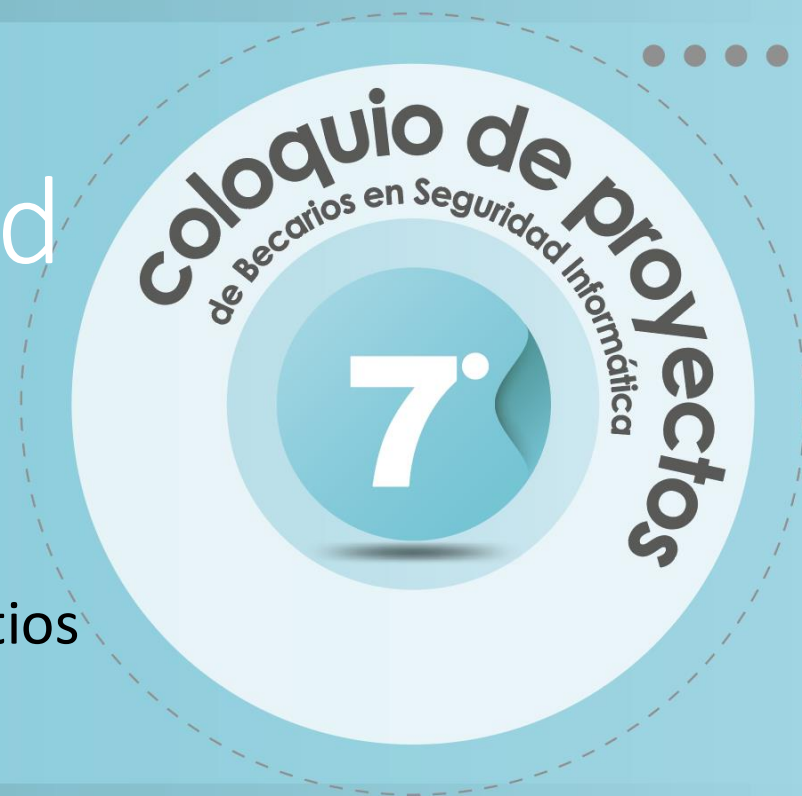




Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Plan de Becarios en Seguridad Informática - UNAM-CERT

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

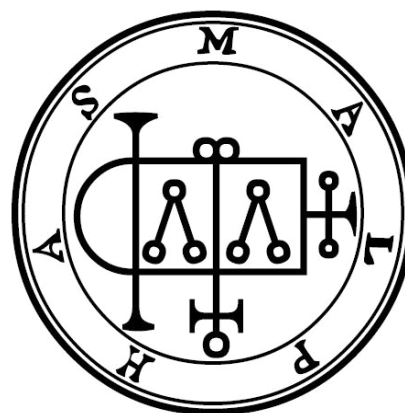




Descripción del proyecto



- 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

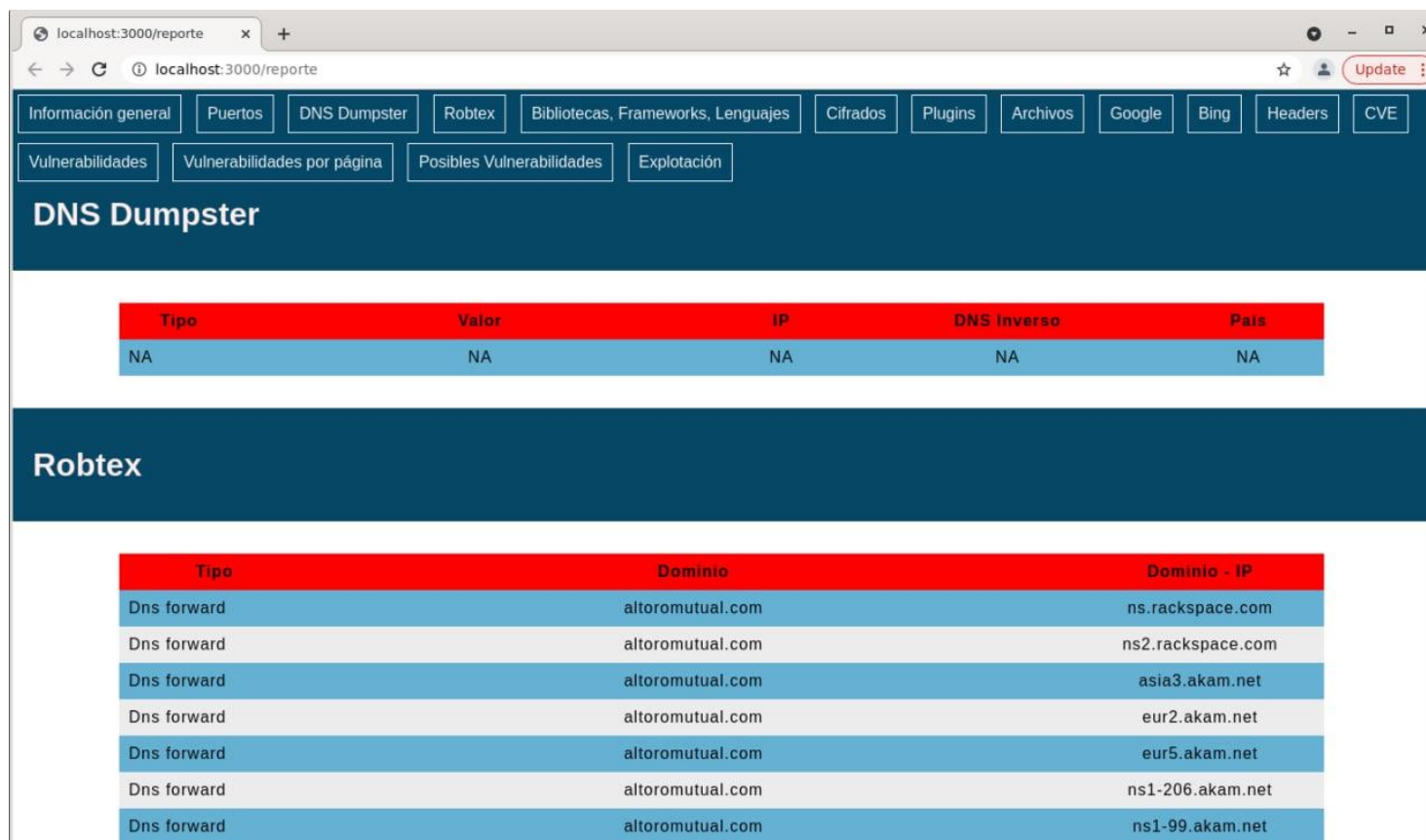
Fuzzing

Consultas y
Reportes

Alertas

Ejecución

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



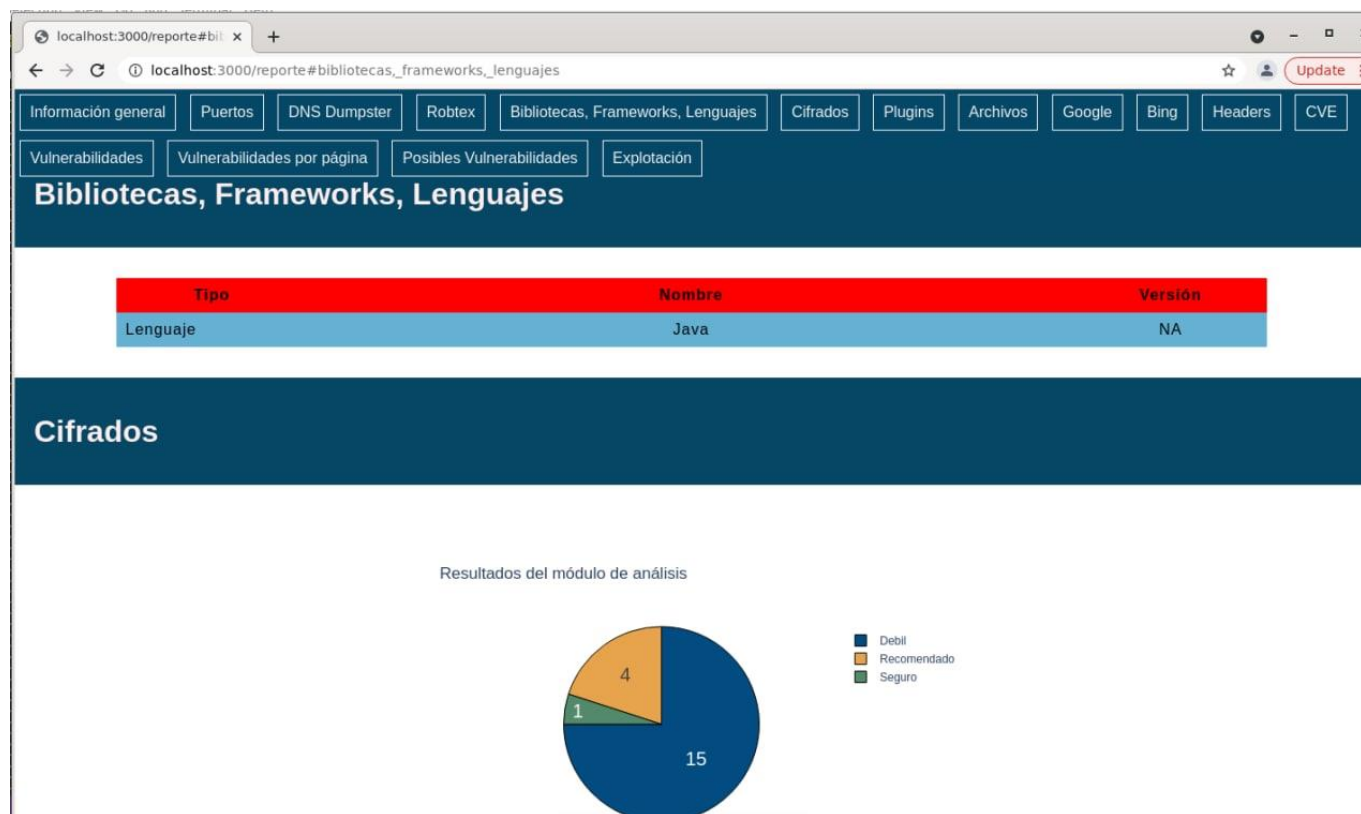
DNS Dumpster

Tipo	Valor	IP	DNS Inverso	Pais
NA	NA	NA	NA	NA

Robtex

Tipo	Dominio	Dominio - IP
Dns forward	altoromutual.com	ns.rackspace.com
Dns forward	altoromutual.com	ns2.rackspace.com
Dns forward	altoromutual.com	asia3.akam.net
Dns forward	altoromutual.com	eur2.akam.net
Dns forward	altoromutual.com	eur5.akam.net
Dns forward	altoromutual.com	ns1-206.akam.net
Dns forward	altoromutual.com	ns1-99.akam.net

- 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

localhost:3000

Nuevo Análisis Consultas Próximos escaneos **Exploits**

Exploits

Drupal 7.0

Edición de exploits cargados

Configuraciones generales

Nombre	Nombre para el exploit	
Contenido	Ingrese el exploit	Seleccione el exploit
Tecnología	[python2 python3 sh ruby otro]	
CVE	En caso de tener un CVE asociado	

Software CMS

- 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

localhost:3000/reporte

← → ↻ ⓘ localhost:3000/reporte

Información general Puertos DNS Dumpster Robtex Bibliotecas, Frameworks, Lenguajes Cifrados Plugins Archivos Google Bing Headers

Vulnerabilidades Vulnerabilidades por página Posibles Vulnerabilidades Explotación

UNAM-CERT Malphas

REPORTE DEL SITIO <https://altoromutual.com/>

28/05/2021 20:09:02

Información general

Nombre	Descripción
Sitio	https://altoromutual.com/
IP	65.61.137.117
País	United States
Puertos	1
Servidor	Apache tomcat 1.1
CMS	NA Na
CVE	0



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/>

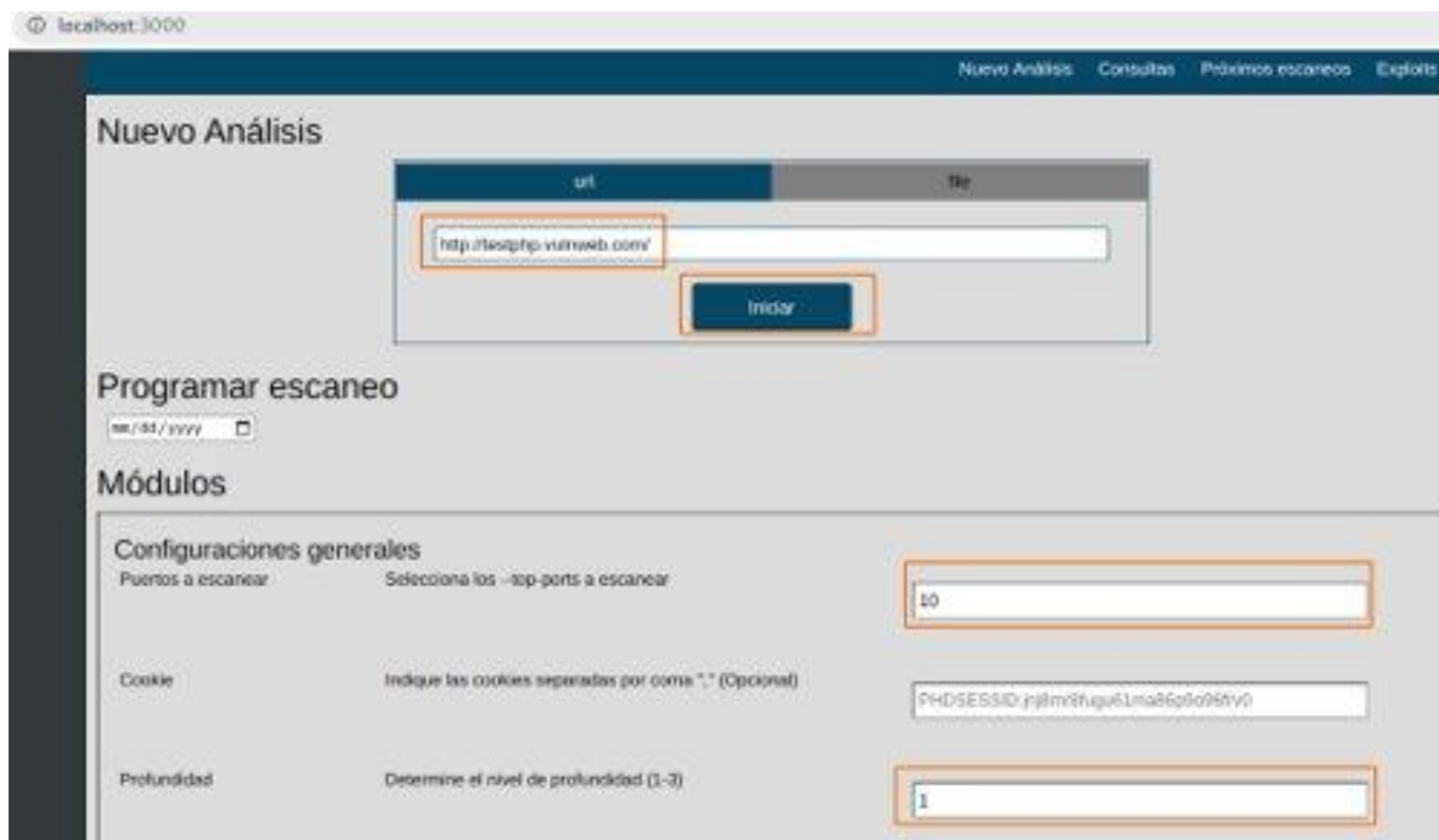
Motivo 91 posibles vulnerabilidades SQLi

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

- Página de ejecución y configuración de la herramienta



localhost:3000

Nuevo Análisis Consultas Próximos escaneos Exploits

Nuevo Análisis

url title

http://testphp.vulnweb.com/ Iniciar

Programar escaneo

mm/dd/yyyy

Módulos

Configuraciones generales

Puentes a escanear Selecciona los --top-ports a escanear 10

Cookie Indique las cookies separadas por coma "," (Opcional) PHPSESSID=...

Profundidad Determine el nivel de profundidad (1-3) 1



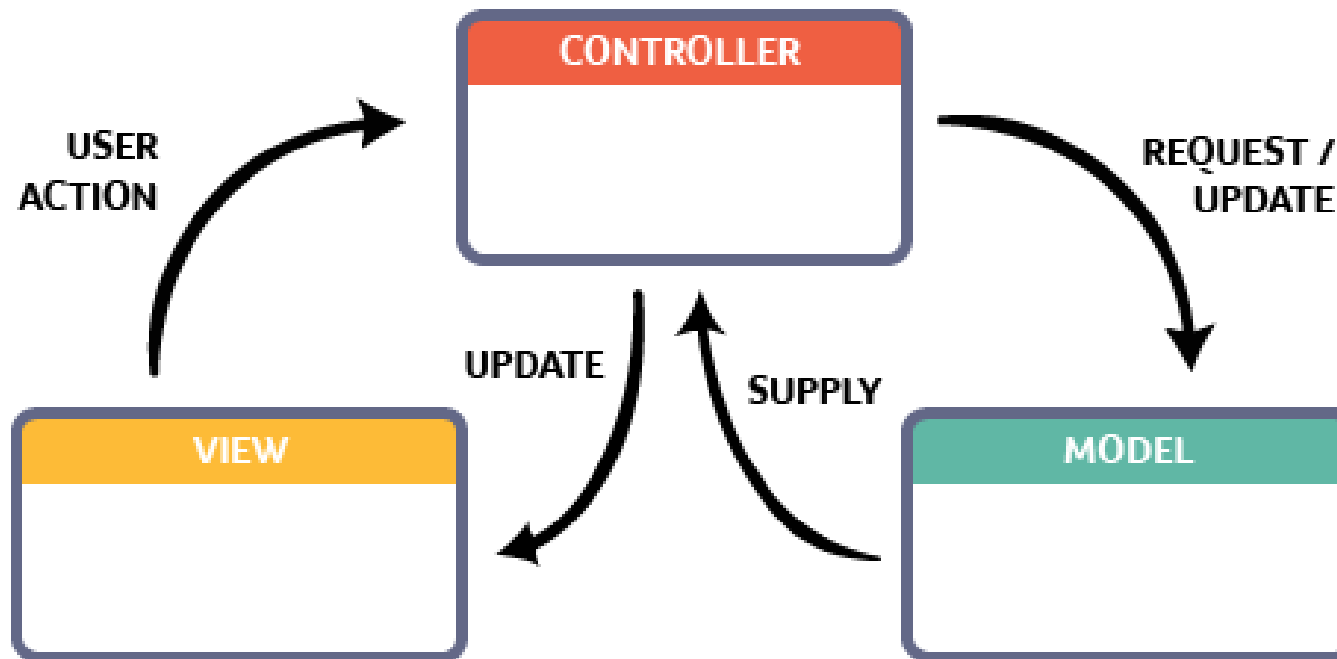
Herramientas utilizadas



- Bash
- Python3
- MongoDB



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



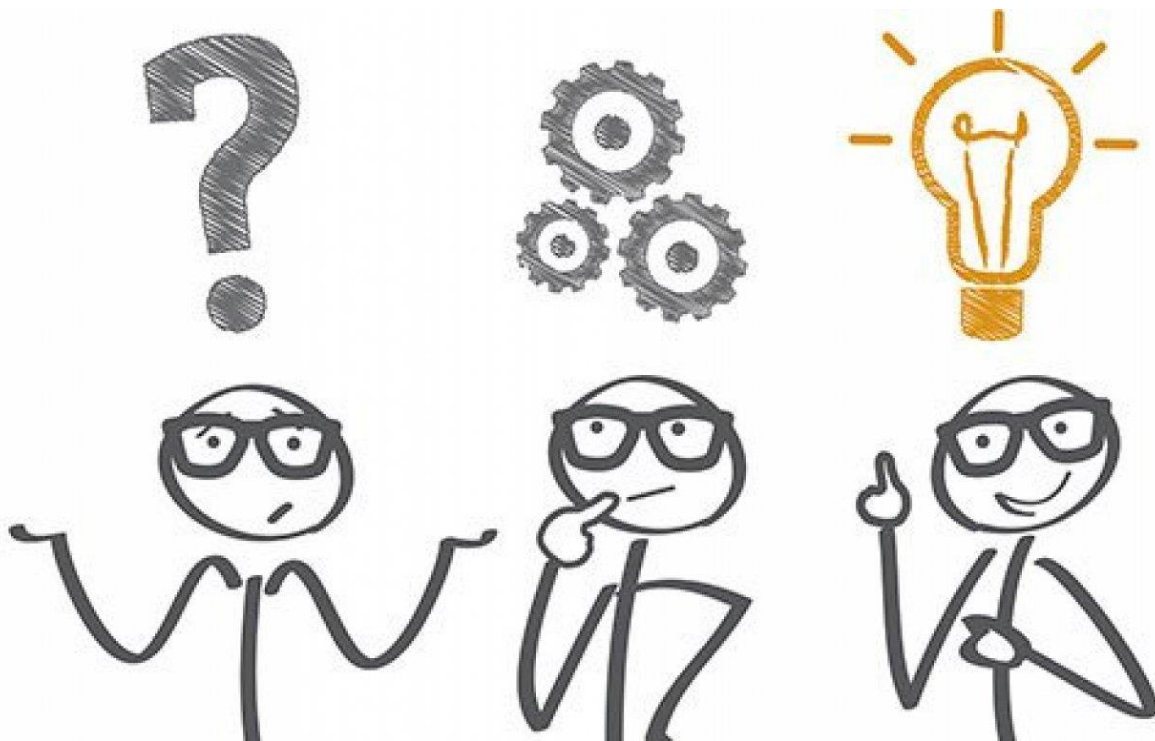


DEMO

Coloquio de proyectos
de Becarios en Seguridad Informática
7



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



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



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





Preguntas

