DGTIC UNAM CERT

Escáner de vulnerabilidades para aplicaciones Web y gestores de contenido

Denise Betancourt Sandoval
Omar Alí Domínguez Cabañas
Rodrigo Augusto Ortiz Ramón

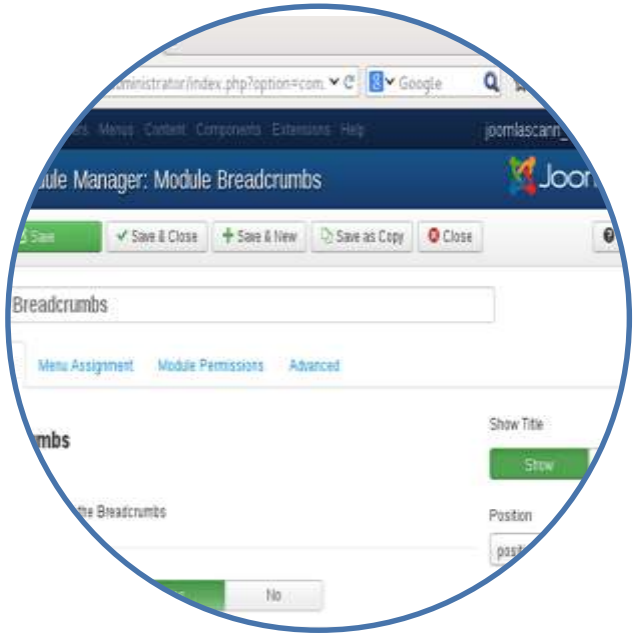
Problemática

- Pruebas de penetración como una de las principales actividades del UNAM-CERT.
- Automatización del proceso de análisis de vulnerabilidades conocidas.
- Combinación de varias herramientas para compensar debilidades y disminuir falsos positivos.
- Ahorrar tiempo al especialista en pruebas de penetración.

Objetivo

- Crear una herramienta para optimizar y automatizar el escaneo de vulnerabilidades a sitios y aplicaciones Web, así como a gestores de contenido, tratando de encontrar y explotar vulnerabilidades específicas y bien conocidas.

Visión general



SGC (**CMS** en inglés)

Crear, administrar, actualizar y dar mantenimiento a un sitio web de un modo sencillo

Alcance

- Búsqueda y explotación de vulnerabilidades, especialmente las mencionadas en el Top 10 de OWASP 2013, a sitios y aplicaciones Web, así como a los CMS de mayor uso en dependencias de la UNAM y líderes en el mercado: Wordpress, Drupal, Joomla y Moodle.

OWASP
The Open Web Application Security Project

Uso de CMS dentro del dominio “unam.mx”

Moodle
- site:unam.mx inurl:moodle
- Cerca de 4,730 resultados

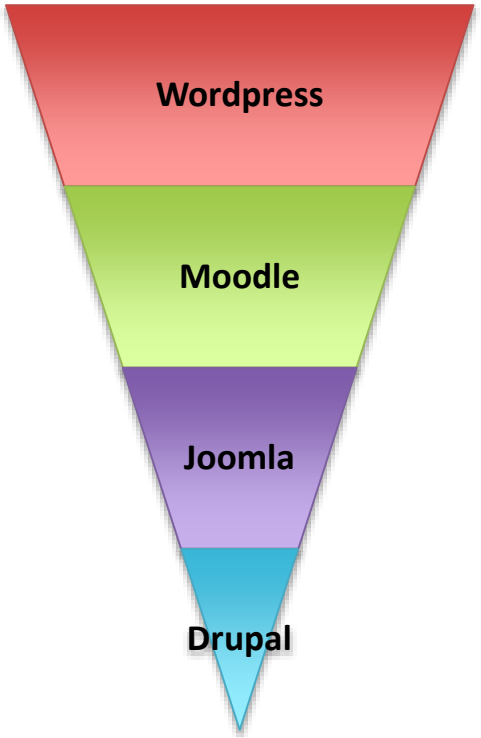
Wordpress
- site:unam.mx inurl:wordpress
- Cerca de 2,650 resultados

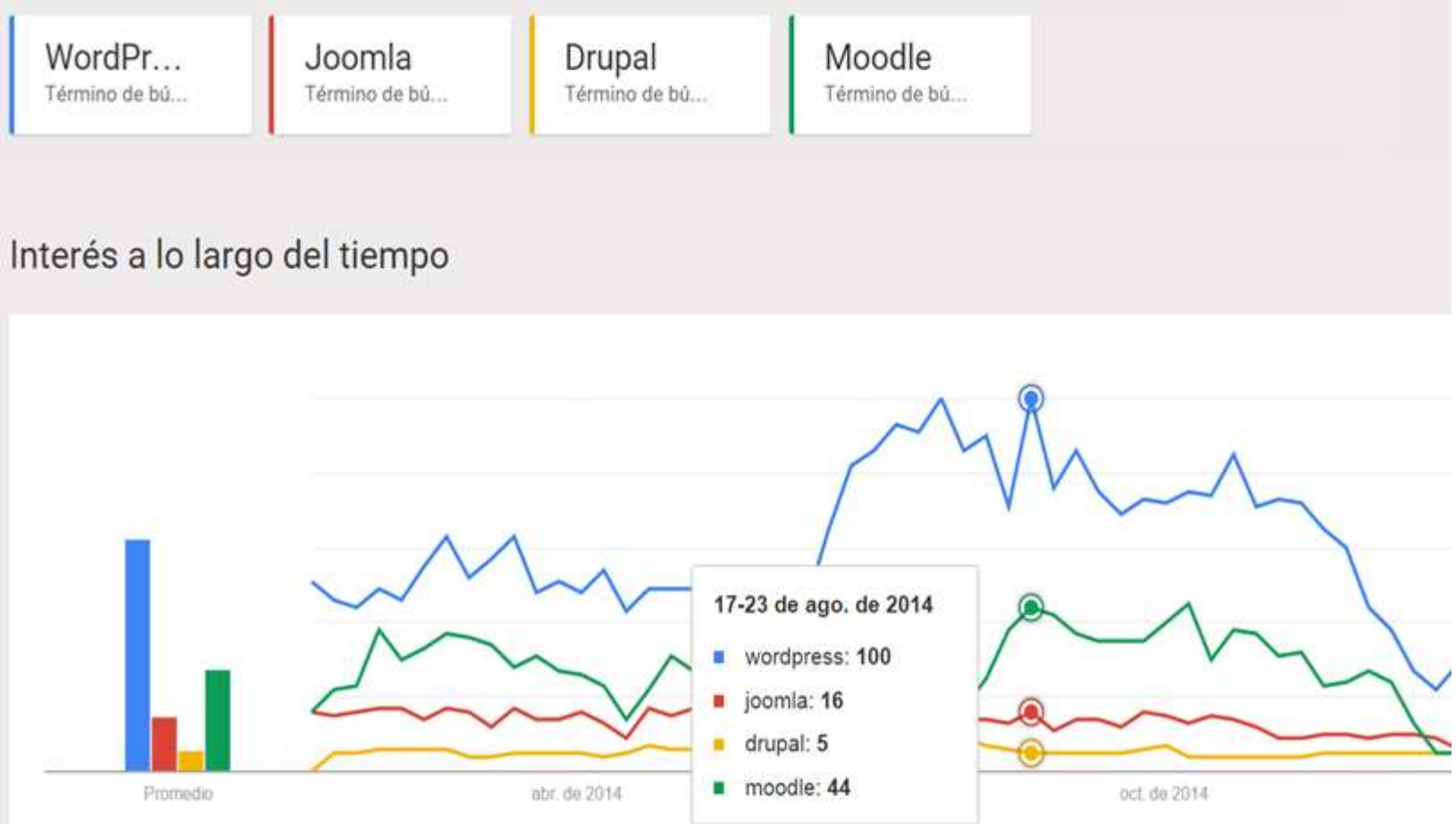
Drupal
- site:unam.mx inurl:drupal
- Cerca de 2,330 resultados

Sharepoint
- site:unam.mx inurl:sharepoint
- Cerca de 379 resultados

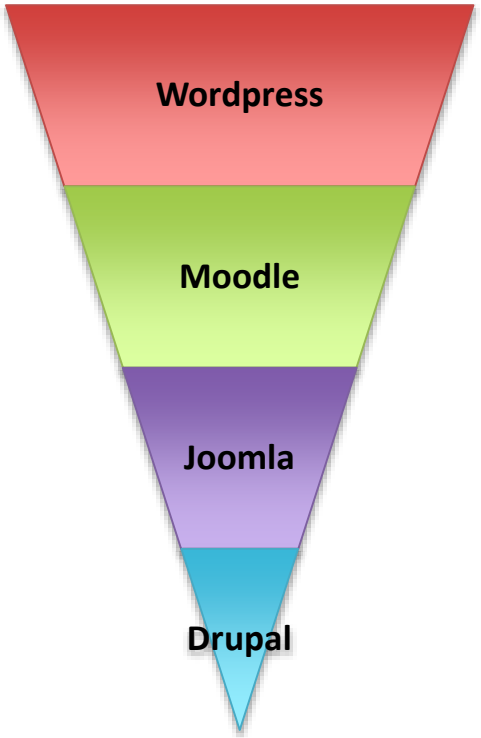
Joomla
- site:unam.mx inurl:joomla
- Cerca de 366 resultados

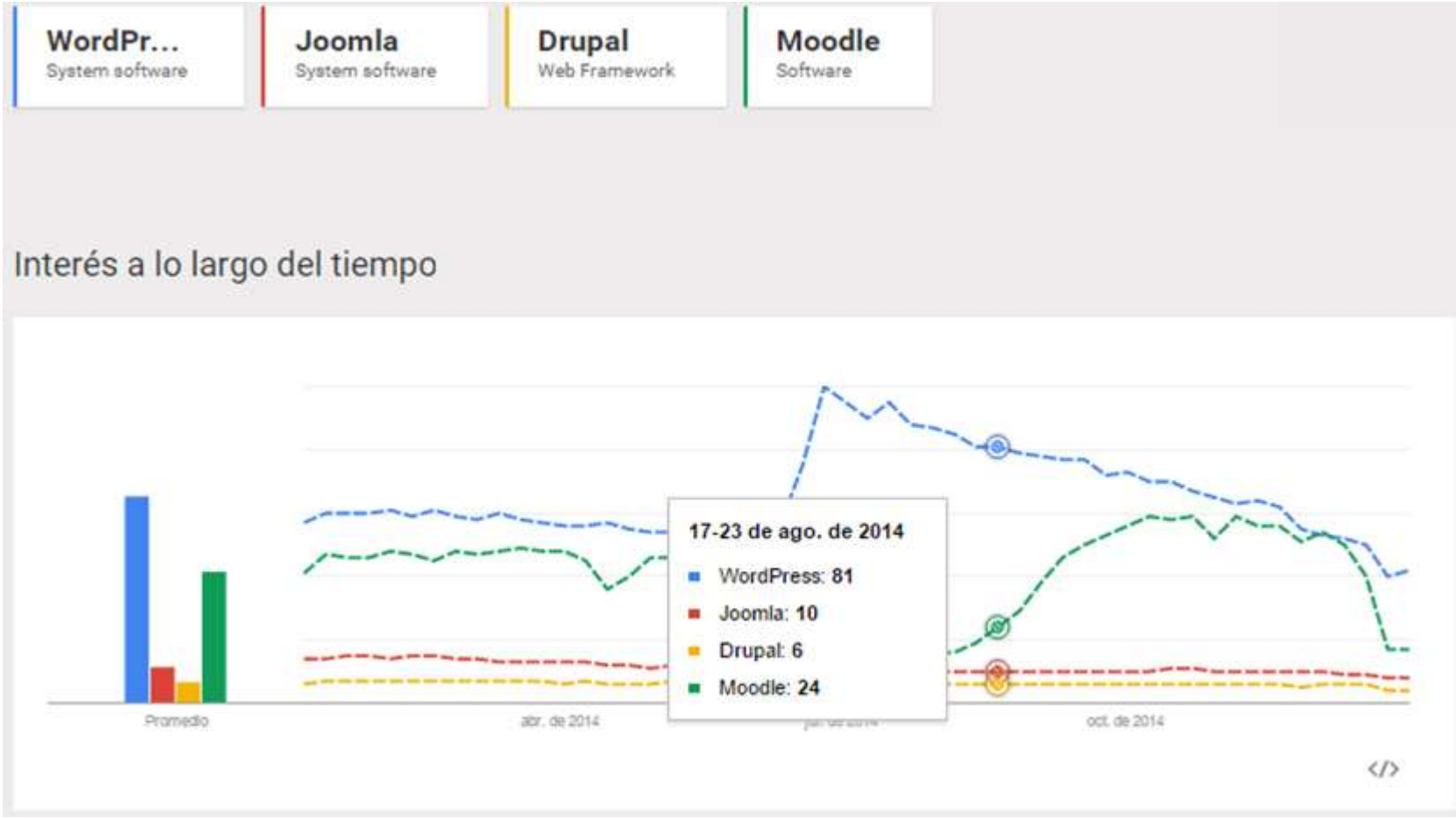
CMS líderes en el mercado (DF)





CMS líderes en el mercado (Mundial)





DGTIC UNAM CERT

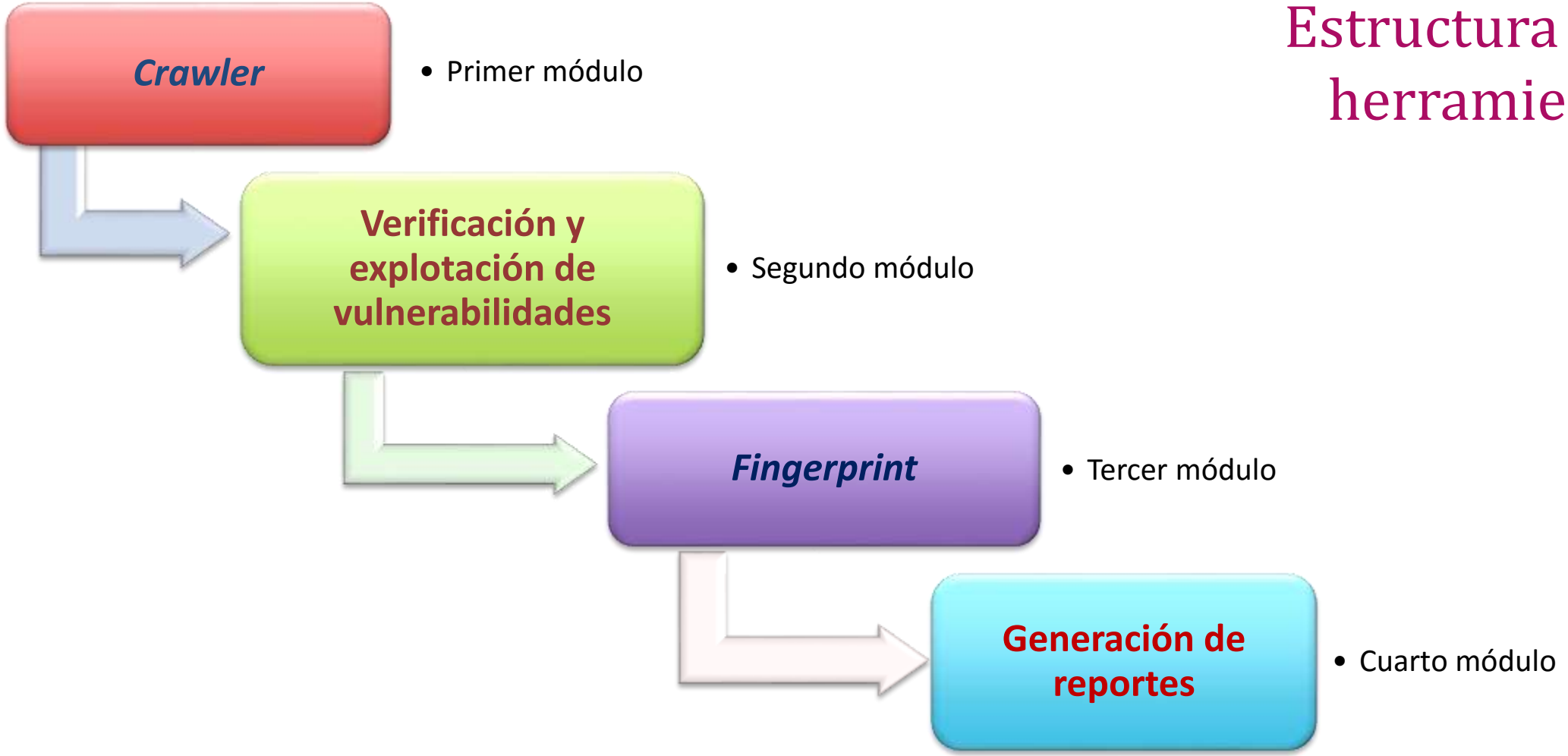
CrawlitaSmasher

python powered

- Crawler
- Análisis de vulnerabilidades web
- CMS fingerprint

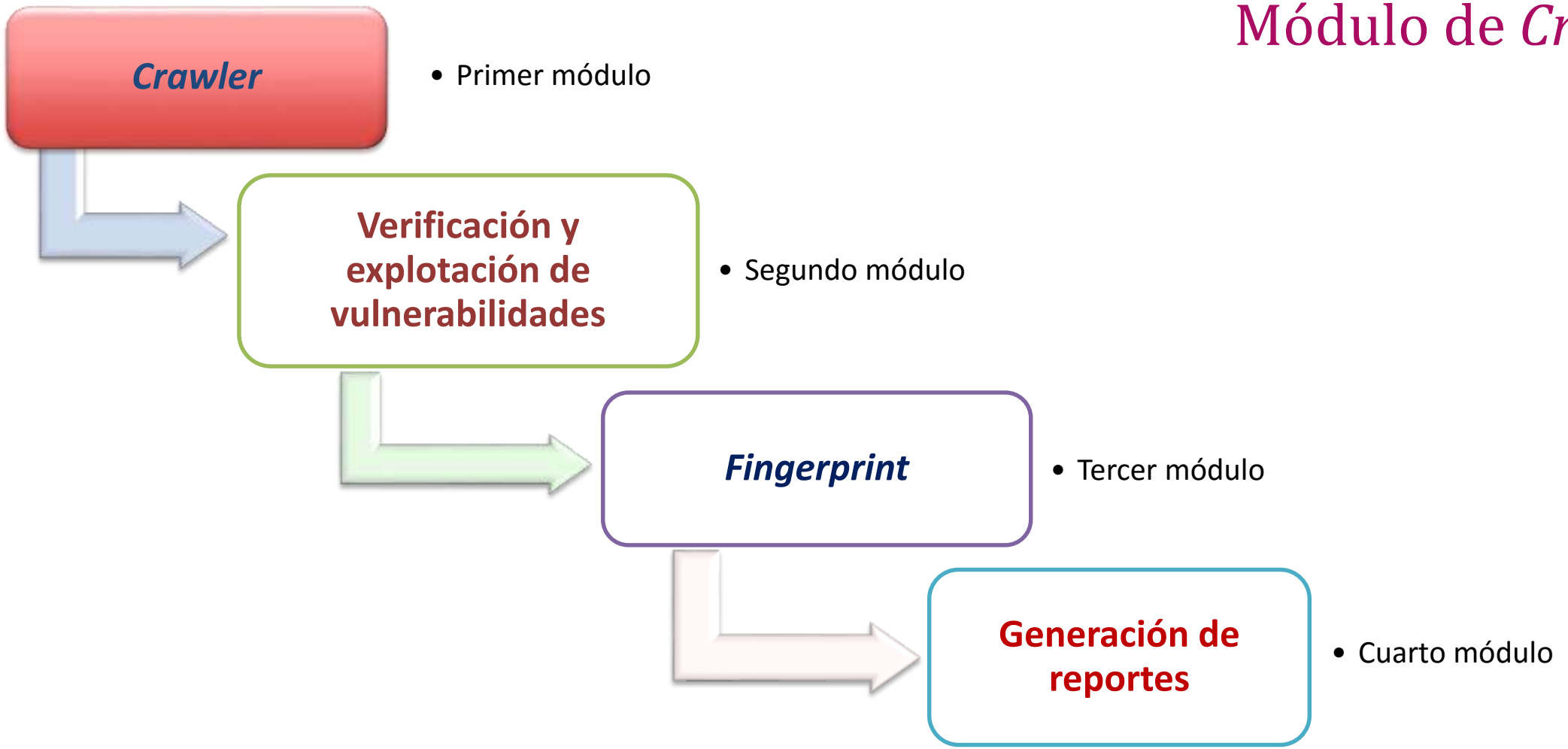
Coloquio de proyectos de Becarios en Seguridad Informática 3er

Estructura de la herramienta



- Primer módulo
- Segundo módulo
- Tercer módulo
- Cuarto módulo

Módulo de *Crawler*



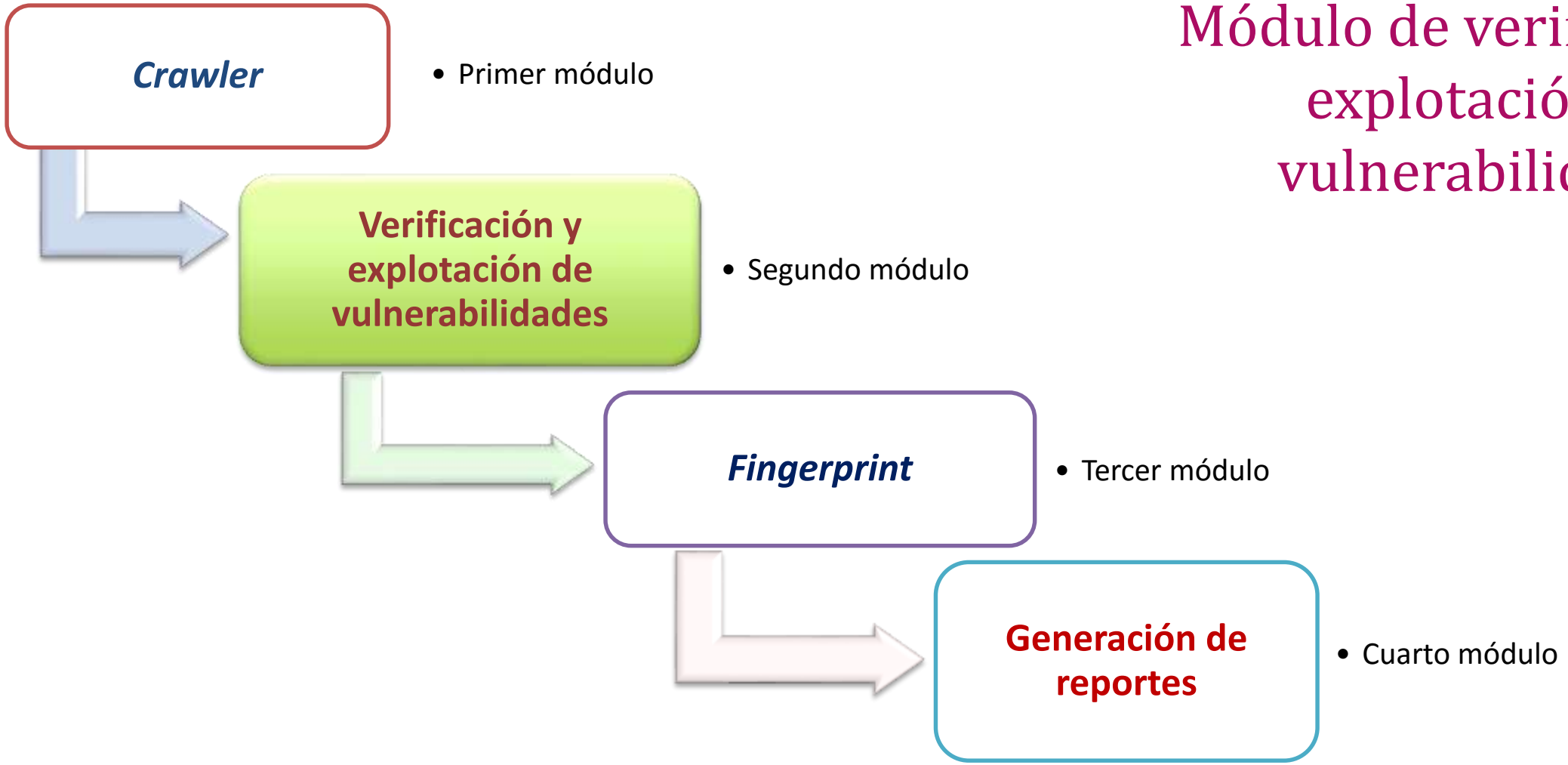
Crawler

- Módulo principal de CrawlitaSmasher
- Construido sobre mechanize, urllib, beautiful soup y requests
- Soporte completo de protocolos http y https
- Realiza el descubrimiento completo del sitio web
- Recolecta información de contacto como e-mails
- Las URL descubiertas son guardadas y visitadas en búsqueda de más información

Crawler

- Módulo de autenticación y seguimiento de sesión
  - Basic, Digest y por formulario
- Módulo de *Fuzzing*
  - Diccionario de 100 ó 43137 palabras clave
  - Encontrar recursos ocultos, sin referencias o respaldos
- Soporte de Proxy
- Cambio de User-Agent

Módulo de verificación y explotación de vulnerabilidades



Análisis de Vulnerabilidades Web

Basado en el TOP 10 OWASP

- XSS (Cross-Site Scripting)
- CSRF (Cross-Site Request Forgery)
- RFI/LFI (Remote/Local File Inclusion)
- SQLi (SQL Injection)

XSS – Cross-Site Scripting

- Motores de simulación completa de cliente web
- Selenium WebDriver – url y formularios
- Dryscrape – url y cabeceras
- Inyección y auto-codificación de 46 payloads (escalables)
- Interpretación completa de código script
- Soporte completo de seguimiento de sesión y proxy

CSRF – Cross-Site Request Forgery

- Genera páginas HTML para explotar la vulnerabilidad
- Soporta peticiones de tipo: GET, POST y multi POST
- Recrea el escenario completo de una solicitud Web
- Esconde y realiza la explotación automáticamente al abrir el documento HTML

RFI/LFI – Local/Remote File Inclusion

- Realiza inyección en cabeceras, url y formularios
- Inyección y auto-codificación de 105 payloads
- Búsqueda de patrones para determinar la vulnerabilidad
- Posibilidad de determinar permisos administrativos en servidor
- Efectivo contra servidores UNIX, GNU/Linux y Windows
- Soporte completo de seguimiento de sesión y proxy

SQLi – SQL Injection

- Realiza inyección de código SQL
- Inyección de 200 payloads
- Búsqueda de patrones para determinar la vulnerabilidad
- Detección de Blind SQLi
- Soporte completo de seguimiento de sesión y proxy

Módulo de *fingerprinting*

Crawler

- Primer módulo

Verificación y explotación de vulnerabilidades

- Segundo módulo

Fingerprint

- Tercer módulo

Generación de reportes

- Cuarto módulo

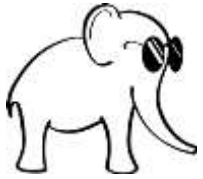
CMS Fingerprint

Algoritmo basado en ponderación y suma de puntos:

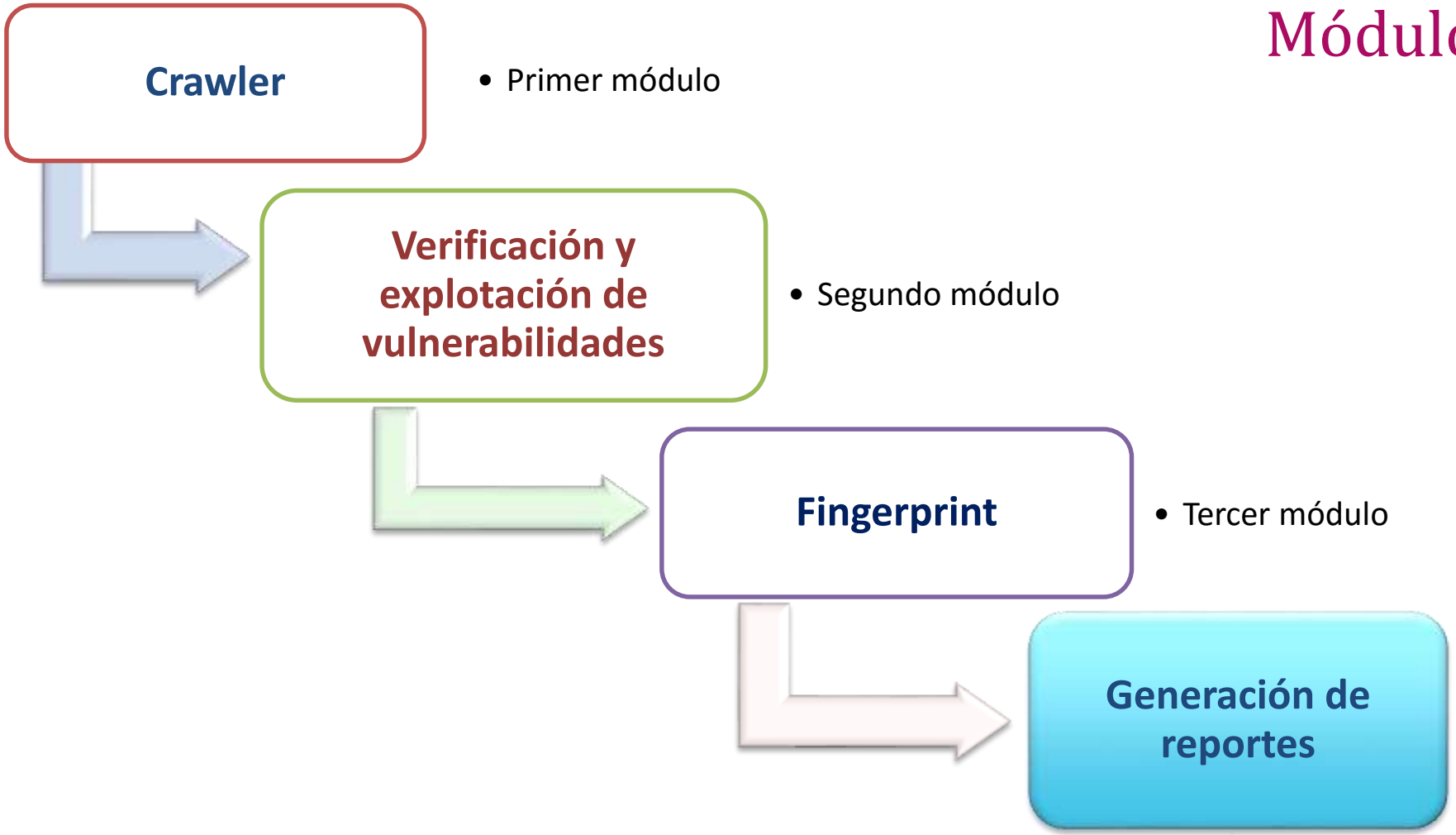
- ✓ Drupal – 225 url y recursos conocidos
- ✓ Joomla – 311 url y recursos conocidos
- ✓ Wordpress – 216 url y recursos conocidos
- ✓ Moodle – 244 url y recursos conocidos

CMS Fingerprint

- Búsqueda de patrones y análisis de respuestas del servidor
- Mejora de resultados con sesiones habilitadas
- Soporte completo de seguimiento de sesión y proxy
- Descubrimiento sobre url existentes en el CMS
- Permite el cambio de la url base de las pruebas



Módulo de Generación de Reportes

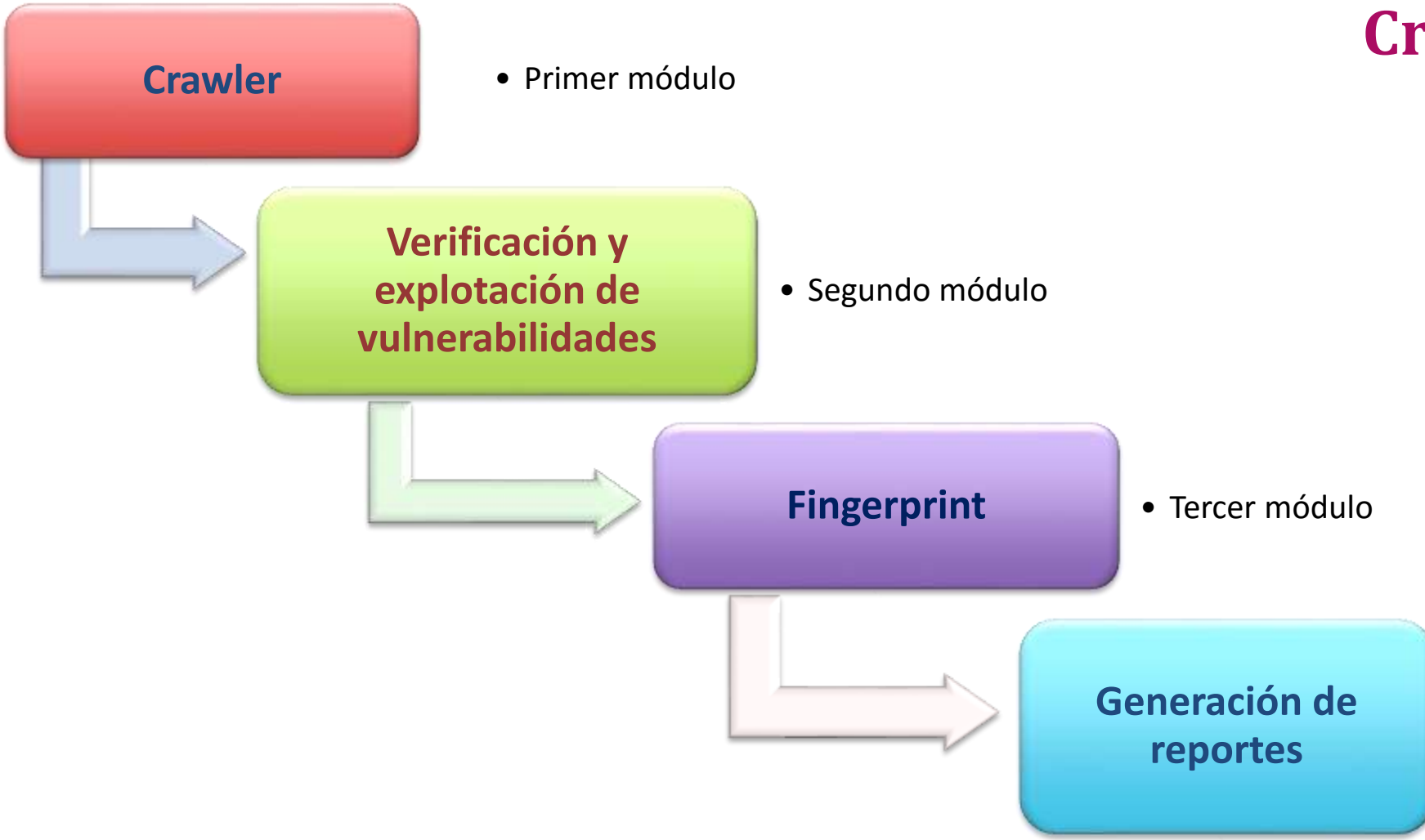


- Primer módulo
- Segundo módulo
- Tercer módulo
- Cuarto módulo

Generación de Reportes

- Al finalizar, los reportes se generan automáticamente
- Disponibles en formatos HTML y PDF
- Contienen:
  - ✓ Vulnerabilidad encontrada
  - ✓ Lugar donde se encontró
  - ✓ Payload utilizado para comprobar la vulnerabilidad
  - ✓ Calificación (criticidad)
  - ✓ Recomendaciones

CrawlitaSmasher



- Primer módulo
- Segundo módulo
- Tercer módulo
- Cuarto módulo

Demostración del funcionamiento

Problemas y Soluciones implementadas

1. Proxy

2. Multithreading
   - Rendimiento

1. Seguimiento sesión a través de los motores de detección
2. Lanzar un proceso hijo para realizar tareas (sólo en algunos casos).
   - Máquina virtual Python

Comparativa de efectividad CrawlitaSmasher

	URL encontradas en www.altoromutual.com	Vulnerabilidades en www.altoromutual.com	URL encontradas en Wivet
CrawlitaSmasher	67	XSS (5) SQLi (1) LFI (1)	5/56
Owasp ZAP	54	XSS (3) SQLi (1)	13/56
Vega	68	XSS (4) SQLi (2) FP LFI (1)	36/56
Wapiti	85	XSS (4) SQLi (3) LFI (1)	40/56

Soporte futuro y nuevas funciones

- Detección de Sharepoint como CMS
- Soporte contra códigos captcha
- Optimización de velocidad de ejecución
- Licenciamiento

GRACIAS

Denise Betancourt Sandoval
denise.betancourt@cert.unam.mx

Omar Alí Domínguez Cabañas
ing.omar.dominguez@gmail.com

Rodrigo Augusto Ortiz Ramón
rodrigo.ortiz@cert.unam.mx

Tel: 5622 8169