5° Coloquio de proyectos
de Becarios en Seguridad Informática

Herramienta para el análisis de vulnerabilidades de sitios basados en Drupal: DruSpawn

Fernando Castañeda González

UNAM CERT

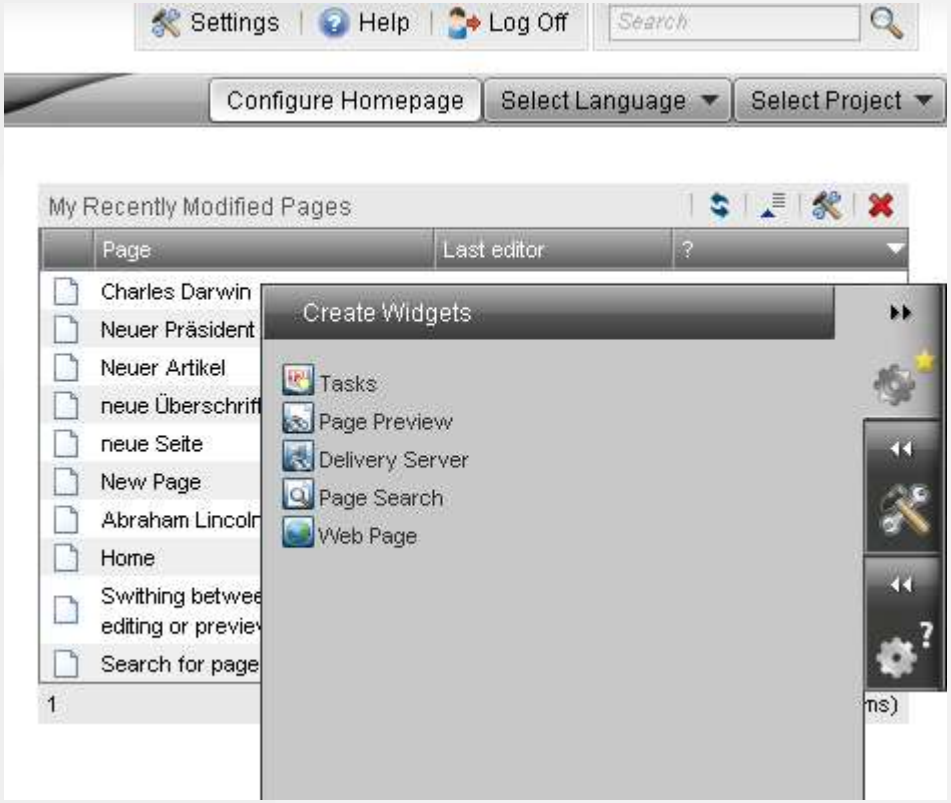
DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

ls

1. ¿Qué es un CMS?
2. Drupal y sus versiones
3. ¿Quiénes usan Drupal?
4. Estadísticas, números y demás formalidades
5. DruSpawn
6. Trabajo futuro
7. Conclusiones
8. Lecciones aprendidas

¿Qué es un CMS?

- Content Management System
- 1995 -> CNET -> Vignette -> OpenText



Fuente: http://www.cmswire.com/~/media/b56f4ee07e534e18847240443a8f308c.png

Clasificación

Por su finalidad:

- Blogs
- Foros
- Galerías
- Wikis
- Educación
- Comercio
- Almacenamiento de archivos
- Portales web

Drupal

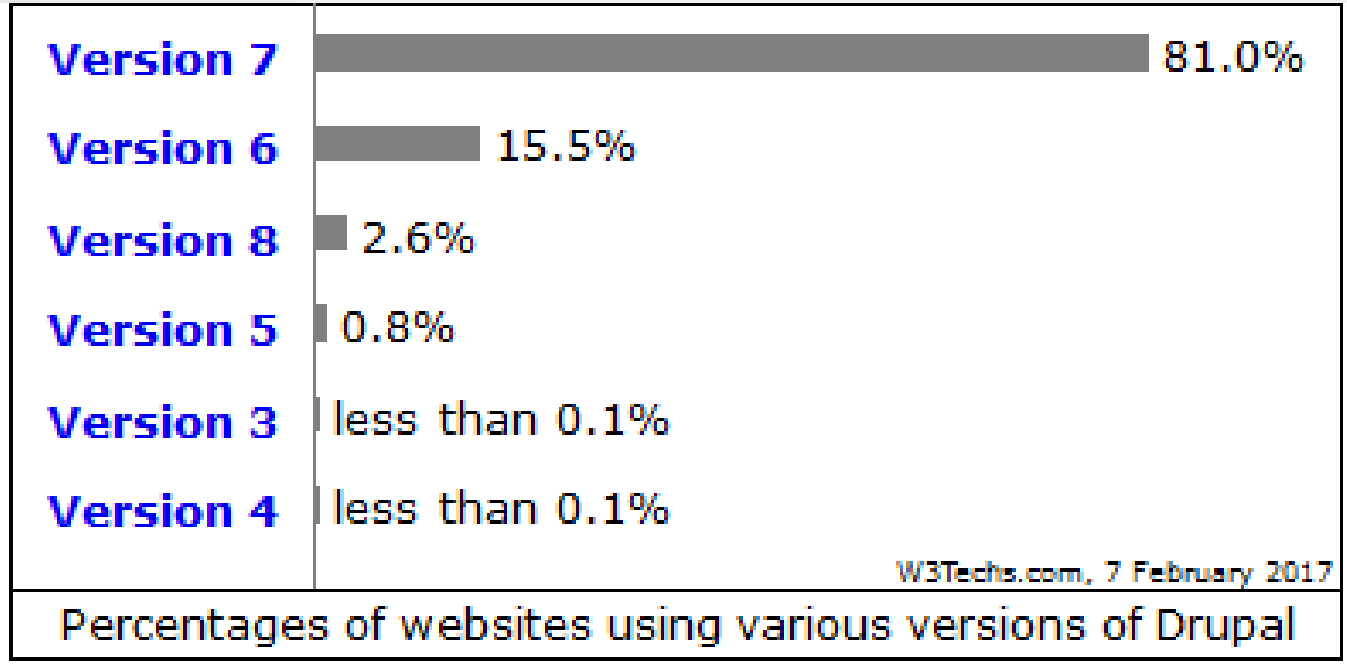
- Lanzamiento de primera versión: 1-Enero-2001
- **Dries Buytaert**

¿Qué tan usado es Drupal?

- Drupal y su sitio oficial tiene un registro de sus usuarios, aunque solo documenta sitios “relevantes”.

Versiones

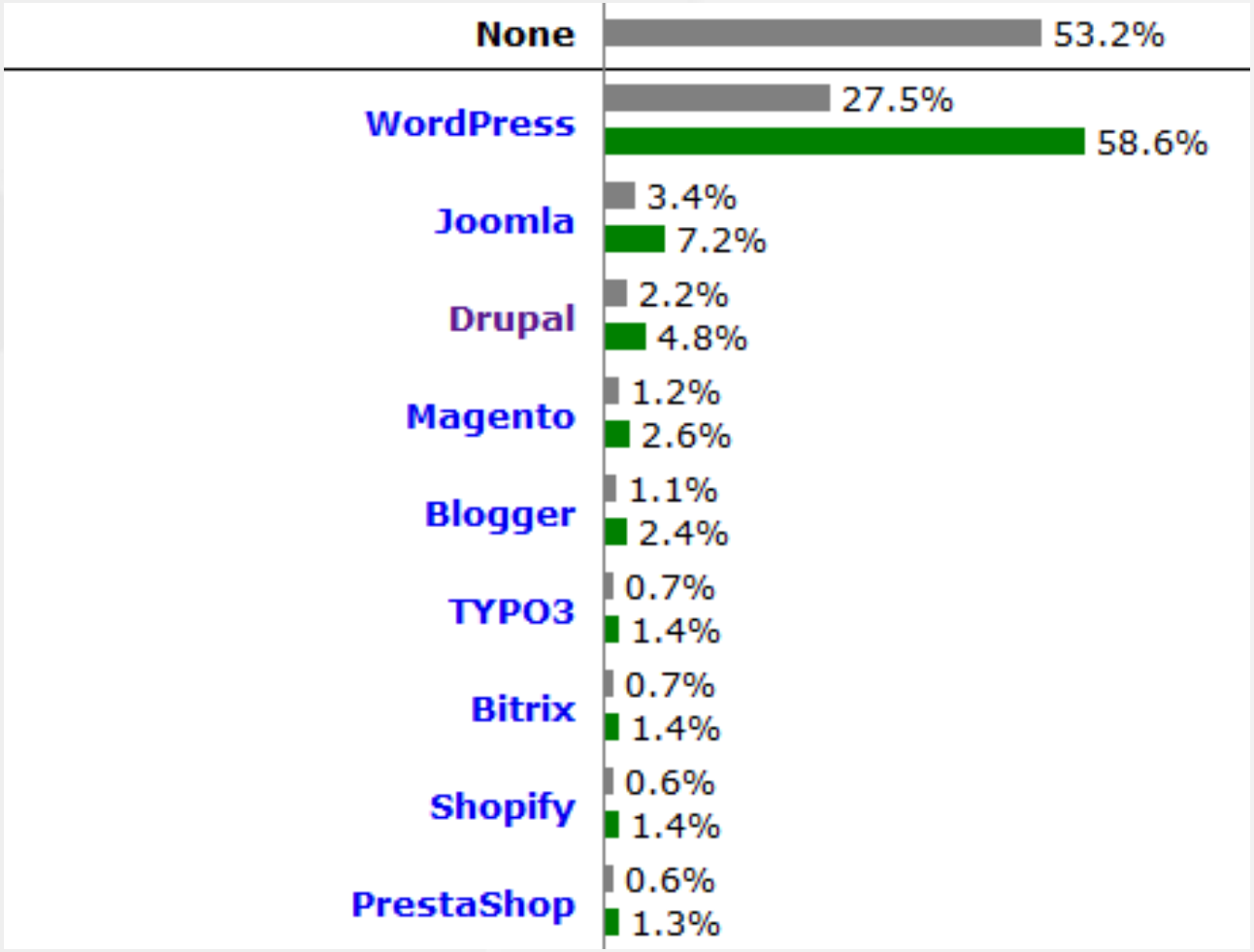
- Drupal 6
- Drupal 7
- Drupal 8



Percentages of websites using various versions of Drupal

Estadísticas

- W3techs.com



DruSpawn

- Escáner de vulnerabilidades solo para Drupal.
- Drupal.org facilita la búsqueda de vulnerabilidades.
- Hecho en Python(2.7).

DrupalScan

- Existe una gran cantidad de programas o escáneres que buscan características especificas de Drupal, como versiones, módulos instalados, temas instalados, entre otras.

- Con solamente una única característica suele venderse a precios elevados.

(https://www.whitefirdesign.com/version-check-for-drupal?pk_campaign=VCD-Chrome)

¿Qué hace DruSpawn?

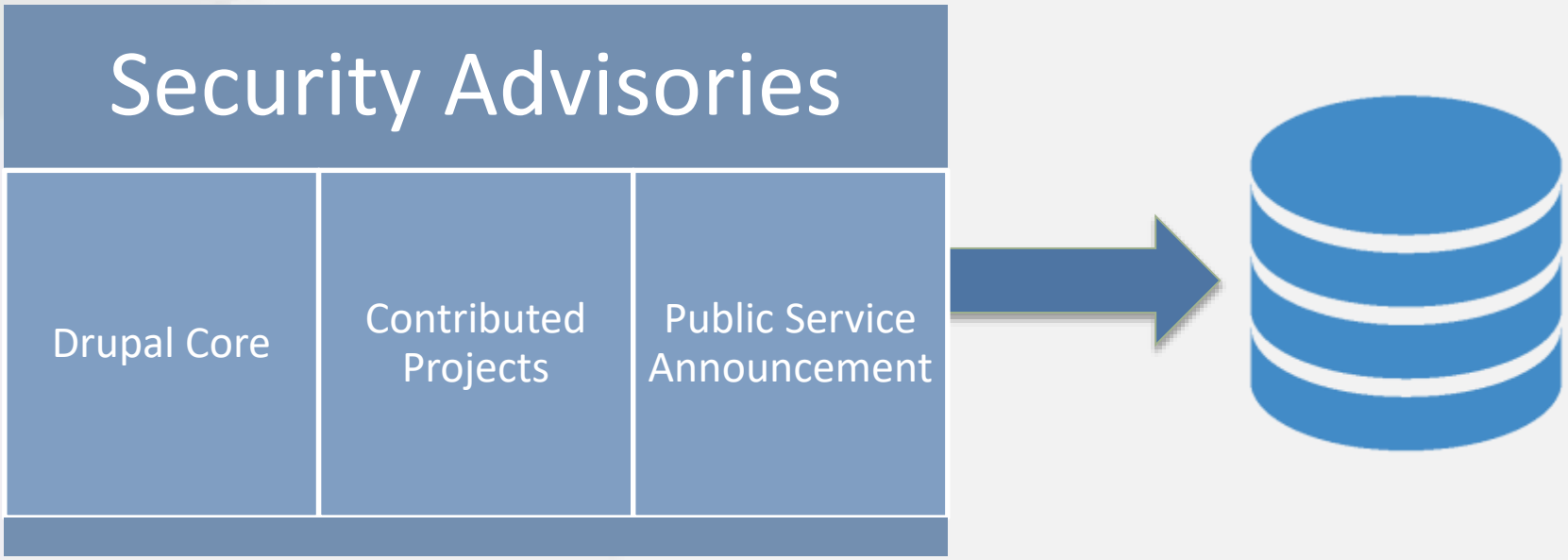
- Listar módulos
- Listar temas
- Listar páginas comunes y archivos de configuración
- Versión de Drupal
- Listar vulnerabilidades basado en temas, módulos, versiones y archivos de configuración encontrados

¿Cómo lo hace?

- Muchas cosas son públicas y están del lado del cliente.
- Vulnerable por defecto.
- Los headers dicen más de lo que deberían.
- Python es increíble para explorar la red de manera automática.
- Los hashes de los archivos del lado del cliente permiten saber la versión especifica.
- La base de datos es la llave, en ella esta todo.

¿Base de datos?

- Las vulnerabilidades de Drupal son publicadas periódicamente como Security Advisories.
- ¿Una alerta de seguridad deriva siempre en una actualización?



Instalación

- Utilizando el script **install.sh**
- Instala dependencias automáticamente
  - tor, bs4, sqlite3, entre otras
- Genera la base de datos durante la instalación o se puede utilizar la base de datos por defecto de la herramienta

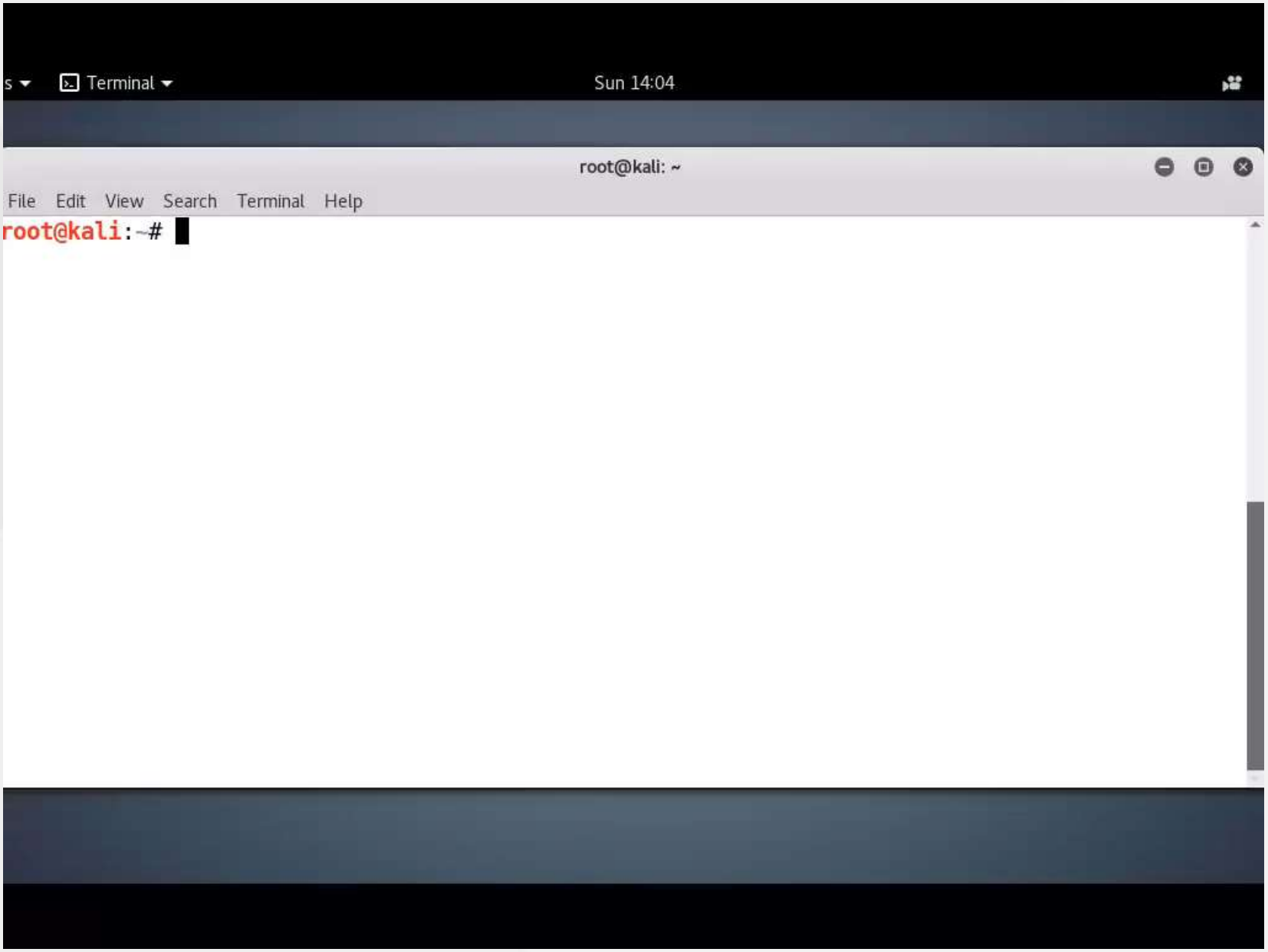
```
CREANDO DIRECTORIO /opt/druspawn
CREANDO DIRECTORIO PARA USUARIO...
Se mantendran directorios en /home/*/ de instalacion previa...
Instalando directorios en /root/ para superusuario...
Moviendo archivos necesarios a /opt/druspawn
¿Desea utilizar la base de datos que viene con el programa, o desea crear una prop
tro caracter para utilizar la base de datos por defecto. ]
N

INSTALACION FINALIZADA, DISFRUTE :)
```

Ejecución

- Tras la instalación se utiliza como herramienta del sistema

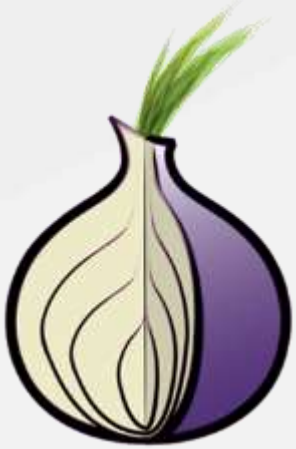
```
root@kali:~/Documents/DruSpawn# druspawn -d honeynet.unam.mx --tor
[*] Utilizando tor...
 [**] Inicializando escaneo a honeynet.unam.mx

[***]Reporte generado en:
 /root/.druspawn/reportes/honeynet.unam.mxSun121486925429/honeynet



[***] Ejecucion finalizada 80.1752679348 segundos transcurridos...
```

Acción…


s
Terminal
Sun 14:04
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#

Valores agregados

- ¿Anonimato?



```
root@kali:~# druspawn -d https://honeynet.unam.mx -v --tor
[**] Modo verboso habilitado
[*] Utilizando tor...
[*]  Se asigno la IP: 93.115.95.205
[**] Inicializando escaneo a https://honeynet.unam.mx
[**] Se encontro el archivo drupal.js en https://honeynet.unam.mx/misc/drupal.js
```

- También se puede usar algún proxy, aunque ese proceso no es automatizado.

Valores agregados

- Script propios

```
[**] Modo verboso habilitado
[**] Ejecutando unicamente script diccionario.py sobre http://192.168.1.148/drupal-7.51

[=>>] Se probara 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 3.10045909882 segundos transcurridos...
```

- Un manual de creación de scripts se descarga junto con la herramienta

¡Reportes!

Se generan automáticamente.

Compatibilidad y ¿dónde conseguirlo?

- Compatible con:
  - Sistemas derivados de Debian
  - Sistemas derivados de RedHat
  - BlackArch
  - BSD…

- UNAM-CERT, Departamento de Auditoría y Nuevas Tecnologías

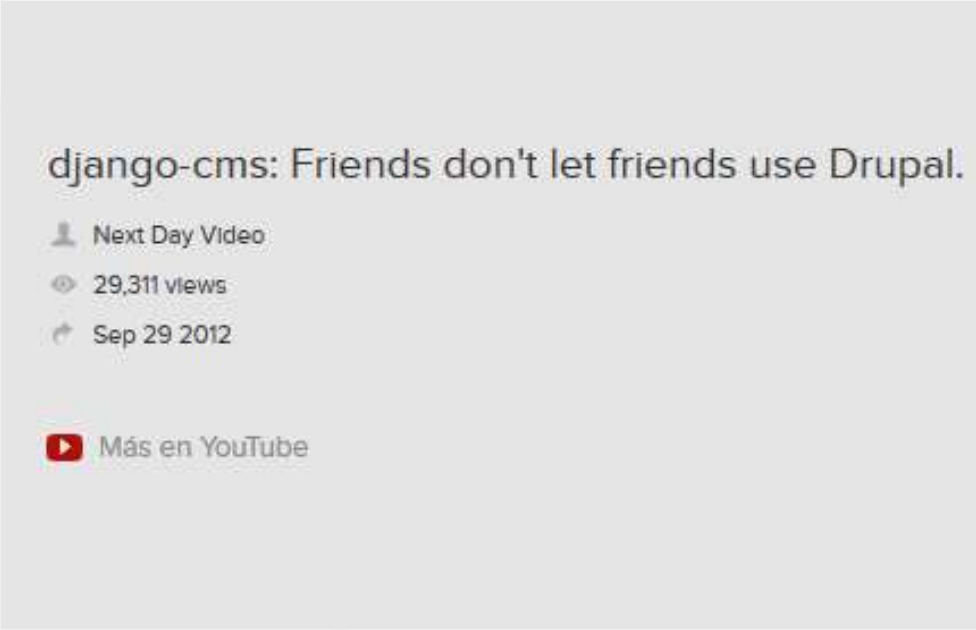
Trabajo futuro

- *Implementar y desarrollar nuevos scripts*
- Mantener el proyecto actual
- Implementar nuevos métodos de escaneo
- Compatibilidad con Windows

Conclusiones

Drupal es ampliamente usado y es una tecnología en la cual se confía demasiado; Drupal por sí solo no es una mala tecnología, podemos atribuir sus problemas de seguridad a quienes lo administran.

Un escaneo de vulnerabilidades no tiene solamente una finalidad maliciosa. Usar un escáner puede incluso ser benéfico, entonces ***¿por qué no usar DruSpawn?***



VI. Lecciones aprendidas

- Los arreglos de cuatro dimensiones tienen un uso real.
- La serialización es un conocimiento básico y muy útil cuando de realizar proyectos se trata.
- Los conocimientos en programación son básicos en seguridad informática.

¡¡GRACIAS!!

Fernando Castañeda González

CSIRT-CIC IPN / UNAM-CERT

https://fcastaneda.herokuapp.com/

6665726e616e646f@gmail.com