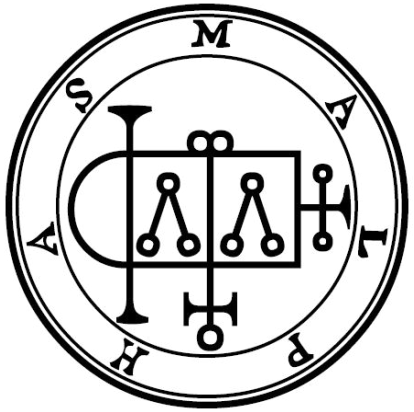
DGTIC Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Plan de Becarios en Seguridad Informática - UNAM-CERT

Herramienta para el análisis masivo y explotación de sitios Vulnerables (Malphas)

Descripción del proyecto

- Malphas es una herramienta dedicada a la validación y explotación de vulnerabilidades en sitios web
- Sirve como apoyo durante los procesos de pruebas de penetración
- Al finalizar la ejecución del programa, la herramienta entrega reportes con la información correspondiente a cada uno de sus módulos



Objetivos de la herramienta

- Apoyar a la identificación, validación y explotación de vulnerabilidades
- Reducir el tiempo de análisis de una aplicación
- Generar reportes sobre el estado actual del sitio

Componentes

Obtención de información

Análisis

Exploits y explotación

Fuzzing

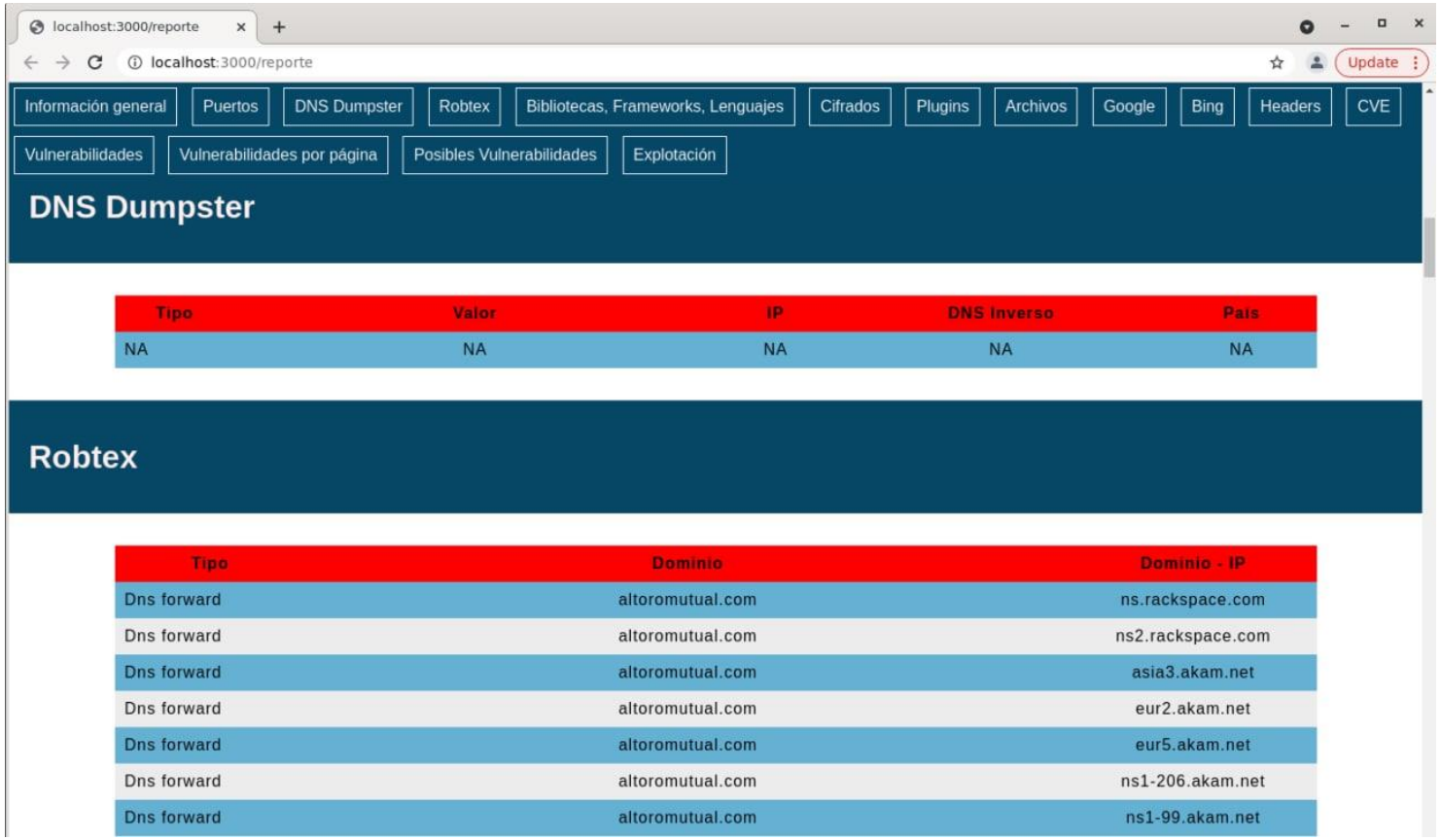
Consultas y Reportes

Alertas

Ejecución

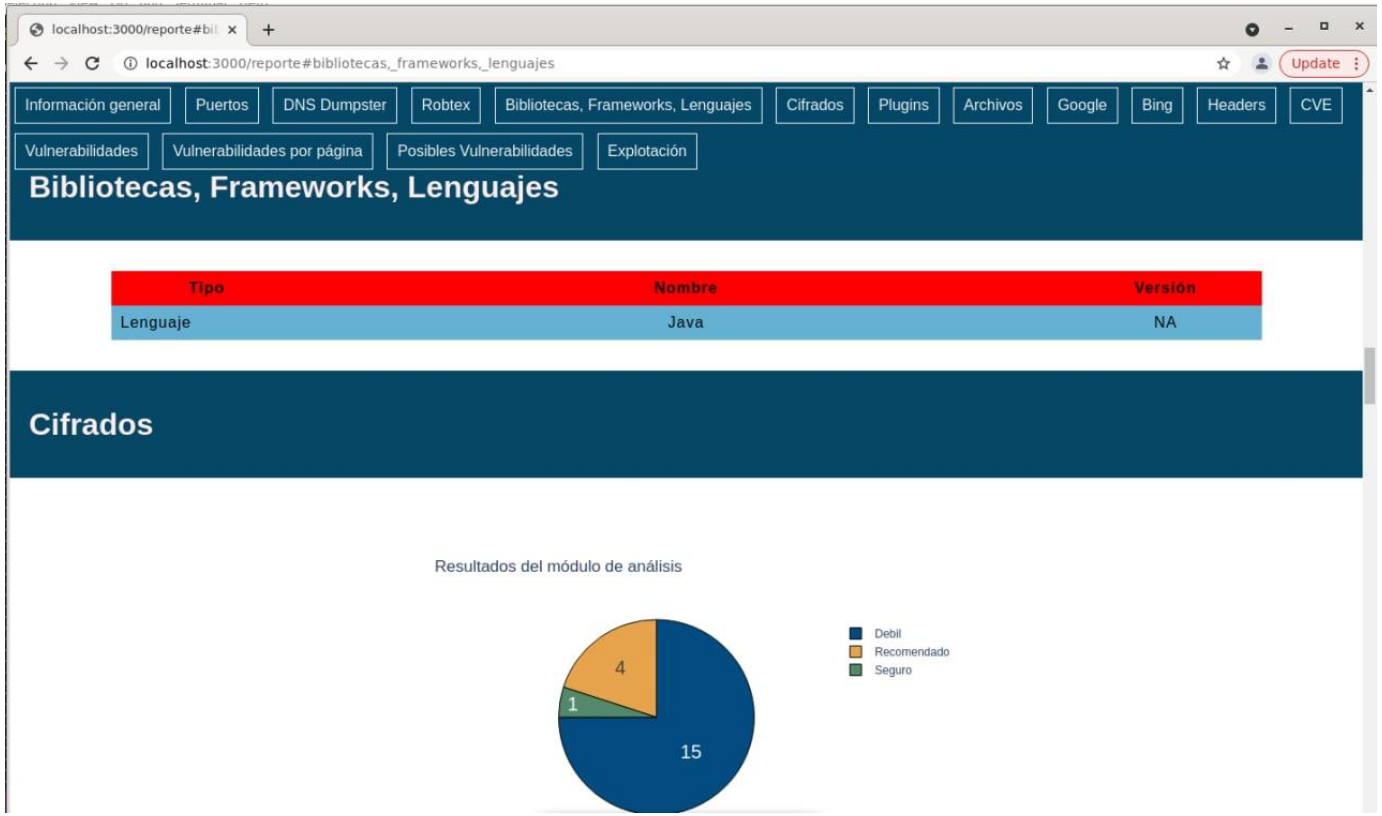
Componentes - Obtención de información

- Obtención de información
- Búsquedas
  - Google
  - Bing
- Robtex
- DNSDumpster
- Ipv4Info
- Scanner de puertos



Componentes - Análisis

- Información del sitio web
  - Versión del servidor
  - Plugins, módulos, recursos
  - Framework, bibliotecas, lenguajes
- Configuración del sitio web
- Listado de páginas
- Indicadores de compromiso



Componentes - Exploits y Explotación

- Identificación de componentes vulnerables
- Proceso de validación de vulnerabilidades

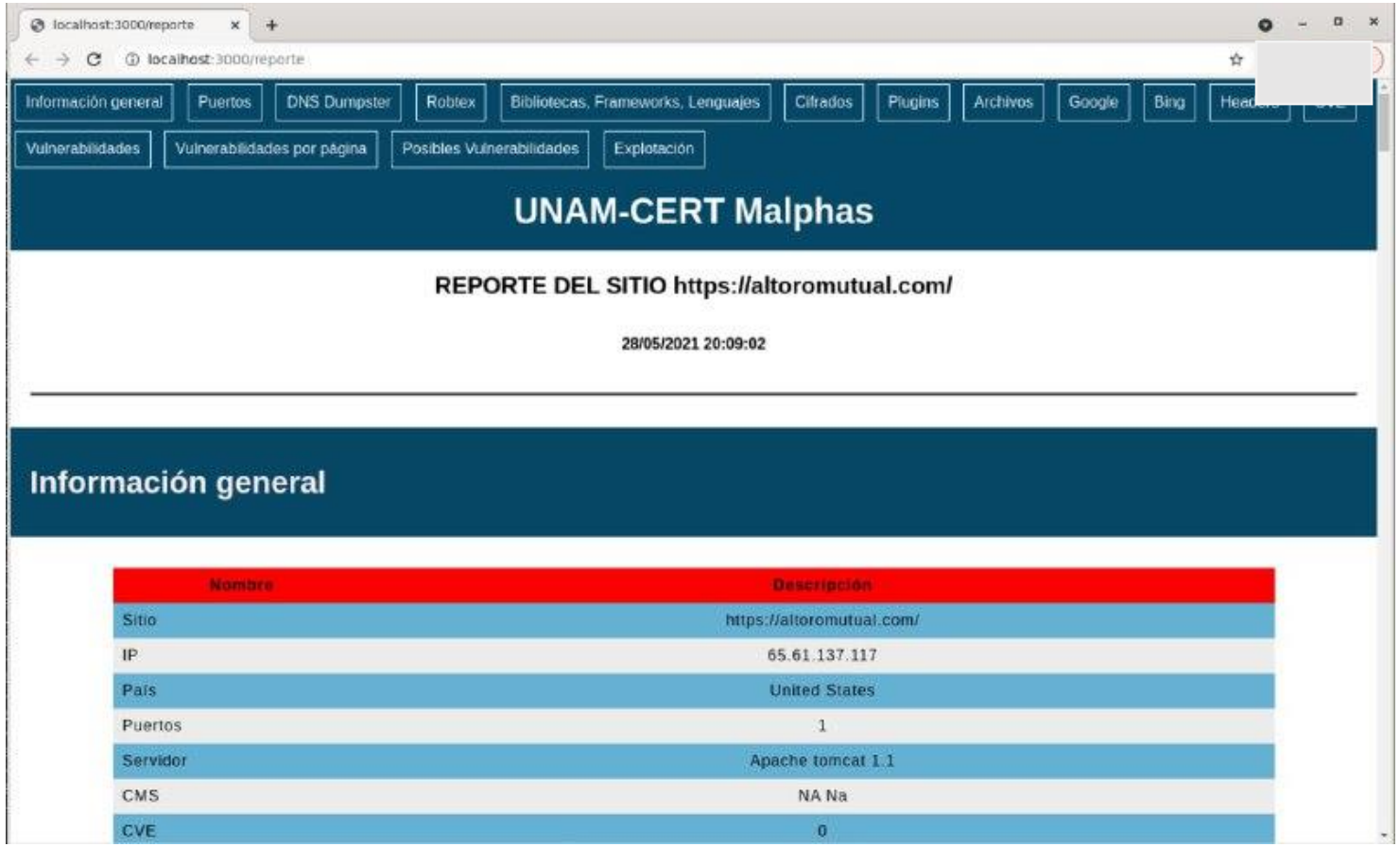
Componentes - Fuzzing

- SQLi
- XSS
- LFI
- File Upload

```
Iniciando Fuzzing
http://testphp.vulnweb.com/
http://testphp.vulnweb.com/index.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/artists.php
---------> http://testphp.vulnweb.com/artists.php ParseResult(scheme='http', net
loc='testphp.vulnweb.com', path='/artists.php', params='', query='', fragment=''
)
---------> http://testphp.vulnweb.com/categories.php ParseResult(scheme='http',
netloc='testphp.vulnweb.com', path='/categories.php', params='', query='', fragm
ent='')
---------> http://testphp.vulnweb.com/ ParseResult(scheme='http', netloc='testph
p.vulnweb.com', path='/', params='', query='', fragment='')
---------> http://testphp.vulnweb.com/index.php ParseResult(scheme='http', netlo
c='testphp.vulnweb.com', path='/index.php', params='', query='', fragment='')
XSS
XSS
XSS
XSS
SQLi
SQLi
SQLi
SQLi
```

Componentes - Reportes

- Reportes
- Descripción y detalles



Componentes - Alertas

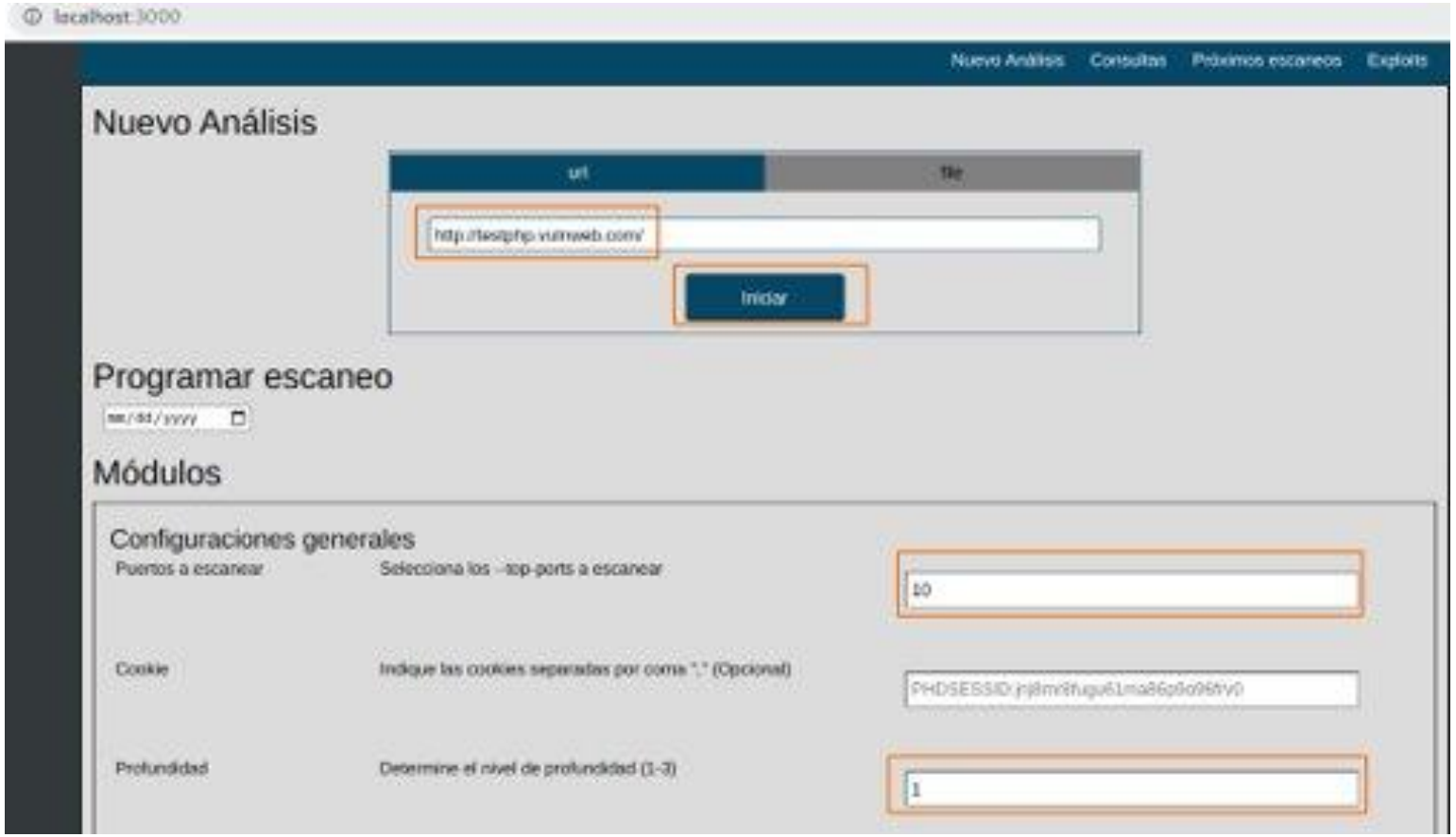
- Envío de notificaciones vía email
- Información preliminar del reporte
- Mensaje de finalización del escaneo

UNAM CERT

Alerta	**19/04/2021 18:15:57**
Pagina	http://localhost/DVWA-master/vulnerabilities/fi/?page=include.php
Motivo	4 vulnerabilidades LFI
Estado	Vulnerable
Pagina	http://localhost/DVWA-master/vulnerabilities/sqli/
Motivo	Form "form__temp__0": 4 vulnerabilidades SQLi Form "form__temp__0": 1 vulnerabilidades SQLi Blind Time
Estado	Vulnerable
Pagina	http://localhost/DVWA-master/vulnerabilities/sqli/
Motivo	91 posibles vulnerabilidades SQLi
Estado	Posibles vulnerables
Pagina	http://localhost/DVWA-master/vulnerabilities/sqli_blind/
Motivo	Form "form__temp__0": 1 vulnerabilidades SQLi Blind Form "form__temp__0": 1 vulnerabilidades SQLi Blind Time

Componentes - Ejecución

- Página de ejecución y configuración de la herramienta

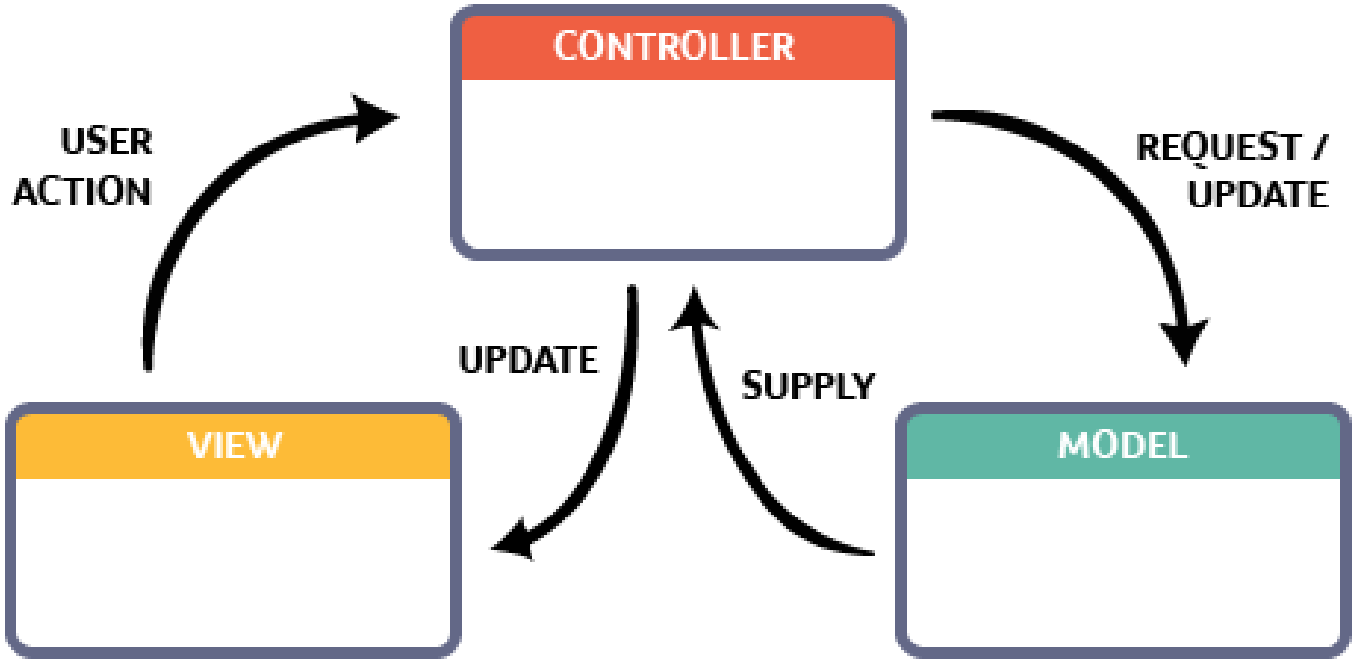


Herramientas utilizadas

- Bash
- Python3
- MongoDB

Metodología de desarrollo

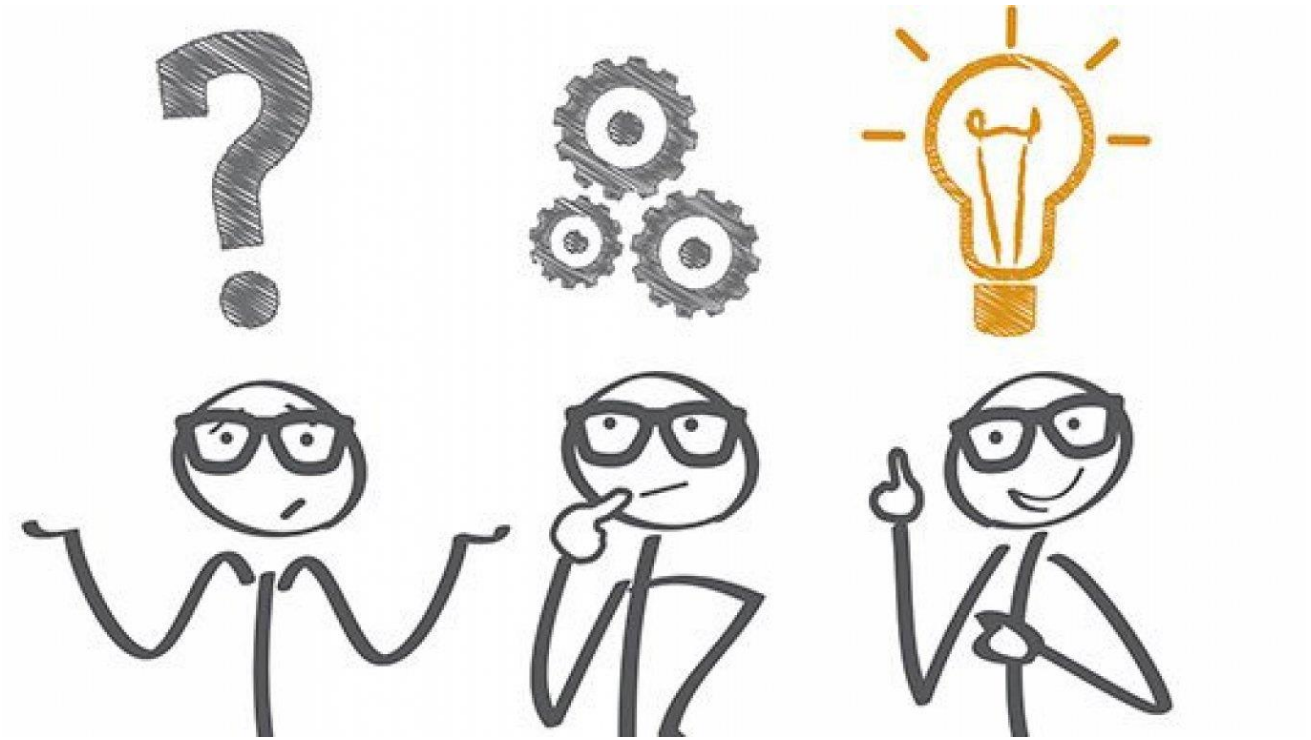
- Metodología ágil SCRUM
  - Desarrollo FrontEnd
  - Desarrollo BackEnd
  - Integración
  - Model View Controller



DEMO

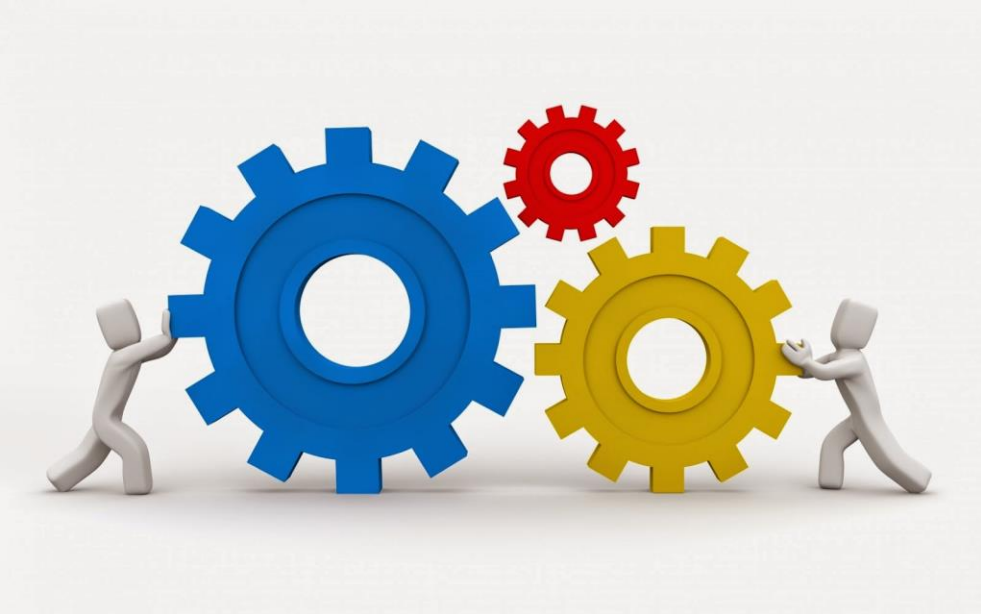
Problemas y retos

- Resolución de captcha después de varias búsquedas de información en Google



El futuro para la herramienta

- Establecer la hora de inicio del escaneo del sitio web
- Mejorar el manejo de bloqueos durante las búsquedas en Google



Conclusiones

- Se reforzaron temas sobre automatización, desarrollo y pruebas de penetración
- Se reforzaron temas de colaboración al integrar metodologías agiles
- Se obtuvo una herramienta útil para el proceso de pruebas de penetración

Preguntas