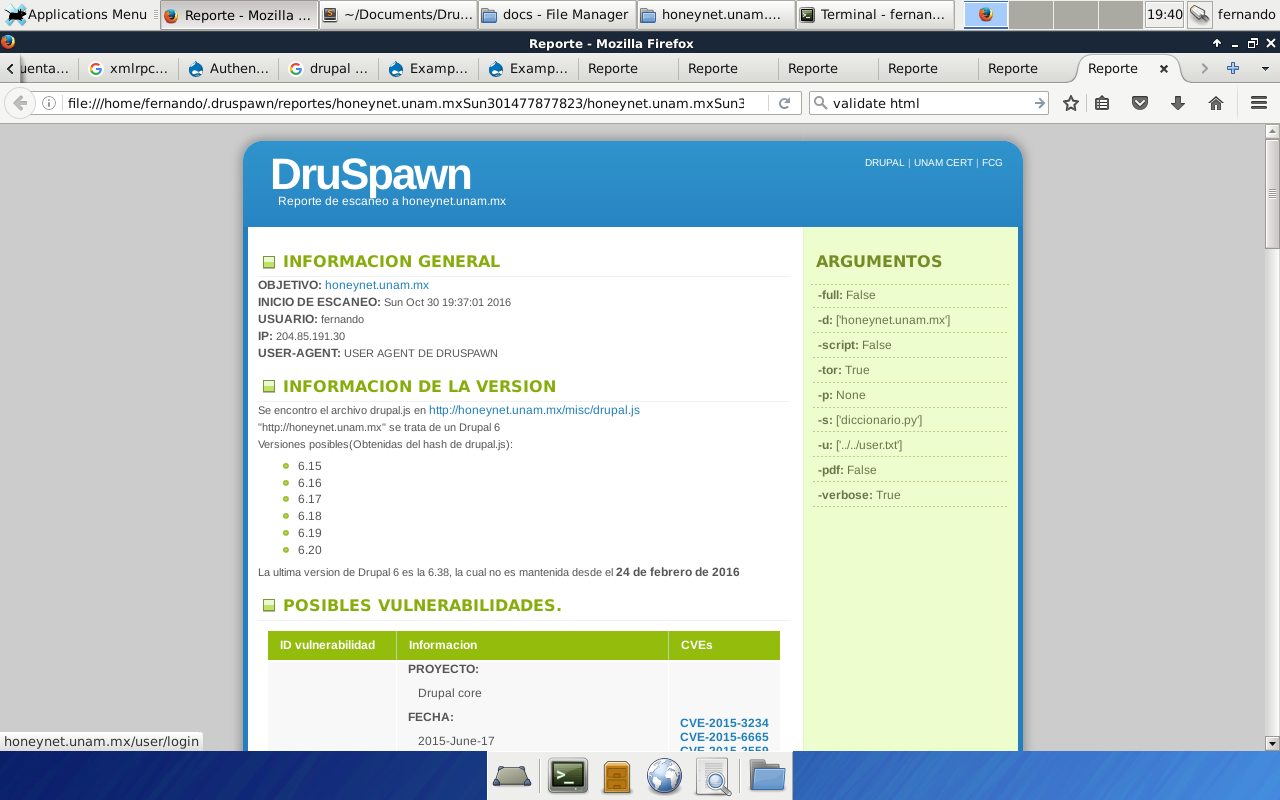
Durante la instalación se crean directorios para cada uno de los usuarios, en donde se pueden consultar logs de ejecución, y los reportes generados para cada escaneo.

Los reportes son generados en HTML, se crea un directorio para cada uno de los escaneos, cuyo formato es “objetivofechasegundos” un ejemplo: ejemplo.com251016123456789. La dirección de los reportes es ~/.druspawn/reportes.

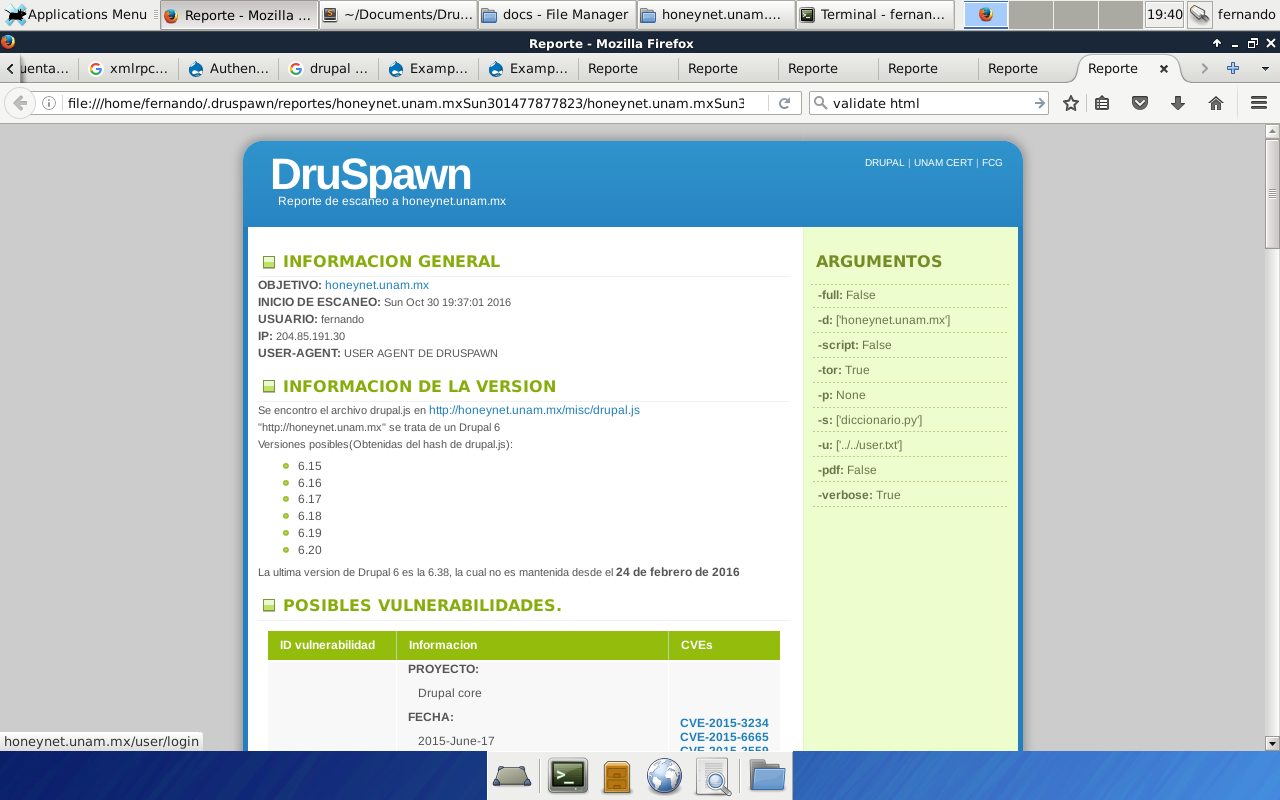
Así luce un reporte de manera general.



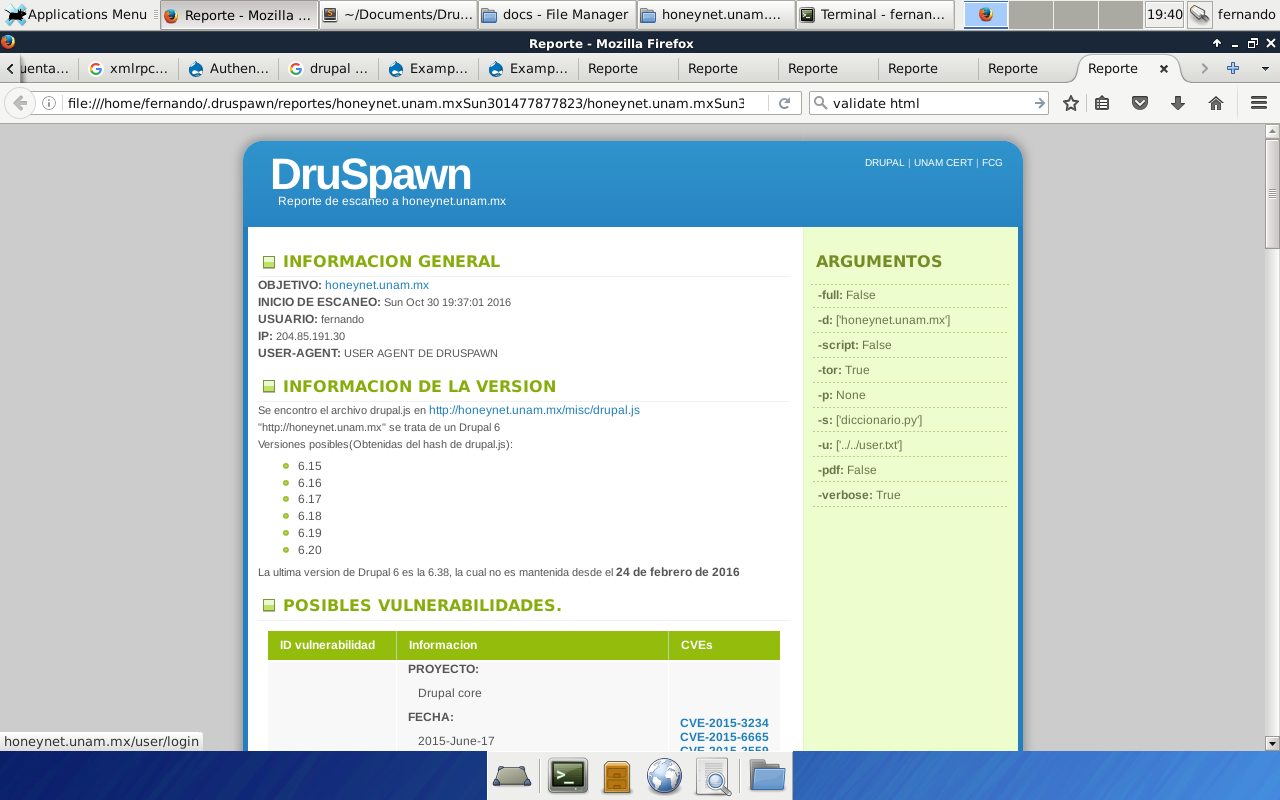
El encabezado de todo reporte, muestra a que página se realizó el escaneo.



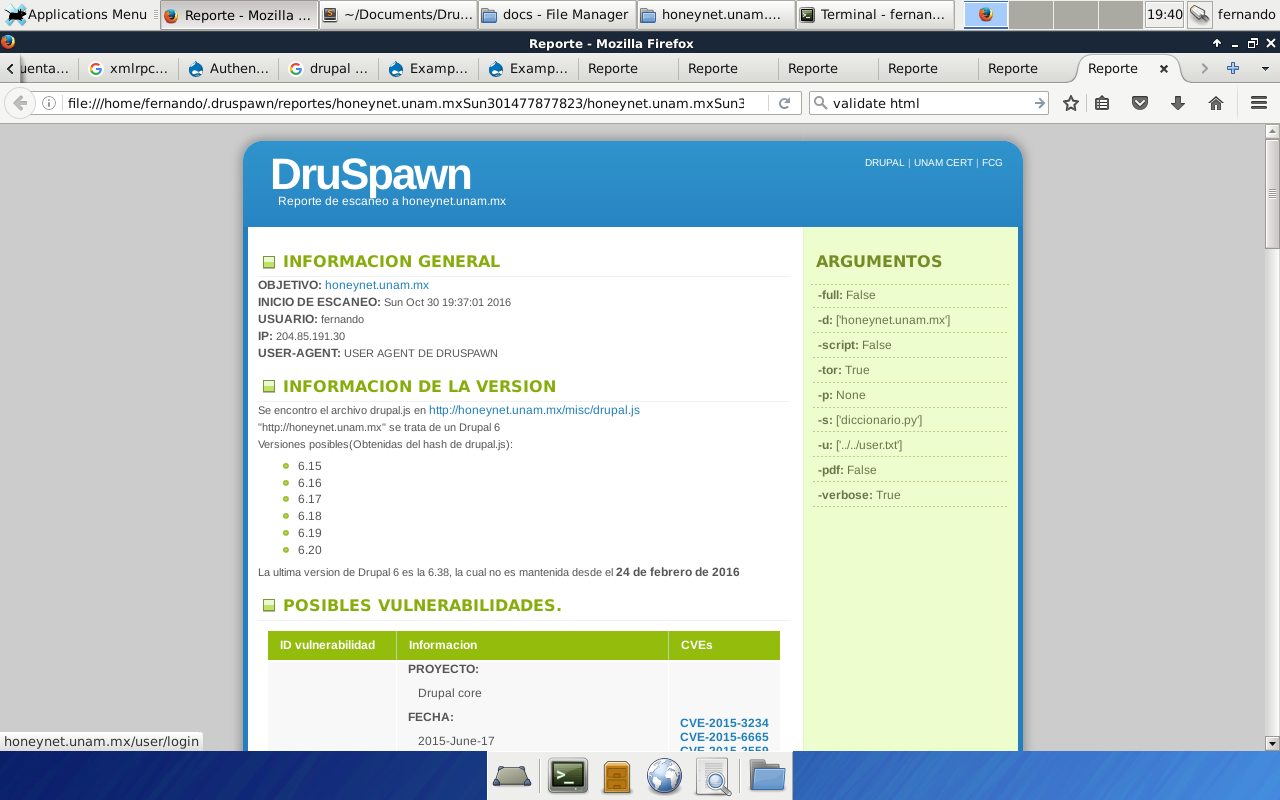
Aunque esta información se muestra mas detallada en la información general.



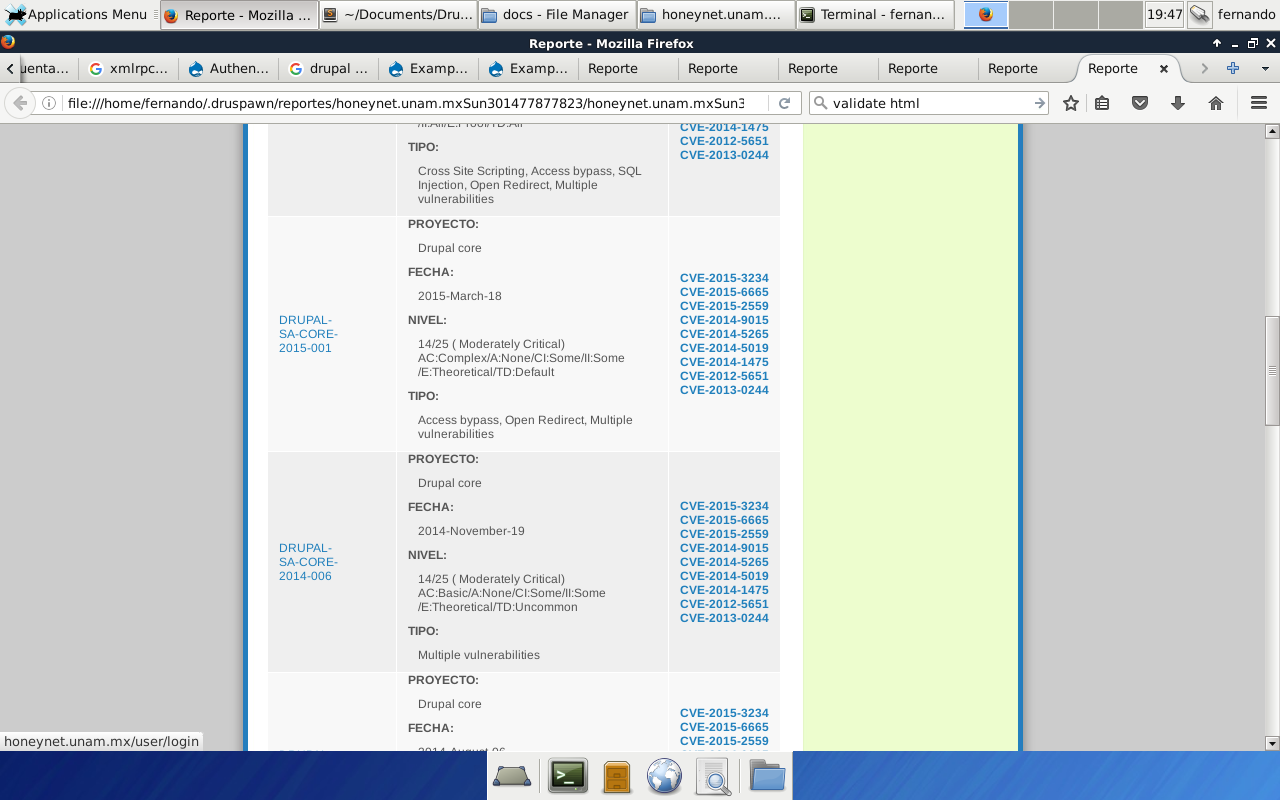
Usuario se refiere al usuario que llevo a cabo el escaneo. Además de esta información también se puede saber cuáles fueron los parámetros utilizados visualizando la barra lateral.



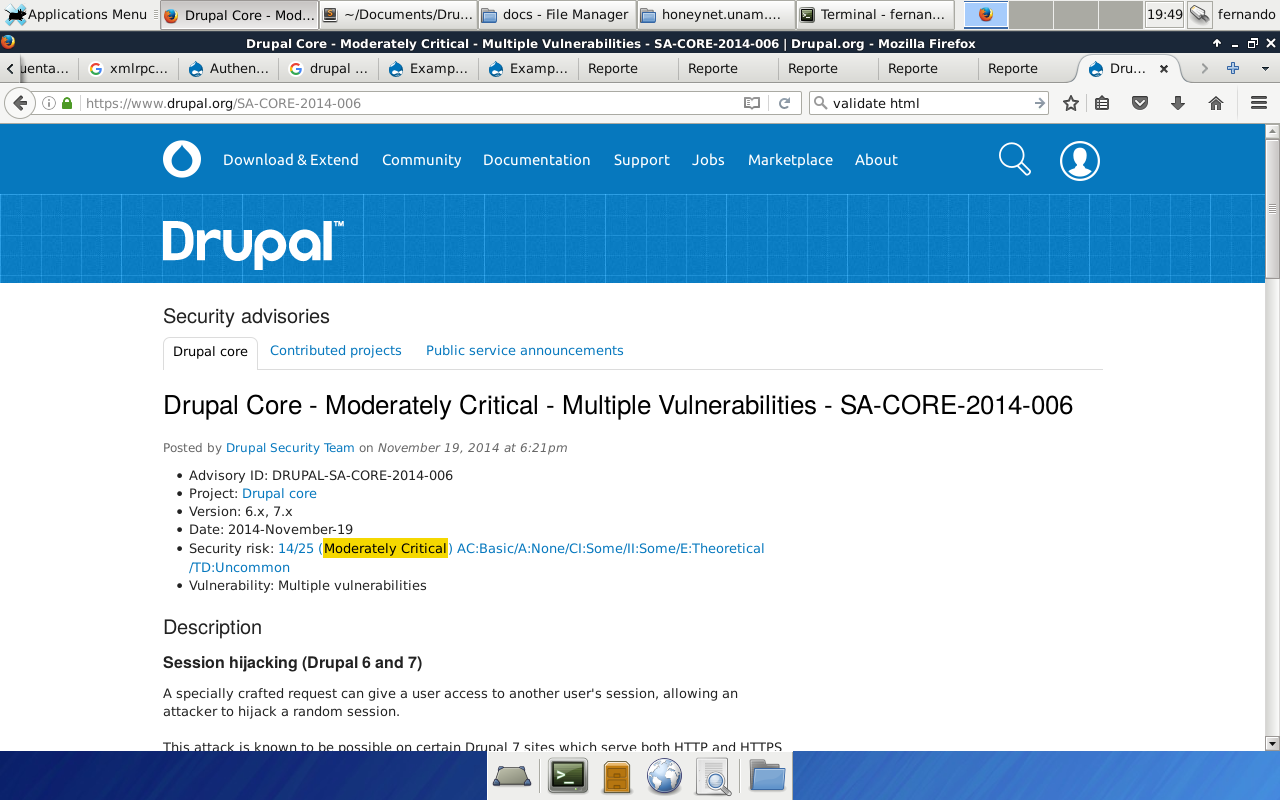
Pertinente a la información sobre la versión se mostrara una sección en la cual se describe la versión exacta o la posible versión y como se obtuvo.



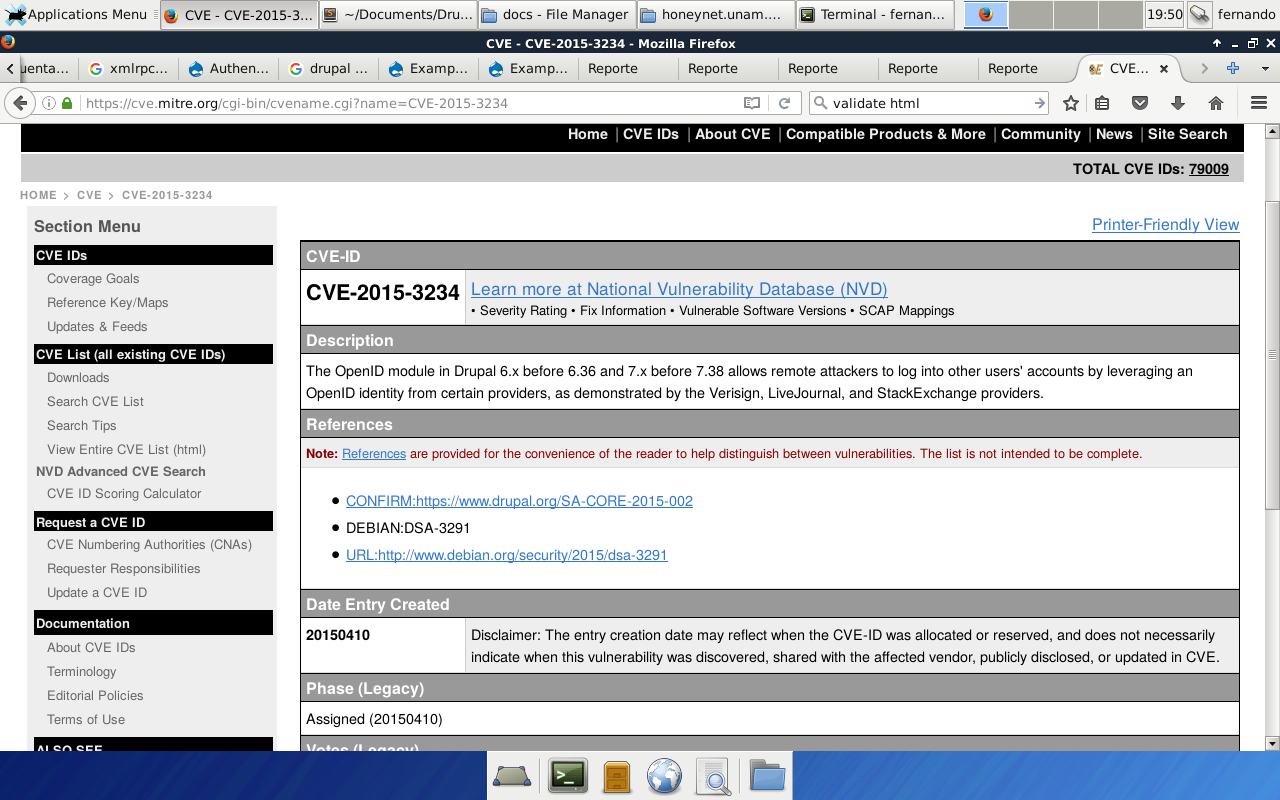
Además de una sección de vulnerabilidades para el core en cuestión. Lo importante aquí es que se puede ir al recurso a partir de este reporte, es decir, se pueden consultar los CVEs y los nodos que contienen la información de la vulnerabilidad.



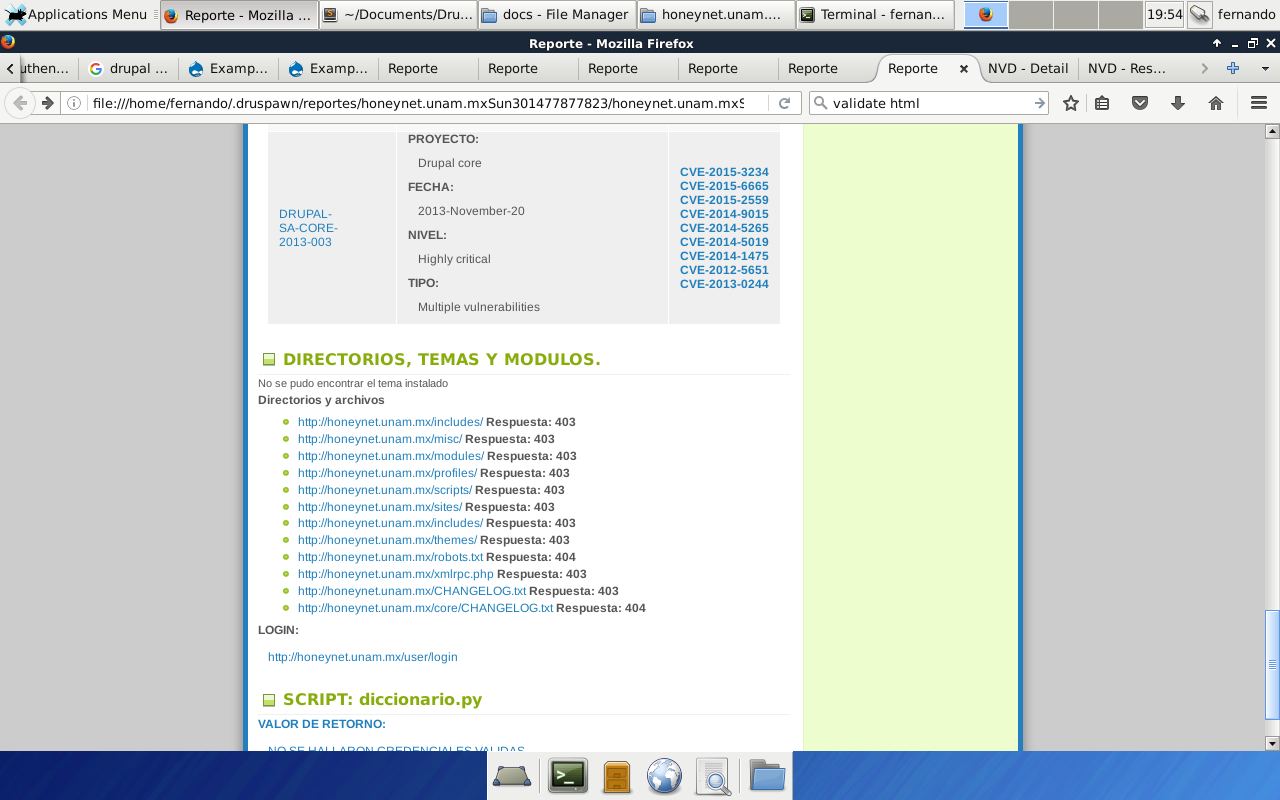
Esto con el fin de desglosar el nivel que se muestra en el reporte.



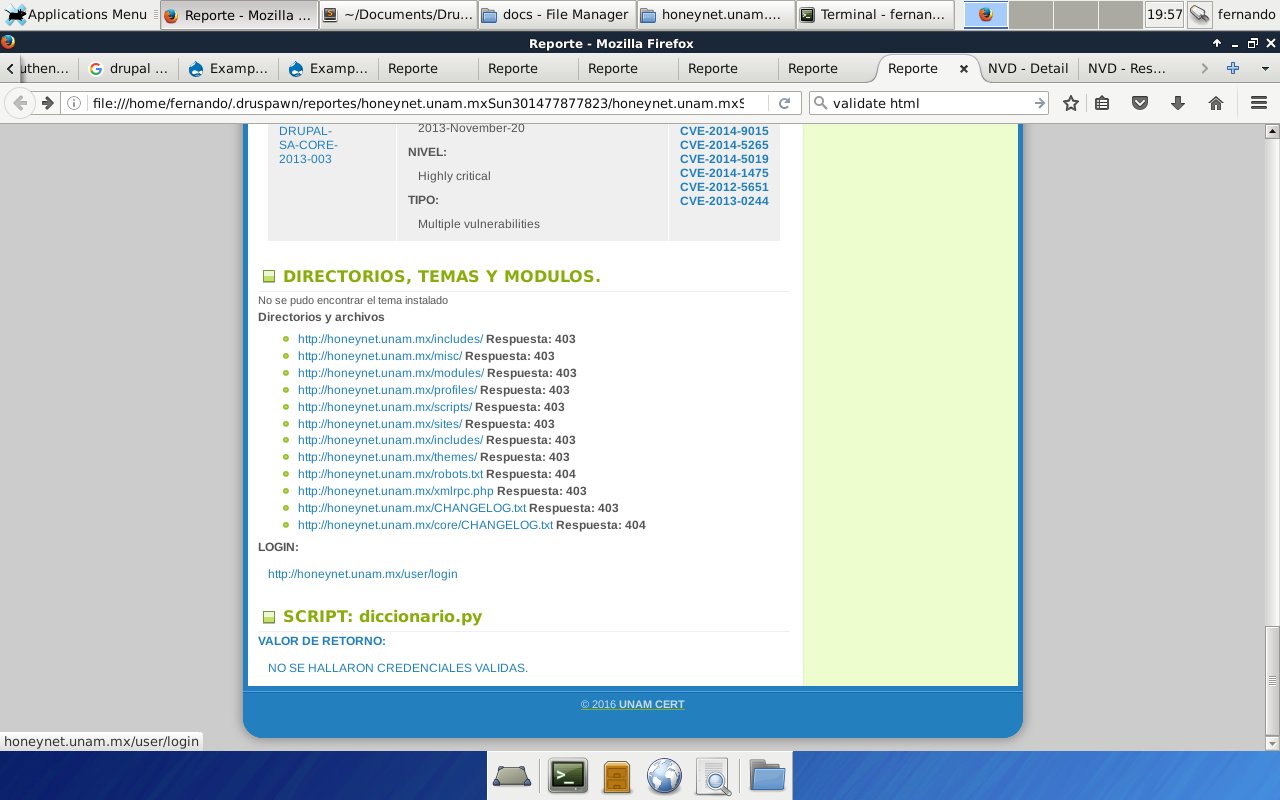
Lo mismo ocurre con los CVEs, si se sigue el enlace se abrirá en CVE en cuestión.



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.



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



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.