



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA



## DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

# “DISEÑO E IMPLEMENTACIÓN DE BOTS PARA AUTOMATIZAR TAREAS DE BÚSQUEDA Y ANÁLISIS DE VULNERABILIDADES EN SISTEMAS WEB”

### **Autores:**

Jordy Javier Quinatoa Medina  
Julio Javier Villares Jimenez

### **Director:**

Ing. Germán Rodríguez Mgtr.



# CONTENIDO:

## CAPÍTULO I - INTRODUCCIÓN

- Introducción
- Antecedentes
- Planteamiento del Problema
- Justificación e Importancia
- Sistemas de Objetivos
- Alcance

## CAPÍTULO II - MARCO TEÓRICO

- ¿Qué son los sistemas web?
- Vulnerabilidades y amenazas web
- Cross-Site Scripting (XSS)
- Robos de cookies
- ¿Qué es RPA?
- ¿Qué son los sistemas CAPTCHA?

## CAPÍTULO III - METODOLOGÍA

- Determinación de la herramienta RPA
- Análisis de vulnerabilidad normal
- Desarrollo del bot para sistemas CAPTCHA
- Desarrollo del bot para XSS

## CAPÍTULO IV - RESULTADOS

- Resultados de las soluciones CAPTCHA
- Resultados del bot de CAPTCHA
- Resultados del bot de XSS
- Resultados de la comparación de las herramientas RPA

## CAPÍTULO V - CONCLUSIONES Y RECOMENDACIONES



# CAPÍTULO I

## INTRODUCCIÓN



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

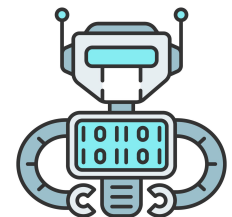
# INTRODUCCIÓN

Muchas empresas y usuarios se han visto en la necesidad de implementar sistemas informáticos basados en una arquitectura cliente-servidor debido a su eficacia y facilidad de acceso. En la mayoría de casos, resulta beneficioso la implementación de sistemas web, sin embargo, pueden estar expuestos a ataques perpetrados por ciberdelincuentes preparados y con sólidos conocimientos.



El uso de sistemas automatizados (bots) se ha intensificado en la integración de los procesos de las compañías y actividades cotidianas de las personas, existen bots que pueden ejecutar desde tareas sencillas hasta manejar toda la lógica de negocio de una empresa. Missouri Enterprise menciona que una organización al integrar bots en sus procesos, puede reducir los costos de un 24% al 50%, cumplir con el tiempo de ciclo de procesos desde el 30% a un 50%

En ese contexto, en este trabajo se desarrollaron bots para automatizar las tareas de búsqueda y análisis de vulnerabilidades en sistemas web, por medio de la utilización de herramientas RPA



RPA bot



# ANTECEDENTES



- Según el Informe de Riesgos Globales 2020 del Foro Económico Mundial, menciona que cada minuto existen 100 intentos de explotación de vulnerabilidades a diferentes sistemas informáticos.



- A raíz de la pandemia del COVID19, los delitos informáticos han aumentado en un 600% a nivel mundial.



- Según el portal Small Business Trends (2020), menciona que de los ataques informáticos de todo el mundo, el 43% fueron dirigidos a pequeñas empresas, de los cuales, solo el 14% lograron mitigar el problema de manera efectiva, mientras que el 29% restante tuvo déficit en la mitigación de riesgos del SI.

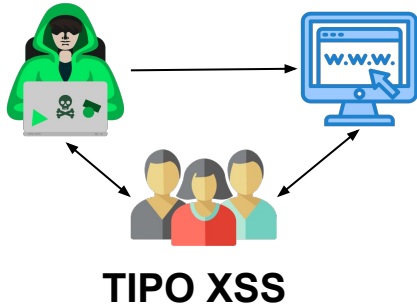


- Según el informe de la Asociación Ecuatoriana de Ciberseguridad (2020), menciona que de 100 empresas encuestadas en el Ecuador el 20% gestionan de manera adecuada la seguridad de la información, mientras que el 80% de empresas restantes poseen un manejo inadecuado de la ciberseguridad.

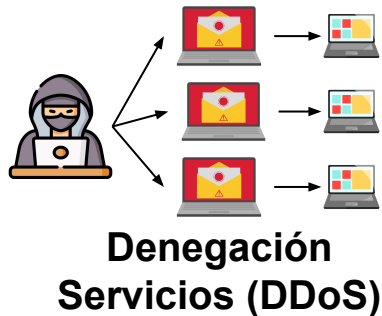


# ANTECEDENTES

Principales ataques cibernéticos a sistemas web empresariales se tiene:



Según OWASP Top 10 (2021), menciona que los ataques de tipo Cross-site Scripting se encuentran englobados en la categoría de ataques de “Inyección” que ocupa la tercera posición en el top 10 de las vulnerabilidades web, con un índice de incidencia medio de 3,37%.



Según una investigación realizada por China y Reino Unido (2018), presentó un modelo de IA capaz de vulnerar los captchas basados en textos de las principales páginas web como Wikipedia, eBay y Microsoft resolviendo el captcha en 0.05 segundos.



El aporte de DARPA, ha generado ideas enfocadas a la creación de sistemas de razonamiento cibernético capaces de detectar vulnerabilidades en los sistemas informáticos.



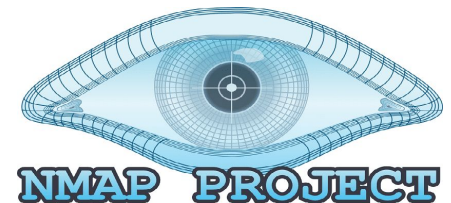


# PLANTEAMIENTO DEL PROBLEMA

## Problema 1:

Un inconveniente en realización de la búsqueda de vulnerabilidades dentro de los sitios web, es que se utilizan herramientas que requieren la intervención humana y procesos manuales (en ocasiones repetitivos) para obtener la información y establecer un reporte, lo que afecta el tiempo para dar una respuesta óptima a la vulnerabilidad existente en el sistema web.

```
nmap <IP>-<IP2>  
nmap 192.168.1.1-115  
nmap -p <número_puerto>
```



## Problema 2:

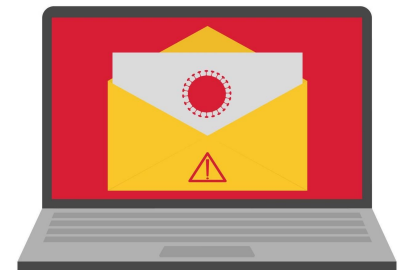
Un inconveniente en los sistemas web es el filtrado de información a través del uso de métodos de inyección de código malicioso. Un elemento que los atacantes optan por vulnerar son las cookies de los sistemas web, ya que son archivos que pueden llegar a contener información sensible de un usuario



WEBSITE  
COOKIES

## Problema 3:

Los sistemas CAPTCHAs permiten contrarrestar los ataques de bots maliciosos, pero hoy en día la implementación de tecnologías como la Inteligencia Artificial y la automatización robótica de procesos, ha hecho que los sistemas CAPTCHAs sean muy fácilmente vulnerados.



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# JUSTIFICACIÓN E IMPORTANCIA



**Justificación 1:** Para mejorar la velocidad de detección de las vulnerabilidades web haciendo uso de bots..

**Justificación 2:** Para ofrecer un modelo de protección de la información del usuario o empresa ante ataques de tipo Cross-site Scripting (XSS).

**Justificación 3:** Para demostrar la vulnerabilidad en los sistemas CAPTCHAs y que futuras investigaciones se enfoquen en complementar su seguridad





# OBJETIVO GENERAL

Diseñar e implementar bots para automatizar tareas de búsqueda y análisis de vulnerabilidades en sistemas web.



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# OBJETIVOS ESPECÍFICOS

Diseñar e Implementar BOTS para ejecutar tareas de web scraping de páginas web vulnerables a ataques de tipo Cross-Site Scripting (XSS).

Diseñar e Implementar BOTS para ejecutar tareas de web scraping de páginas web vulnerables a ataques de tipo Cross-Site Scripting (XSS).



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# ALCANCE

El alcance del proyecto se centra en demostrar que las páginas web son vulnerables a ataques XSS por medio del análisis de sus cookies; y la vulnerabilidad de los sistemas CAPTCHA basado en imágenes, por medio de ataques perpetrados por un bot.



# CAPÍTULO II

## MARCO TEÓRICO



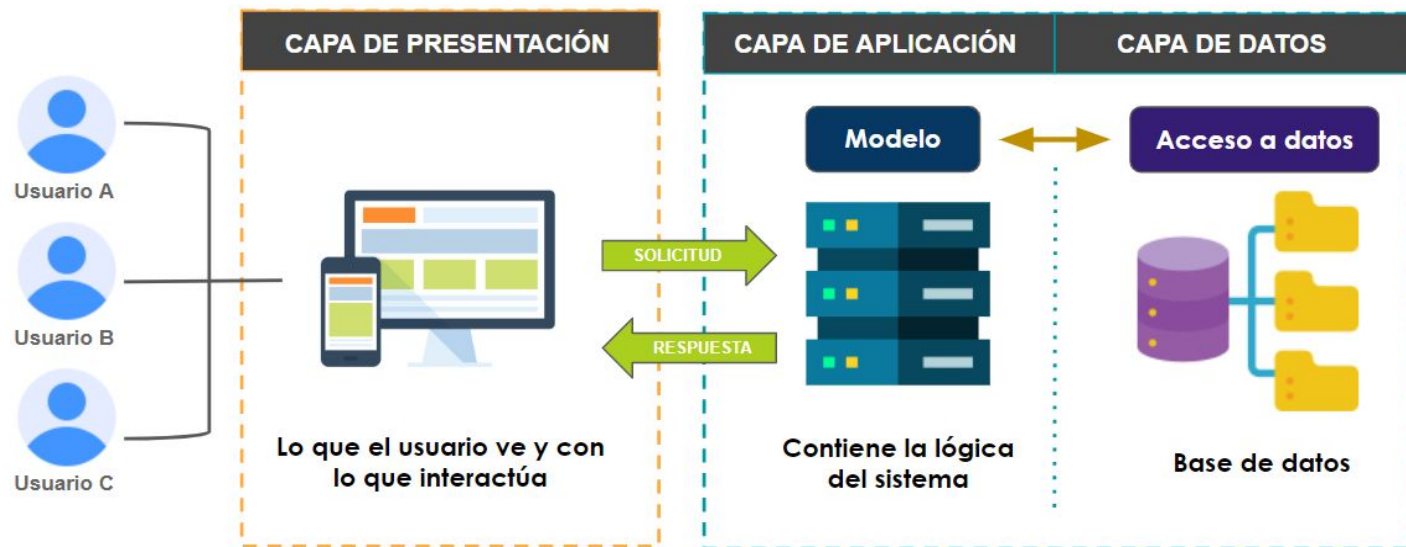
**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# MARCO TEÓRICO

## ¿QUÉ SON LOS SISTEMAS WEB?

Según Maldonado (2016), se denominan sistemas web a todas aquellas aplicaciones en las cuales los usuarios pueden acceder a través del internet.

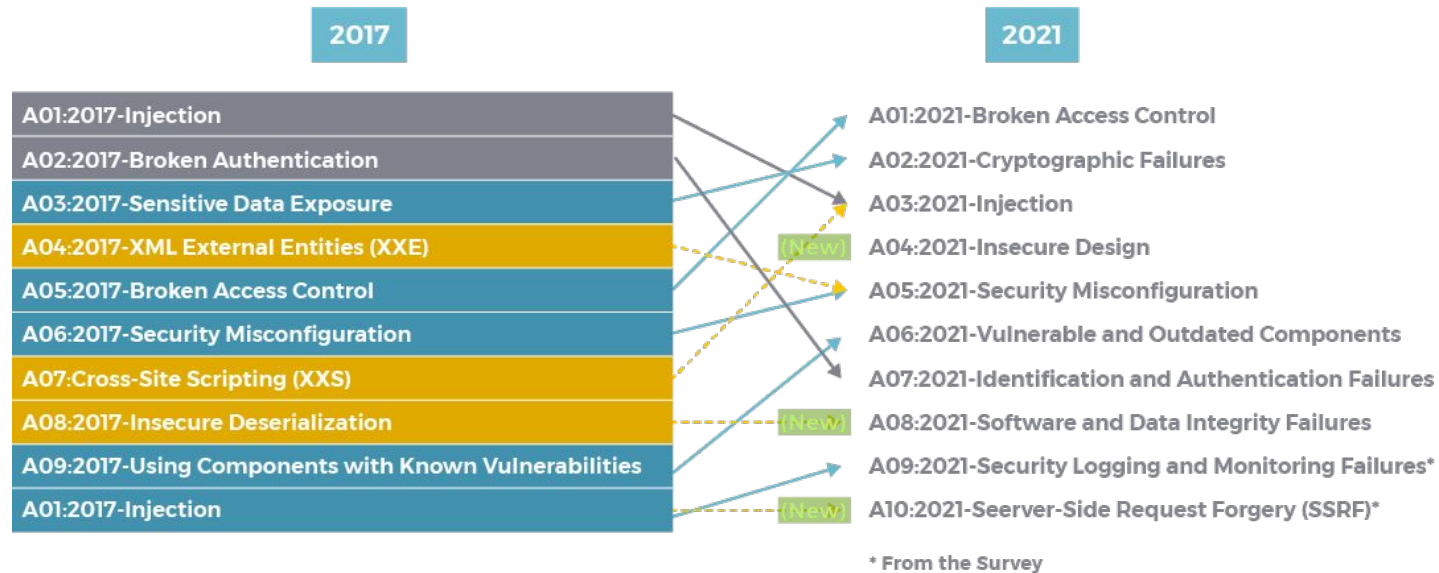
## COMPONENTES DE UN SISTEMA WEB Y SU ARQUITECTURA



# MARCO TEÓRICO

## VULNERABILIDADES Y AMENAZAS DE SISTEMAS WEB

Principales amenazas web según OWASP Top 10 2021



## ATAQUES MÁS COMUNES DE LOS SISTEMAS WEB

- Cross-site scripting (XSS).
- Inyección SQL (SQLi).
- Falsificación de solicitudes entre sitios (CSRF).
- Ataques DDoS.





# MARCO TEÓRICO

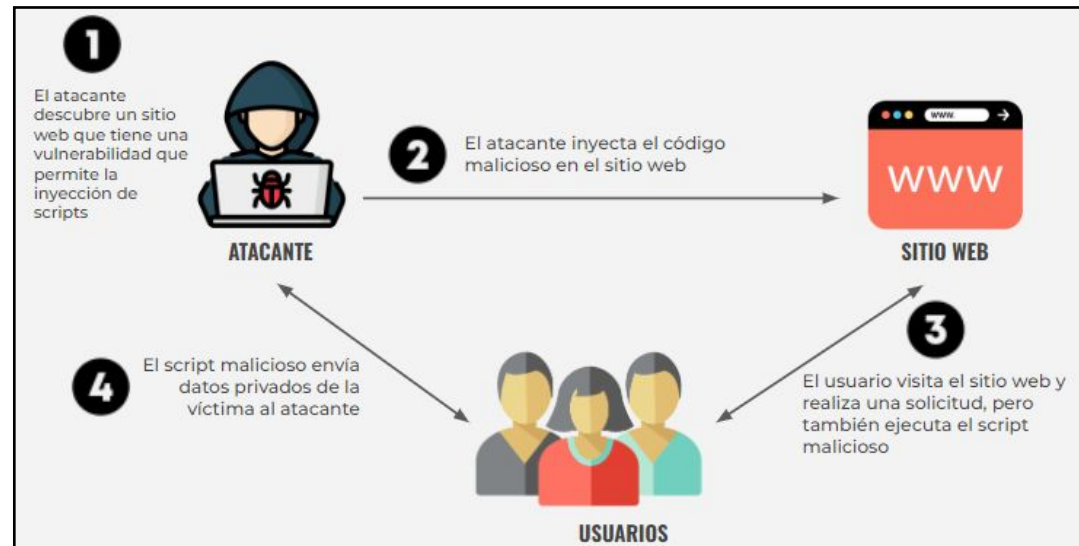
## CROSS-SITE SCRIPTING (XSS)

XSS se considera como una vulnerabilidad que aprovecha las fallas de seguridad que permite a los atacantes inyectar scripts ejecutables y maliciosos en una aplicación o sitio web del lado del cliente (Subía, 2018).

### Consecuencias de los ataques XSS

- Acceso a las cookies del usuario.
- Robo de credenciales.
- Recopilación de datos personales.
- Redirigir a páginas web maliciosas.
- Acceder al control del equipo de la víctima.
- Cambiar el contenido de un sitio web.
- Ejecutar ataques basados en navegador web.

### Funcionamiento de un ataque XSS



# MARCO TEÓRICO

## Tipos ataques XSS



XSS persistente o almacenado



XSS reflejado




XSS basado en el DOM

# MARCO TEÓRICO

## Robo de cookies mediante ataques XSS

El atacante por medio de la ejecución de un script del lado del cliente puede obtener acceso de las cookies de la base de datos del navegador (Rodríguez et al., 2019).



**Las cookies** son archivos de datos que los navegadores y páginas web generan automáticamente en el ordenador del usuario. La mayoría de las cookies contienen información personal del usuario, además permiten una navegación acorde a las preferencias del visitante

## TIPOS DE COOKIES



**Cookies de sesión**



**Cookies persistentes**



**Cookies propia**



**Cookies Zombi**



**Cookies de terceros**



**Cookies seguras**











**Cookies HttpOnly**



# MARCO TEÓRICO

## Herramientas para buscar vulnerabilidades en sitios web

<p>Vega</p> 	<p>Parseo</p> 
<p>WPScan</p> 	<p>Burp Suite Community Edition</p> 
<p>Joomscan</p> 	<p>jSQL injection</p> 
<p>Nikto</p> 	<p>Websploit</p> 



# MARCO TEÓRICO

## ¿QUÉ ES RPA?

La automatización robótica de procesos (RPA) se define como la automatización de procesos manuales de gran volumen, repetitivos, mediante la utilización de robots de software avanzados, también conocidos como "bots".

## Beneficios de las RPA

- Reducción de errores.
- Mejora el análisis de datos.
- Ahorro de costes.
- Mejora la productividad del negocio.



## TIPOS DE RPA

- Automatización RPA asistida
- Automatización RPA no asistida

## HERRAMIENTAS RPA

- UI.Vision
- Robot framework
- TagUI
- Automagica
- UiPath Community Edition

## BOTs QUE AUTOMATIZAN

- Software Mayhem
- Mechanical Phish



# MARCO TEÓRICO

## SISTEMAS CAPTCHA

El test de Turing completamente automático y público para diferenciar ordenadores de humanos. Es un desafío que permite determinar si el que intenta ingresar a un sistema es un bot o un humano.

### TIPOS DE CAPTCHA

CAPTCHA basados en texto

CAPTCHA basados en gráficos

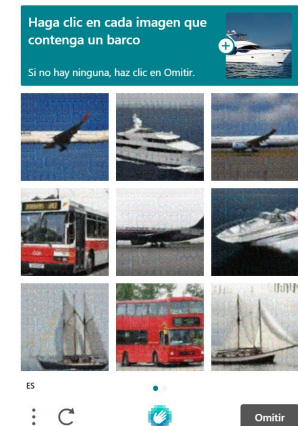
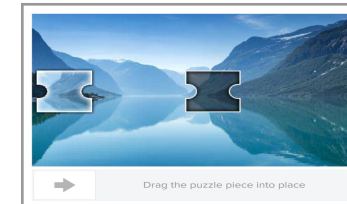
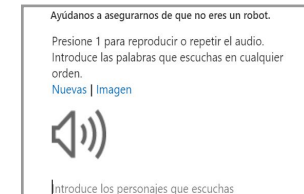
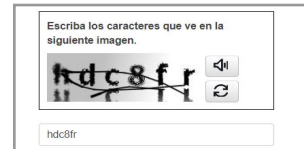
CAPTCHA basados en audio

CAPTCHA de problemas matemáticos y lógicos

CAPTCHA lúdicos

reCAPTCHA

hCAPTCHA



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA



# MARCO TEÓRICO

## ESTADO DE ARTE

La presente Tabla, presente un análisis de los principales estudios enfocados en la detección automática de vulnerabilidades

Código	Título	Link
TR1	Una herramienta inteligente y automatizada de descubrimiento de vulnerabilidades en el WCMS: El estado actual de la web	<a href="#">Link</a>
TR2	Un analizador automático de vulnerabilidades para aplicaciones web	<a href="#">Link</a>
TR3	Ruptura robusta en tiempo real de CAPTCHA de imagen utilizando el modelo Inception v3	<a href="#">Link</a>
TR4	Un ataque de bajo costo contra el sistema hCAPTCHA	<a href="#">Link</a>
TR5	Una extensión del navegador Google Chromium para detectar ataques XSS en sitios web basados en HTML5	<a href="#">Link</a>
TR6	Cookie Scout: Un modelo analítico para la prevención de Cross-Site Scripting (XSS) utilizando un clasificador de cookies	<a href="#">Link</a>



# CAPÍTULO III

## METODOLOGÍA



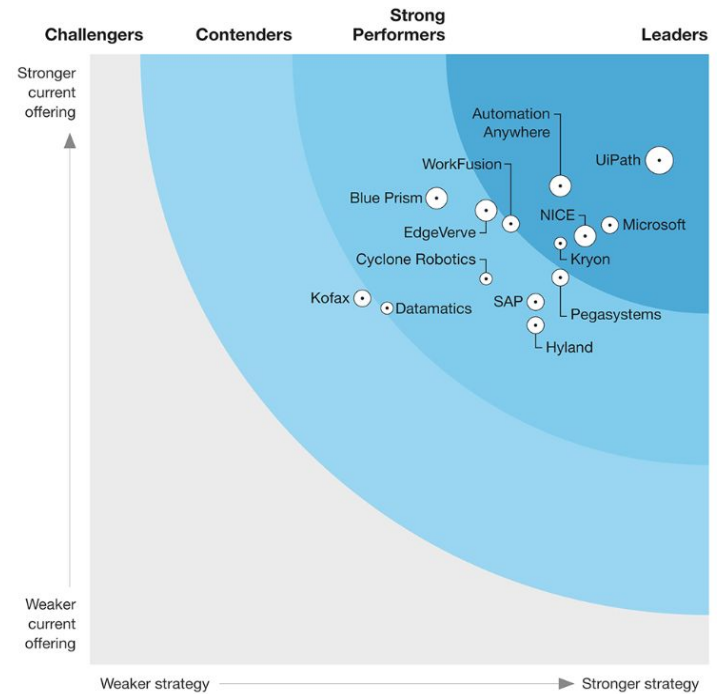
**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# METODOLOGÍA

## Metodología para la Obtención de la Herramienta RPA



**CUADRANTE MÁGICO DE GARTNER (2021)**



**ONDA DE LÍDERES DE FORRESTER WAVE**



# METODOLOGÍA

## Selección del software RPA UiPath en su versión Community Edition



Escalabilidad	4.5		(1231)
Integración	4.5		(1230)
personalización	4.4		(1230)
Facilidad de implementación, administración y mantenimiento	4.7		(1229)

Ediciones de UiPath		
Community	Enterprise	
	Enterprise Server	Enterprise Cloud
Utilizado por desarrolladores y pequeños equipos que inician su viaje en la automatización.	Utilizado en el despliegue de tareas en empresas y grandes organizaciones.	Utilizado en despliegues empresariales en la nube y empresas de cualquier tamaño.
Versión siempre <b>GRATIS</b>	Prueba gratuita por 60 días	Solo por licencia
<ul style="list-style-type: none"> <li>- 2 módulos Studio para el diseño de la automatización.</li> <li>- 3 robots.</li> <li>- Orquestador alojado en la nube.</li> <li>- Soporte solo por foros y videotutoriales.</li> <li>- Acceso a la academia UiPath.</li> </ul>	<ul style="list-style-type: none"> <li>- Módulos Studios ilimitados para el diseño de la automatización.</li> <li>- Robots ilimitados.</li> <li>- Orquestador on-premises (forma local y servidores de la empresa).</li> <li>- Soporte de primera calidad.</li> <li>- Escala a medida que crece la empresa.</li> <li>- Actualizaciones autogestionadas.</li> </ul>	<ul style="list-style-type: none"> <li>- Módulos Studios ilimitados para el diseño de la automatización.</li> <li>- Robots ilimitados.</li> <li>- Orquestador alojado 100% en la nube.</li> <li>- Soporte de primera calidad.</li> <li>- Escala a medida que crece la empresa.</li> <li>- Actualizaciones constantes, siempre al día.</li> <li>- Gestión centralizada del acceso de los usuarios.</li> </ul>



# METODOLOGÍA



## Comparativa del IDE Selenium y Ui.Vision IDE

### La principal razón por la que seleccionó la opción de Ui.Vision

- Permite la automatización de procesos basándose en macros
- Es ideal para funcionar en los sitios web más complejos.
- Permite la grabación y reproducción de procesos de manera visual.
- Permite realizar pruebas basadas en la utilización de datos con importación de archivos CSV.

Característica	IDE de Selenium	Ui.Vision RPA Selenium IDE
Implementa todos los comandos importantes de Selenium IDE	Sí	Sí
Código abierto	sí (licencia Apache 2.0)	sí (Licencia GNU AGPL 3.0)
Línea de comandos para programar ejecuciones, ejecutar en una cuadrícula.	selenium-ide-runner	interfaz de línea de comandos
Tomar captura de pantalla	Sí	Sí
Tomar captura de pantalla de página completa	No	Sí
Automatizar descargas de archivos	No	Sí
Exportación de scripts a Java	No	No
Pruebas visuales de la interfaz de usuario	No	Sí
Pruebas de elementos de lienzo	No	Si



# METODOLOGÍA

## Análisis de vulnerabilidades web con herramientas convencionales



```
[root@jordy-qm]~/home/jordy
└─# nikto -h http://redisd.org
└─ Nikto v2.1.5
-----
+ Target IP:          69.174.114.113
+ Target Hostname:    redisd.org
+ Target Port:        80
+ Start Time:         2022-06-26 16:59:27 (GMT-5)
```

```
[~]-[root@jordy-qm]~/home/jordy/XStrike
└─# python3 xsstrike.py -u http://pizza.com/?s=test
XStrike v3.1.5

[-] Checking for DOM vulnerabilities
[+] Potentially vulnerable objects found
-----
4      document.cookie = " utms=" + ($(this).attr("data-source") ? $(this).attr("data-source")
: "0RAvNwywFBPp5iV0eL_VU0JRqhk1bCK_MfpqgKAH1pvngbxPPAjas.bwVmpz_e0ovvzF4VFTa9PskEgFgtSu_WCWPTYq.JIeUtr5UXMZSepY
hwQHAAarxr2nfLazGqC.") + "; path=/";
7      document.cookie = " utms=" + ($(this).attr("data-source") ? $(this).attr("data-source")
: "0RAvNwywFBPp5iV0eL_VU0JRqhk1bCK_MfpqgKAH1pvngbxPPAjas.bwVmpz_e0ovvzF4VFTa9PskEgFgtSu_WCWPTYq.JIeUtr5UXMZSepY
hwQHAAarxr2nfLazGqC.") + "; path=/";
3      return decodeURIComponent((new RegExp('[?&]' + name + '=' + '([^\&]+?)(&#|;|$)').exec(location.search)
[|[,,"]])[1].replace(/\+/g, '%20'))||null
9      ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga
.js';

[+] WAF Status: Offline
[!] Testing parameter: s
[!] Reflections found: 1
[-] Analysing reflections
[-] Generating payloads
[!] Payloads generated: 3072
```

The screenshot shows a web browser window with a security warning: "No seguro" (Not secure) for the URL `pizza.com/?s=<script>alert%281%29<%2fscript>`. The page content shows "pizza.com dice" and the number "1". An "Aceptar" (Accept) button is visible at the bottom right of the warning box.

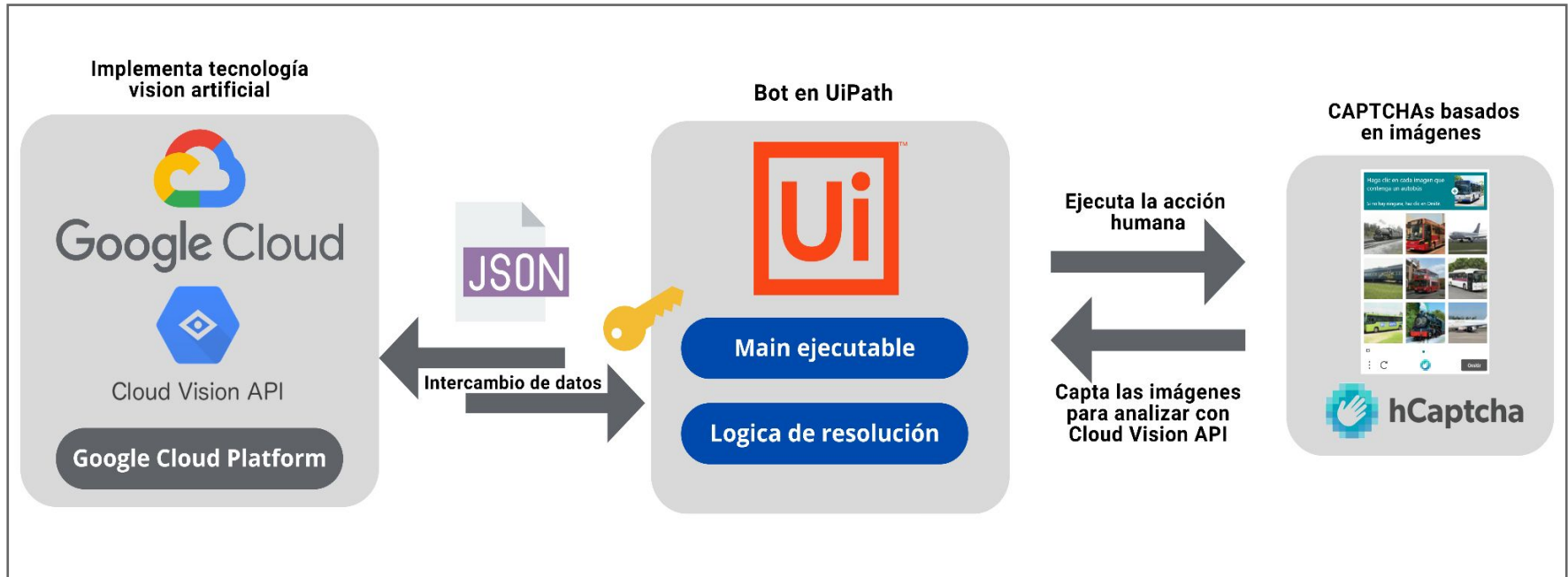




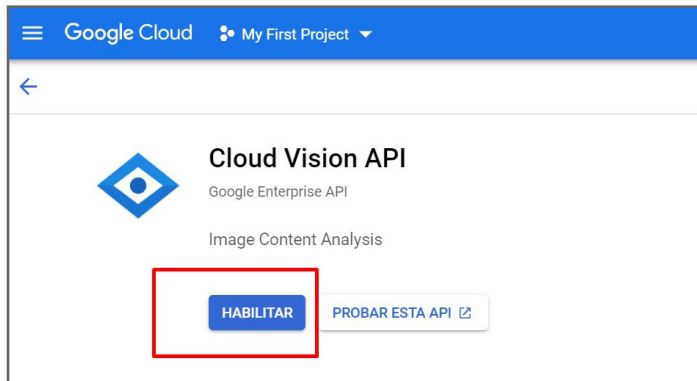
# METODOLOGÍA

## Bot para el análisis de vulnerabilidades en los Sistemas CAPTCHA

### Desarrollo del bot propuesto para vulnerar un sistema CAPTCHA



## EN LA API DE GOOGLE CLOUD



ADMINISTRAR CUOTAS

Nombre del proyecto \*  
UiPathGVision

ID de proyecto: uipathvision-355121. No se podrá cambiar más tarde. [EDITAR](#)

Organización \*  
espe.edu.ec

Selecciona una organización para vincularla a un proyecto. No podrás cambiar esta selección más adelante.

Ubicación \*  
espe.edu.ec [EXPLORAR](#)

Organización o carpeta superior

**CREAR** CANCELAR

API y servicios

Editar el registro de la app

1 Pantalla de consentimiento de OAuth — 2 Permisos — 3 Resumen

Información de la aplicación

Esta información aparece en la pantalla de consentimiento y permite que los usuarios finales sepan quién eres y cómo comunicarse contigo

Nombre de la aplicación \*  
UiPathGVision

El nombre de la aplicación que solicita el consentimiento

Correo electrónico de asistencia del usuario \*  
wsledesma@espe.edu.ec

Para que los usuarios se comuniquen contigo si tienen preguntas sobre su consentimiento

Logotipo de la app  
hcaptcha.jpg

Sube una imagen con ayuda a los usuarios. Acepta formatos de imagen JPG, PNG y BMP.

<input type="checkbox"/>	Cloud Trace API	.../auth/trace.append	Permite escribir los datos de seguimiento de proyecto o una aplicación.
<input checked="" type="checkbox"/>	Cloud Vision API	.../auth/cloud-vision	Aplicar modelos de aprendizaje automático para comprender y etiquetar imágenes
<input type="checkbox"/>	Service Management API	.../auth/service.management	Administrar la configuración de los servicios de Google
<input type="checkbox"/>	Service Management API	.../auth/service.management.readonly	Permite ver la configuración de los servicios de Google



## Se creó la clave de API

Para usar esta clave en tu aplicación, transfírela con el parámetro `key=API_KEY`.

Tu clave de API

[Redacted API Key]

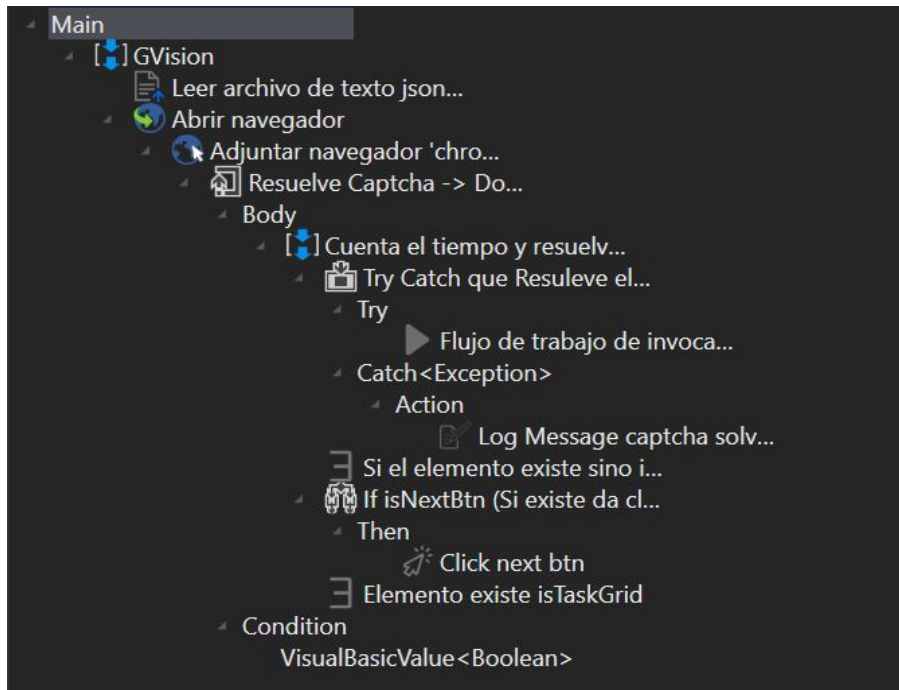
⚠ Esta clave no tiene restricciones. A fin de evitar el uso no autorizado, te recomendamos restringir dónde y para qué API se puede usar. [Edita la clave de API](#) para agregar restricciones. [Más información](#)

CERRAR

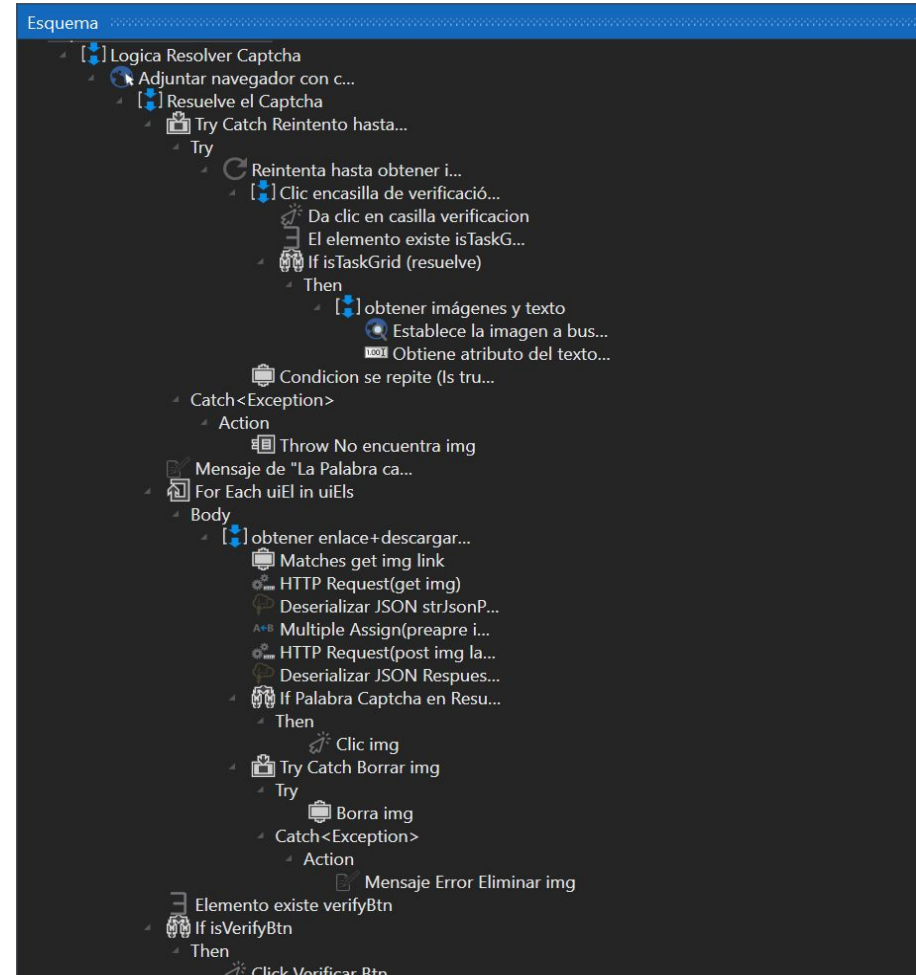


## EN LA API DE GOOGLE CLOUD

### Desarrollo del *Main.xaml*

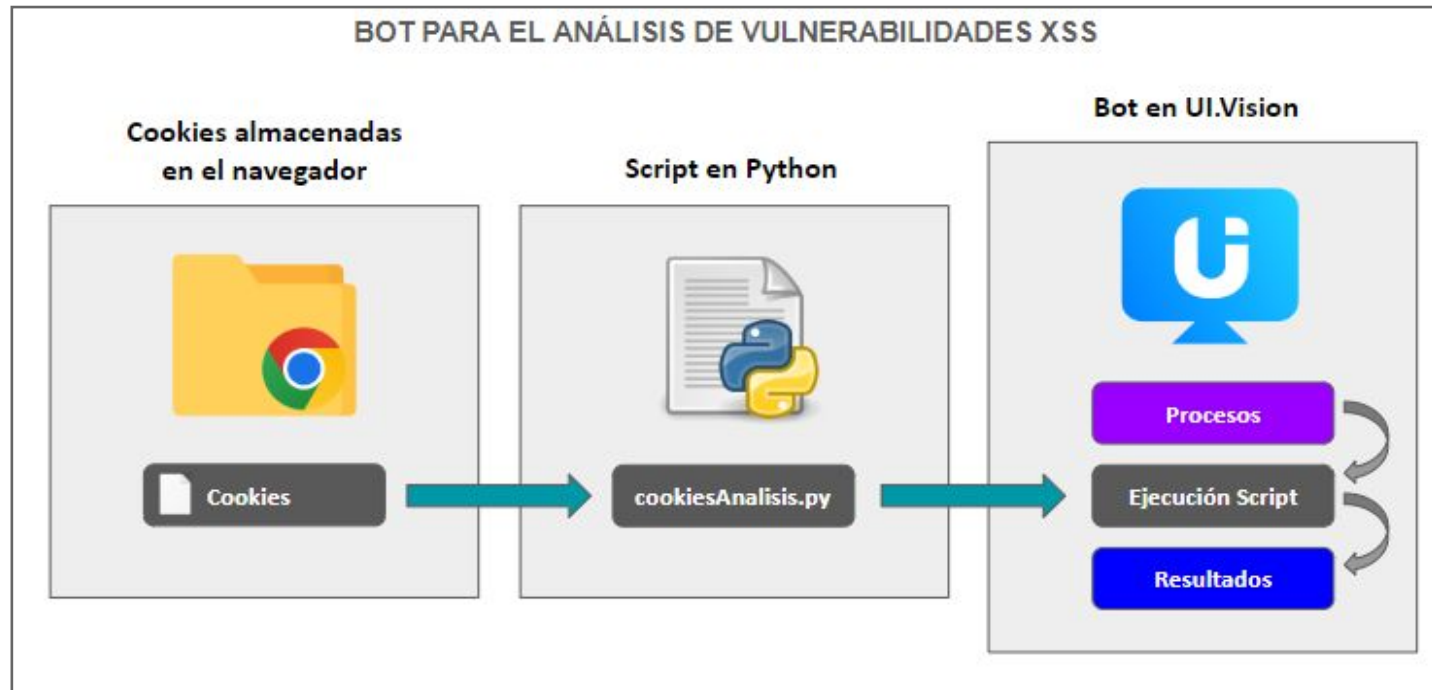


### Desarrollo del *CatpchaSolver.xaml*



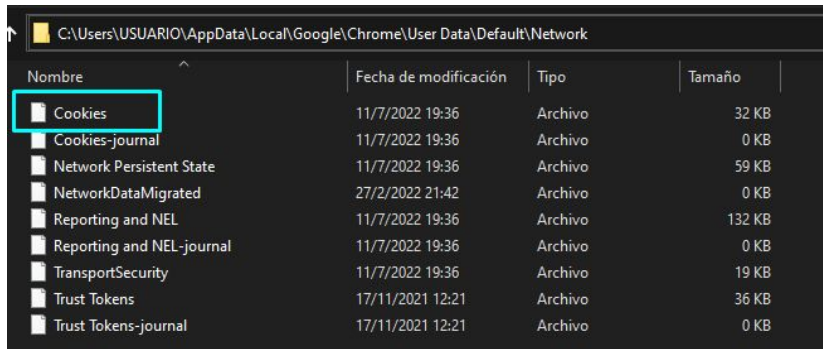
# METODOLOGÍA

## Bot para el análisis de vulnerabilidades de tipo Cross-Site Scripting (XSS)



# METODOLOGÍA

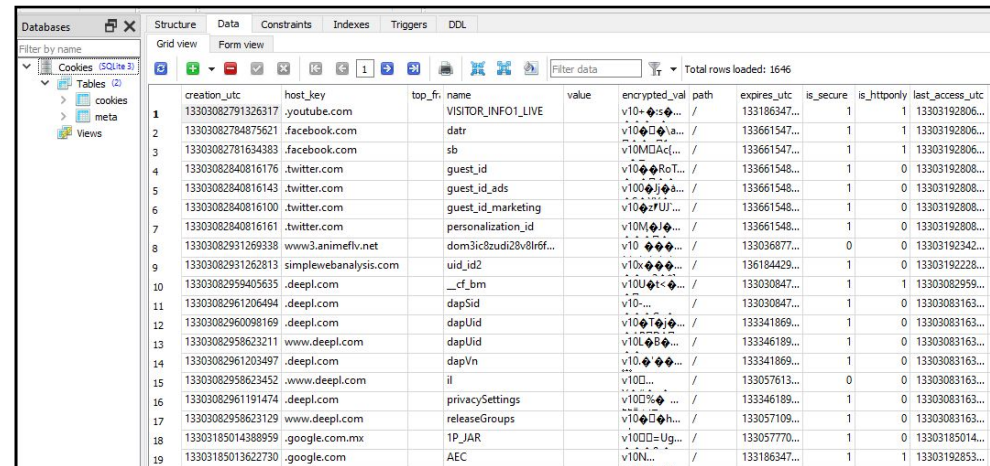
## Ubicación del archivo “Cookies”



C:\Users\USUARIO\AppData\Local\Google\Chrome\User Data\Default\Network

Nombre	Fecha de modificación	Tipo	Tamaño
Cookies	11/7/2022 19:36	Archivo	32 KB
Cookies-journal	11/7/2022 19:36	Archivo	0 KB
Network Persistent State	11/7/2022 19:36	Archivo	59 KB
NetworkDataMigrated	27/2/2022 21:42	Archivo	0 KB
Reporting and NEL	11/7/2022 19:36	Archivo	132 KB
Reporting and NEL-journal	11/7/2022 19:36	Archivo	0 KB
TransportSecurity	11/7/2022 19:36	Archivo	19 KB
Trust Tokens	17/11/2021 12:21	Archivo	36 KB
Trust Tokens-journal	17/11/2021 12:21	Archivo	0 KB

## Contenido del archivo “Cookies”



creation_utc	host_key	top_fr	name	value	encrypted_val	path	expires_utc	is_secure	is_httponly	last_access_utc
13303082791326317	.youtube.com		VISITOR_INFO1_LIVE		v10+...	/	133186347...	1	1	13303192806...
13303082784875621	.facebook.com		dctr		v10+...	/	133661547...	1	1	13303192806...
13303082781634383	.facebook.com		sb		v10MDAct...	/	133661547...	1	1	13303192806...
13303082840816176	.twitter.com		guest_id		v10+...	/	133661548...	1	0	13303192808...
13303082840816143	.twitter.com		guest_id_ads		v100+...	/	133661548...	1	0	13303192808...
13303082840816100	.twitter.com		guest_id_marketing		v10+...	/	133661548...	1	0	13303192808...
13303082840816161	.twitter.com		personalization_id		v10M+...	/	133661548...	1	0	13303192808...
13303082931269338	www3.animeflv.net		dom3ic8zudi28v8lrf...		v10...	/	133036877...	0	0	13303192342...
13303082931262813	simplewebanalysis.com		uid_id2		v10x...	/	136184429...	1	0	13303192228...
13303082959405635	.deepl.com		__cf_bm		v10U+...	/	133030847...	1	1	13303082959...
13303082961206494	.deepl.com		dapSid		v10...	/	133030847...	1	0	13303083163...
13303082960098169	.deepl.com		dapUId		v10+...	/	133341869...	1	0	13303083163...
13303082958623211	www.deepl.com		dapUId		v10L+...	/	133346189...	1	0	13303083163...
13303082961203497	.deepl.com		dapVn		v10+...	/	133341869...	1	0	13303083163...
13303082958623452	www.deepl.com		il		v10D...	/	133057613...	0	0	13303083163...
13303082961191474	.deepl.com		privacySettings		v10D%...	/	133346189...	1	0	13303083163...
13303082958623129	www.deepl.com		releaseGroups		v10+...	/	133057109...	1	0	13303083163...
13303185014388959	.google.com.mx		1P_JAR		v10D=Ug...	/	133057770...	1	0	13303185014...
13303185013622730	.google.com		AEC		v10N...	/	133186347...	1	1	13303192853...



# METODOLOGÍA

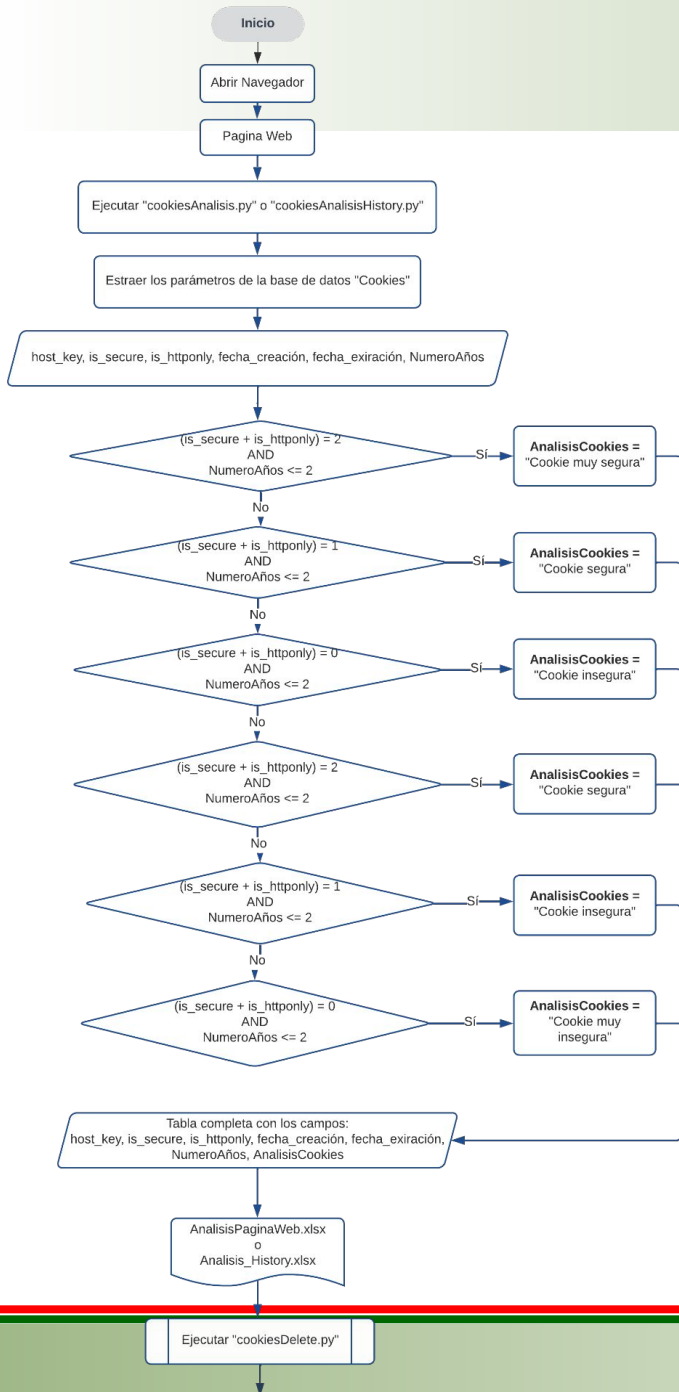
## Variables identificadas para el diseño del análisis del bot.

Campo	Detalle
<b>host_key</b>	Representa el dominio o página web de la cookie generada por la página web visitada por el usuario
<b>creation_utc</b>	Corresponde a la fecha y hora en qué se creó la cookie. Este dato es almacenado en formato Unix epoch, el cual es el número de segundos que han transcurrido desde el 1 de enero de 1601.
<b>expires_utc</b>	Corresponde a la fecha y hora de caducidad de la cookie. Al igual que <code>creation_utc</code> , este se encuentra en formato Unix epoch.
<b>is_secure</b>	El valor [0] en el atributo <code>is_secure</code> , representa que el navegador puede enviar la cookie a través de un canal o conexión HTTP. Lo cual permite que los atacantes accedan a las cookies.
	El valor [1] en el atributo <code>is_secure</code> , representa que la cookie se utiliza a través de HTTPS y se transmite de forma segura en texto cifrado, protegiendo la confidencialidad de la cookie.
<b>is_httponly</b>	El valor [0] en el atributo <code>is_httponly</code> , indica que la cookie no está protegida ante ataques XSS por lo que existe la posibilidad de acceder a sus datos.
	El valor [1] en un atributo <code>is_httponly</code> , prohíbe que se acceda a la cookie a través de scripts del lado del cliente, en específico con la propiedad <code>document.cookie</code> .



## Modelo en Python para el análisis del archivo "Cookies"

Análisis para determinar si una cookie es segura o insegura a ataques XSS



is_httponly	is_secure	num_years	Cookie muy segura	Cookie segura	Cookie insegura	Cookie muy insegura
1	1	<= 2	X			
1	0	<= 2		X		
0	1	<= 2		X		
0	0	<= 2			X	
1	1	> 2		X		
1	0	> 2			X	
0	1	> 2			X	
0	0	> 2				X





# METODOLOGÍA

## cookiesAnalysis.py

```
#Consulta para determinar el analisis final-----
print('\n=====')
print(' ANALISIS FINAL')
print('=====')
print('| DOMINIO | HTTPONLY | SECURE | FECHA CREACION | FECHA EXPIRACION | DURACION (ANIOS) | ANALISIS EN BASE DE LAS COOKIES |')

conv_fcrToYears = "strftime('%J', date(creation_utc/1000000 + (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime'))"
conv_fexToYears = "strftime('%J', date(expires_utc/1000000 + (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime'))"
num_years = "round((" + conv_fexToYears + " - " + conv_fcrToYears + ") / 365, 4)"

sqlanalisis = """SELECT
host_key AS DominioCookie, is_secure AS Segura, is_httponly AS HttpOnly,
"""+fecha_creacion+"" AS FechaCreacion,
"""+fecha_expiracion+"" AS FechaExpiracion,
(CASE
WHEN """+num_years+"" >= 0
THEN """+num_years+""
ELSE 'No Deff'
END) AS NumeroAños,
(CASE
WHEN (is_secure + is_httponly) = 2 and """+num_years+"" <= 2
THEN 'Cookie muy segura'
WHEN (is_secure + is_httponly) = 1 and """+num_years+"" <= 2
THEN 'Cookie segura'
WHEN (is_secure + is_httponly) = 0 and """+num_years+"" <= 2
THEN 'Cookie insegura'
WHEN (is_secure + is_httponly) = 2 and """+num_years+"" > 2
THEN 'Cookie segura'
WHEN (is_secure + is_httponly) = 1 and """+num_years+"" > 2
THEN 'Cookie insegura'
WHEN (is_secure + is_httponly) = 0 and """+num_years+"" > 2
THEN 'Cookie muy insegura'
END) AS AnalisisCookies
FROM
cookies"""

cur.execute(sqlanalisis)
rows2 = cur.fetchall()

for row2 in rows2:
    print(row2)
```

Consulta SQLite con todos los parámetros que analizan las cookies en base a las condiciones.

```
97 #Enviar los resultados a un excel
98 analisis = pd.read_sql(sql = sqlanalisis , con = con)
99 nombre = dom.replace('/://', '')
100 analisis.to_excel("C:\\Users\\JORDY\\Desktop\\AnalisisXSS\\AnalisisPaginasWeb\\analisis_( "+ nombre + " ).xlsx", index=False)
101 #-----
102
103 con.close()
104
```

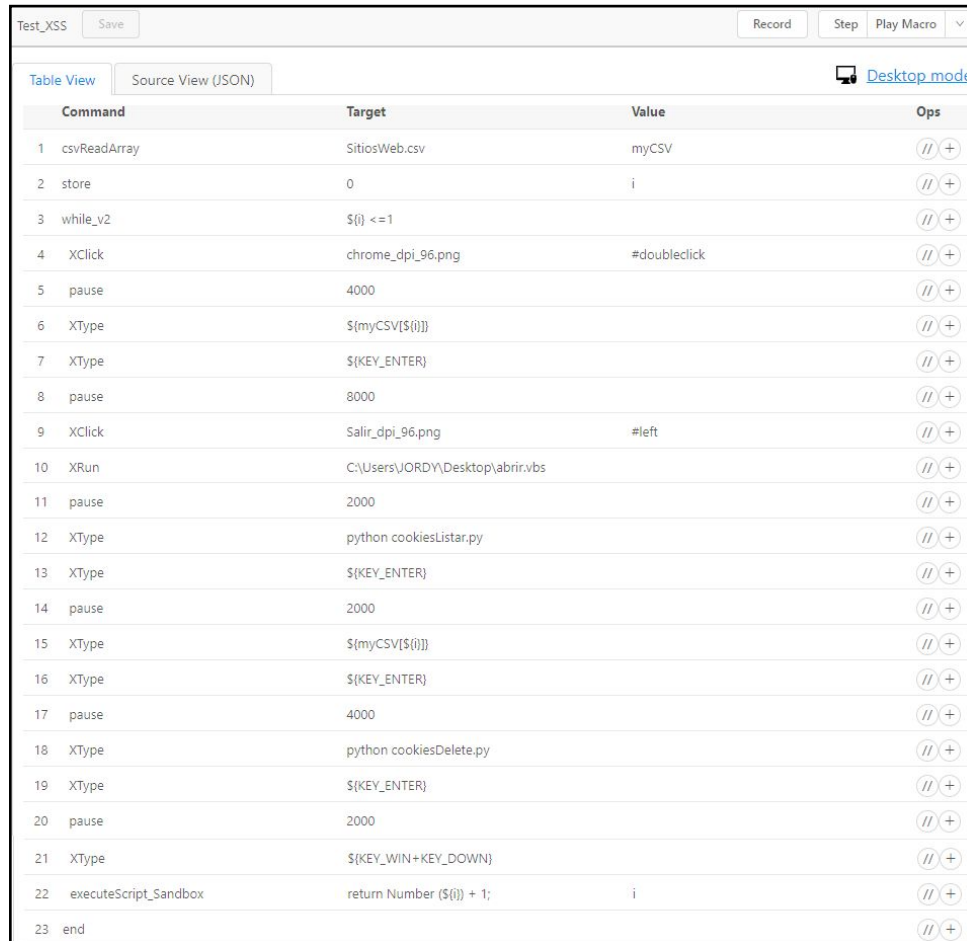
### cookiesDelete.py X

```
analizador > cookiesDelete.py > ...
1 import sqlite3 as sql
2
3 con = sql.connect('./Cookies')
4 cur = con.cursor()
5
6 cur.execute('DELETE FROM cookies')
7 con.commit()
8
9 con.close()
```



# METODOLOGÍA

## Desarrollo del bot en el software UI.Vision



The screenshot displays the UI.Vision software interface. At the top, there are buttons for 'Test\_XSS', 'Save', 'Record', 'Step', and 'Play Macro'. Below these, there are tabs for 'Table View' and 'Source View (JSON)', and a 'Desktop mode' button. The main area contains a table with the following columns: 'Command', 'Target', 'Value', and 'Ops'. The table lists 23 steps of a macro recording process.

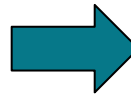
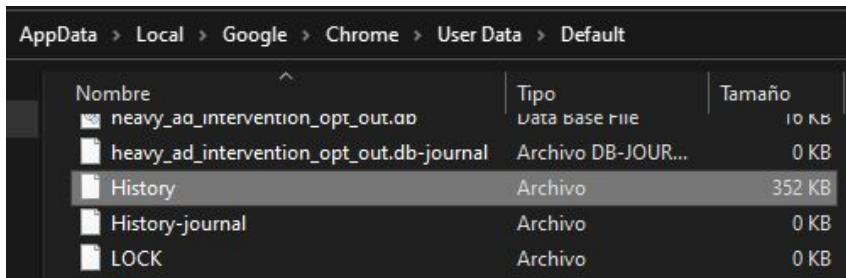
Command	Target	Value	Ops
1 csvReadArray	SitiosWeb.csv	myCSV	// +
2 store	0	i	// +
3 while_v2	\$(i) <= 1		// +
4 XClick	chrome_dpi_96.png	#doubleclick	// +
5 pause	4000		// +
6 XType	\$(myCSV[\$(i)])		// +
7 XType	\$(KEY_ENTER)		// +
8 pause	8000		// +
9 XClick	Salir_dpi_96.png	#left	// +
10 XRun	C:\Users\JORDY\Desktop\abrir.vbs		// +
11 pause	2000		// +
12 XType	python cookiesListar.py		// +
13 XType	\$(KEY_ENTER)		// +
14 pause	2000		// +
15 XType	\$(myCSV[\$(i)])		// +
16 XType	\$(KEY_ENTER)		// +
17 pause	4000		// +
18 XType	python cookiesDelete.py		// +
19 XType	\$(KEY_ENTER)		// +
20 pause	2000		// +
21 XType	\$(KEY_WIN+KEY_DOWN)		// +
22 executeScript_Sandbox	return Number \$(i) + 1;	i	// +
23 end			// +

Una característica de UI.Vision es que el proceso de automatización ya sea web o de escritorio está compuesto por un conjunto de pasos que se ejecutan de manera secuencial.

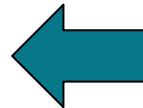
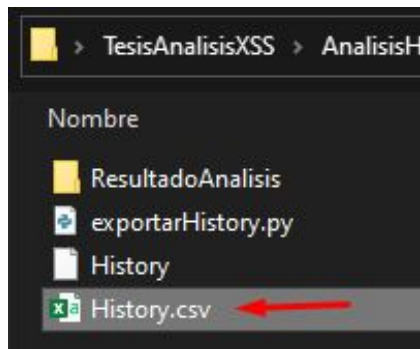


# METODOLOGÍA

## Análisis del historial de visitas de un usuario en Chrome



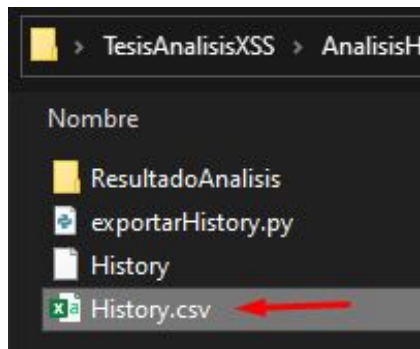
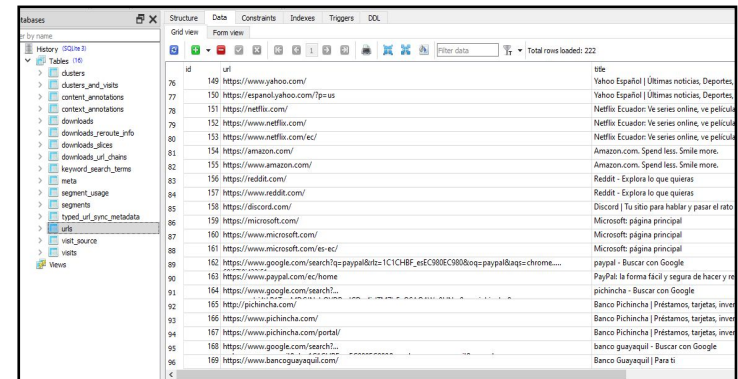
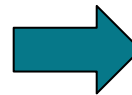
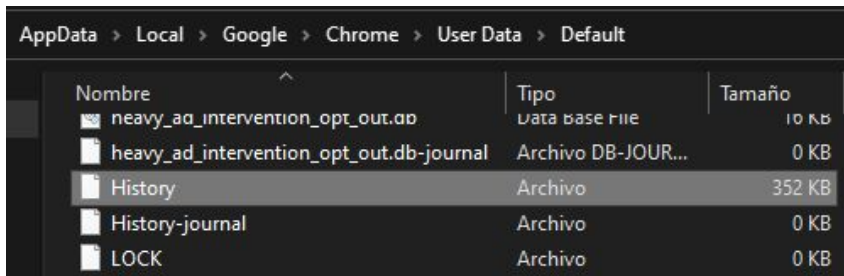
id	url	title
76	https://www.yahoo.com/	Yahoo Español   Últimas noticias, Deportes,
77	https://espanol.yahoo.com/?pa-us	Yahoo Español   Últimas noticias, Deportes,
78	https://netflix.com/	Netflix Ecuador: Ve series online, ve pelucl
79	https://www.netflix.com/	Netflix Ecuador: Ve series online, ve pelucl
80	https://www.netflix.com/ec/	Netflix Ecuador: Ve series online, ve pelucl
81	https://amazon.com/	Amazon.com. Spend less. Smile more.
82	https://www.amazon.com/	Amazon.com. Spend less. Smile more.
83	https://reddit.com/	Reddit - Explora lo que quieras
84	https://www.reddit.com/	Reddit - Explora lo que quieras
85	https://discord.com/	Discord   Tu sitio para hablar y pasar el rato
86	https://microsoft.com/	Microsoft: página principal
87	https://www.microsoft.com/	Microsoft: página principal
88	https://www.microsoft.com/es-ec/	Microsoft: página principal
89	https://www.google.com/search?q=paypal&rlz=C1C1HBF_e5C80EC980&oeq=paypal&aq=chrome...	paypal - Buscar con Google
90	https://www.paypal.com/ec/home	PayPal: la forma fácil y segura de hacer y re
91	https://www.google.com/search?...	pichincha - Buscar con Google
92	http://pichincha.com/	Banco Pichincha   Préstamos, tarjetas, inve
93	https://www.pichincha.com/	Banco Pichincha   Préstamos, tarjetas, inve
94	https://www.pichincha.com/portal/	Banco Pichincha   Préstamos, tarjetas, inve
95	https://www.google.com/search?...	banco guayaquil - Buscar con Google
96	https://www.bancoguayaquil.com/	Banco Guayaquil   Para ti



```
exportarHistory.py X
exportarHistory.py > ...
1 import sqlite3 as sql
2 import pandas as pd
3
4 #-----
5 con = sql.connect('./History')
6
7 #Consulta para obtener los URLs-----
8 sqlhistory = 'SELECT url FROM urls'
9 #-----
10
11 #Exportar los URLs a CSV
12 analisis = pd.read_sql(sql = sqlhistory , con = con)
13 analisis.to_csv("C:\\Users\\JORDY\\Desktop\\TesisAnálisisXSS\\AnálisisHistory\\History.csv", index=False)
14 #-----
15
```



# METODOLOGÍA



```
exportarHistory.py X
exportarHistory.py > ...
1 import sqlite3 as sql
2 import pandas as pd
3
4 #-----
5 con = sql.connect('./History')
6
7 #Consulta para obtener los URLs-----
8 sqlhistory = 'SELECT url FROM urls'
9 #-----
10
11 #Exportar los URLs a CSV
12 analisis = pd.read_sql(sql = sqlhistory , con = con)
13 analisis.to_csv("C:\\Users\\JORDY\\Desktop\\TesisAnálisisXSS\\AnálisisHistory\\History.csv", index=False)
14 #-----
15
```



# METODOLOGÍA

## Análisis de las cookies del historial de Chrome de un usuario

```
EXPLORADOR ... cookiesAnalisisHistory.py X
NETWORK
  analizador > cookiesAnalisisHistory.py > ...
  analizador
  cookiesAnalisis.py
  cookiesAnalisisHistory.py
  cookiesDelete.py
  Cookies
  Cookies-journal
  Network Persistent State
  NetworkDataMigrated
  Reporting and NEL
  Reporting and NEL-journal
  TransportSecurity
  Trust Tokens
  Trust Tokens-journal

1 import sqlite3 as sql
2 import pandas as pd
3
4 #-----
5 con = sql.connect('../Cookies')
6
7 print('\n      **** ANALISIS DE XSSS ****')
8 print(' | TESIS DE GRADO: QUINATAO JORDY - VILLARES JULIO | \n')
9
10 #transformar las fechas -----
11 fecha_creacion = "date(creation_utc/1000000 + (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime')" #Variable que tra
12 fecha_expiracion = "date(expires_utc/1000000 + (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime')" #Variable que t
13
14 conv_fcrToYears = "strftime('%J', date(creation_utc/1000000 + (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime'))"
15 conv_fexToYears = "strftime('%J', date(expires_utc/1000000 + (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime'))"
16 num_years = "round(((+conv_fexToYears+ - +conv_fcrToYears+))/365),4)"
17
18 sql analisis = """SELECT
19     host_key AS DominioCookie, is_secure AS Segura, is_httponly AS HttpOnly,
20     """+fecha_creacion+"" AS FechaCreacion,
21     (CASE
22         WHEN expires_utc > 0
23         THEN """+fecha_expiracion+""
24         ELSE 'Fecha no definida'
25     END) AS FechaExpiracion,
26     (CASE
27         WHEN """+num_years+"" >= 0
28         THEN """+num_years+""
29         ELSE 'No Deff'
30     END) AS NumeroAños,
31     (CASE
32         WHEN (is_secure + is_httponly) = 2 and """+num_years+"" <= 2
33         THEN 'Cookie muy segura'
34         WHEN (is_secure + is_httponly) = 1 and """+num_years+"" <= 2
35         THEN 'Cookie segura'
36         WHEN (is_secure + is_httponly) = 0 and """+num_years+"" <= 2
37         THEN 'Cookie insegura'
38         WHEN (is_secure + is_httponly) = 2 and """+num_years+"" > 2
39         THEN 'Cookie segura'
40         WHEN (is_secure + is_httponly) = 1 and """+num_years+"" > 2
41         THEN 'Cookie insegura'
42         WHEN (is_secure + is_httponly) = 0 and """+num_years+"" > 2
43         THEN 'Cookie muy insegura'
44     END) AS AnalisisCookies
45 FROM
46     cookies"""
47
```

```
45 #Exportar los resultados a un excel
46 analisis = pd.read_sql(sql = sql analisis , con = con)
47 analisis.to_excel("C:\\Users\\JORDY\\Desktop\\TesisAnalisisXSS\\AnalisisHistory\\ResultadoAnalisis\\Analisis_History.xlsx", index=False)
48 #-----
49
50 con.close()
51
52 #Mostrar mensaje en consola
53 print('||||| Resultados exportados correctamente |||||')
54
```





# METODOLOGÍA

historyURLS Save Record

Table View Source View (JSON)

Command	Target	Value
1 csvReadArray	History.csv	historyCSV
2 store	0	i
3 XClick	chrome_dpi_96.png	#doubleclick
4 pause	3000	1
5 while_v2	\$(i) <= 218	
6 XType	\$(KEY_CTRL+KEY_L)	
7 XType	\${historyCSV[\${(i)}]}	
8 XType	\$(KEY_ENTER)	
9 pause	6000	
10 executeScript_Sandbox	return Number (\$(i)) + 1;	i
11 end		
12 XClick	Salir_dpi_96.png	#left
13 pause	2000	2
14 XRun	C:\Users\JORDY\Desktop\abrir.vbs	
15 pause	2000	
16 XType	python cookiesAnalisisHistory.py	
17 pause	2000	
18 XType	\$(KEY_ENTER)	

**Implementación del bot con los procesos para realizar el análisis de las cookies de un usuario en base a su historial de navegación de Chrome**

WHILE que contiene las instrucciones o comandos que cumplen la acción de abrir cada una de las páginas web o URLs del archivo CSV que se extrajeron desde la base de datos "History".

Instrucciones para ejecutar el script "cookiesAnalisisHistory", para obtener el excel de resultados con el análisis de las cookies.



# CAPÍTULO IV

## RESULTADOS



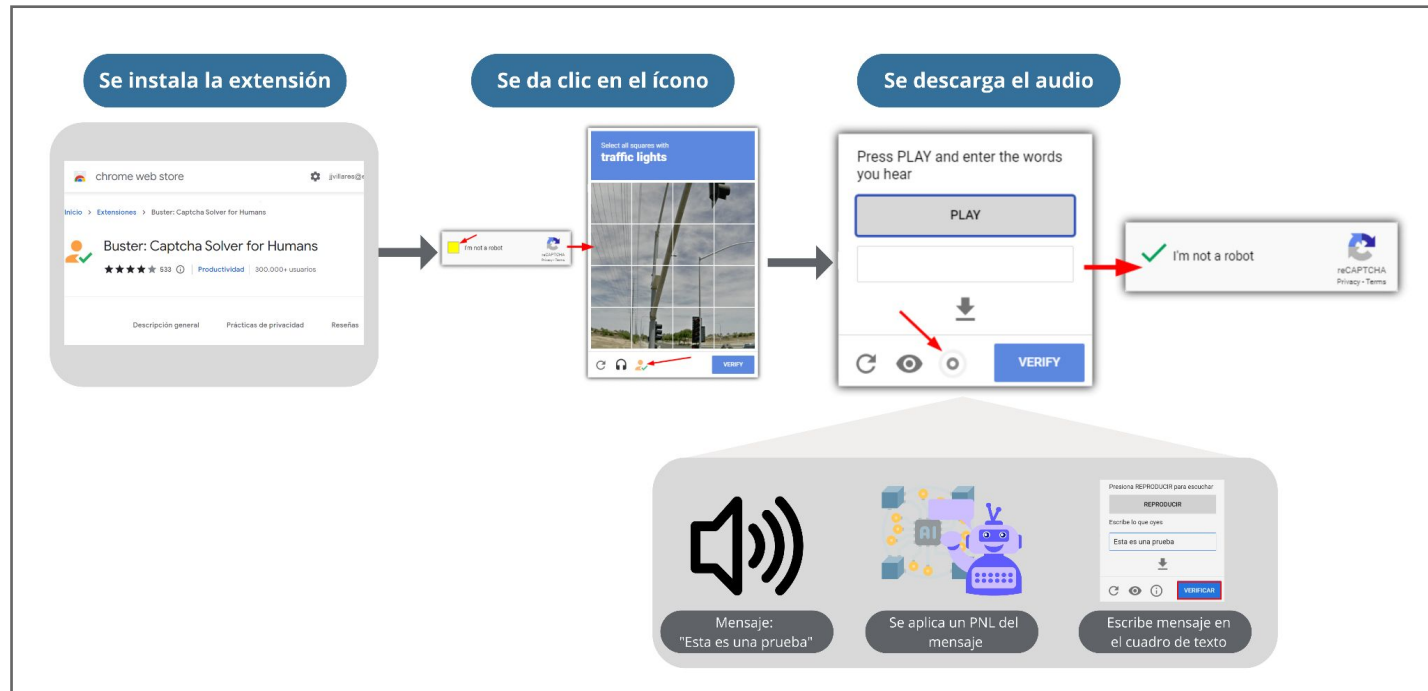
**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA



# RESULTADOS

## Resultados de la solución implementada con alternativas existentes

### Buster: CAPTCHA Solver for Humans



# RESULTADOS

## Anti-CAPTCHA Solving



# RESULTADOS

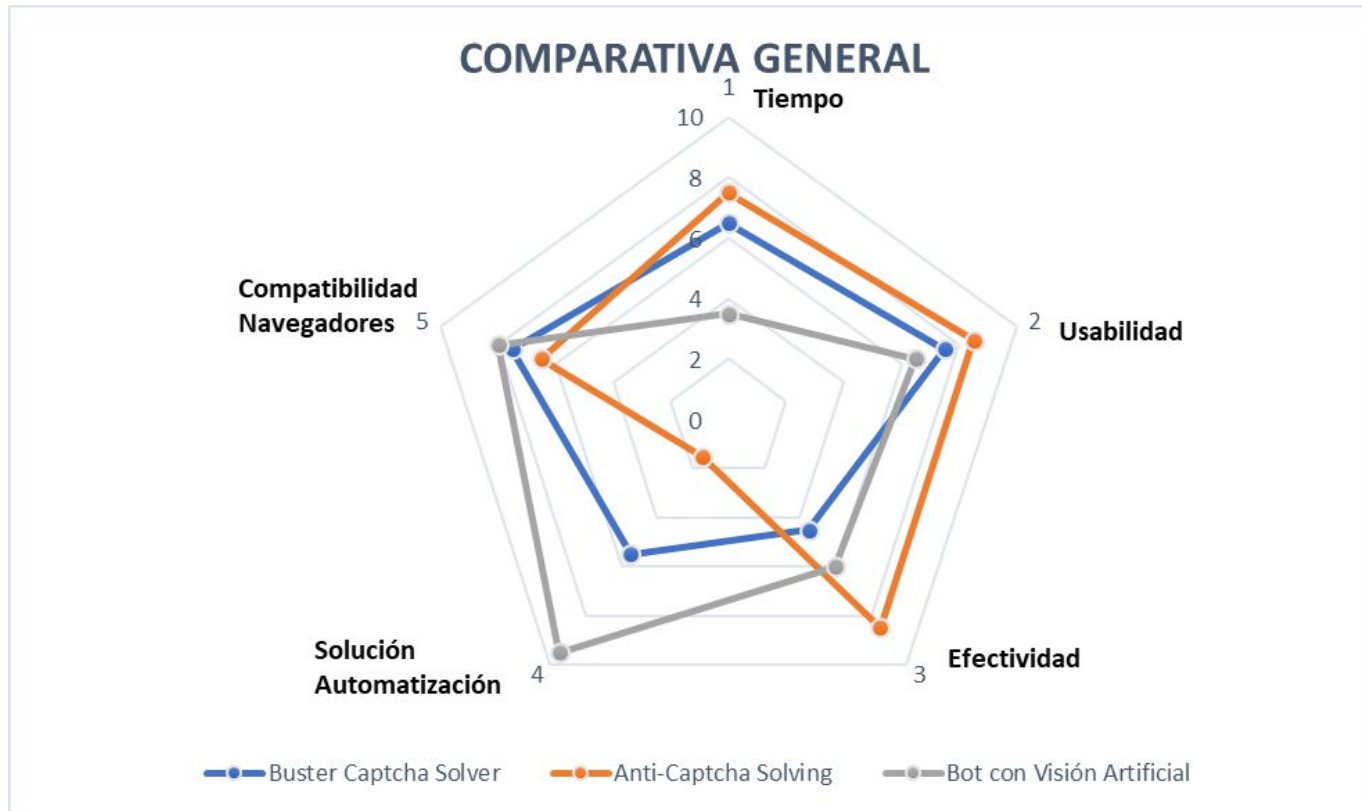
## Análisis comparativo de las soluciones encontradas para resolver CAPTCHA

Parámetros evaluados	Buster CAPTCHA Solver				Anti-CAPTCHA Solving				Bot con Visión Artificial			
	U1	U2	Prom	Cali. A	U1	U2	Prom	Cali. B	U1	U2	Prom	Cali. C
Tiempo de ejecución	6	7	6,5	MEDIO	8	7	7,5	ALTO	3	4	3,5	BAJO
Usabilidad	8	7	7,5	ALTO	9	8	8,5	ALTO	7	6	6,5	MEDIO
Efectividad	5	4	4,5	MEDIO	8	9	8,5	ALTO	7	5	6	MEDIO
Solución para automatización	6	5	5,5	MEDIO	1	2	1,5	BAJO	9	10	9,5	ALTO
Compatibilidad con navegadores	8	7	7,5	ALTO	6	7	6,5	MEDIO	7	9	8	ALTO
	TOTAL		6,3		TOTAL		6,5		TOTAL		6,7	



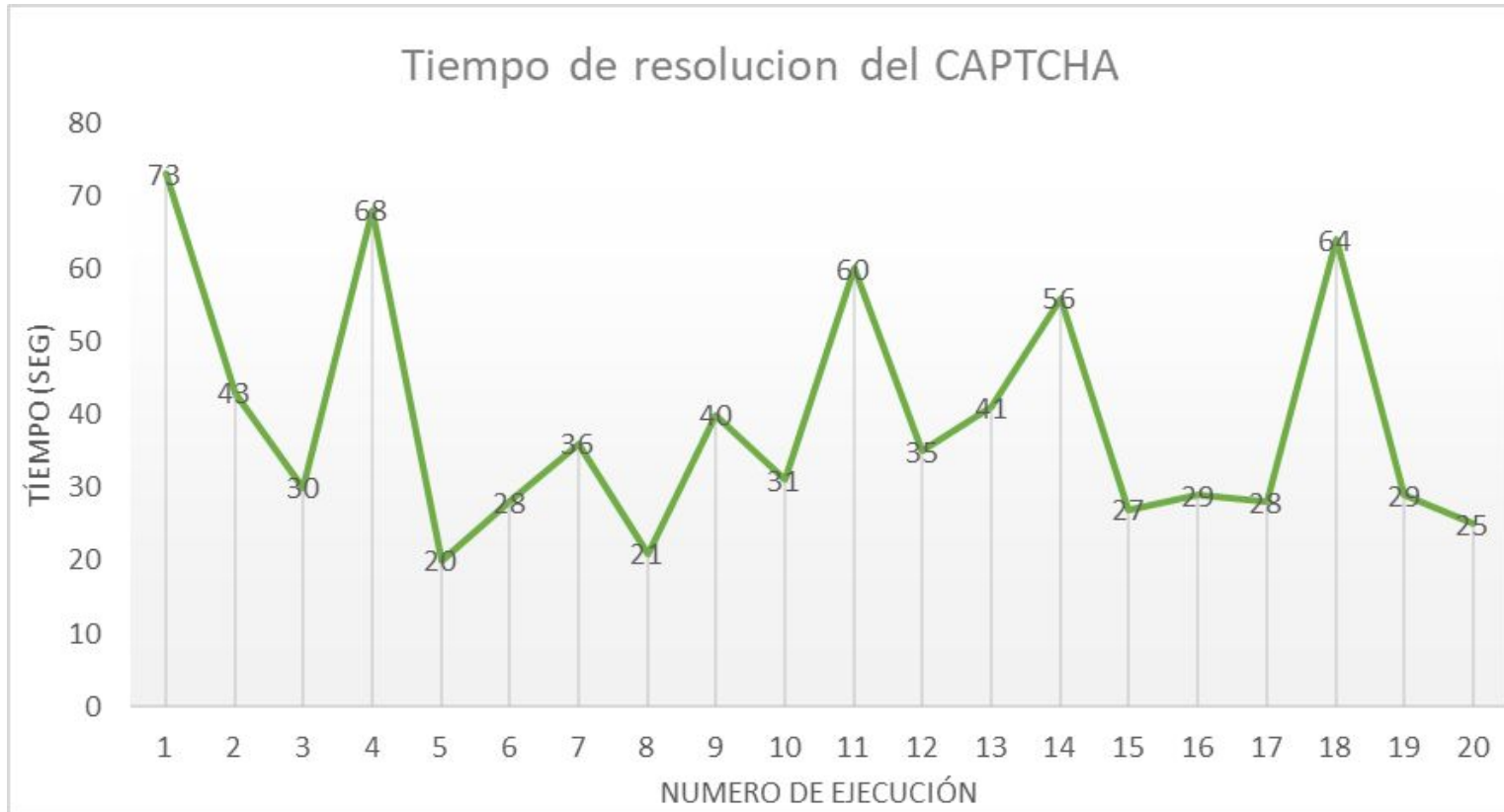
# RESULTADOS

## Análisis general de las herramientas para resolver los sistemas CAPTCHA



# RESULTADOS

## Pruebas de rendimiento y ejecución del Bot

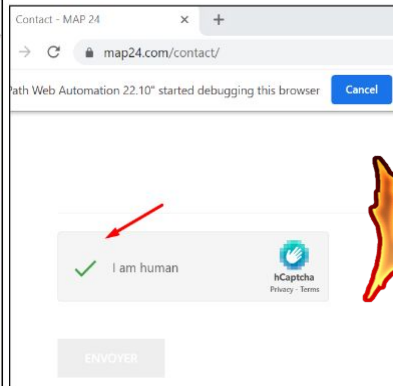
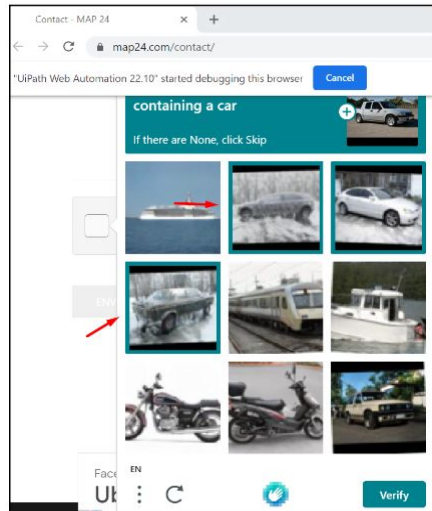


# RESULTADOS

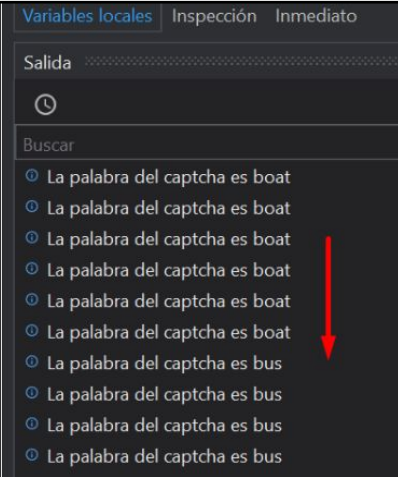
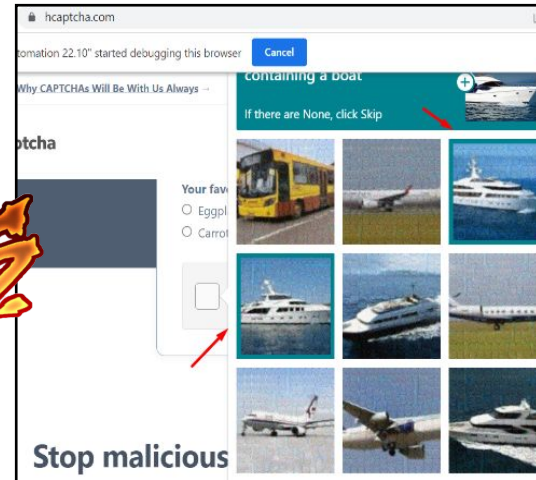
## Pruebas de rendimiento y ejecución del Bot

<https://www.map24.com/contact/>

<https://www.hCAPTCHA.com>



VS



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# RESULTADOS

## Resultados del bot de análisis de ataques XSS a páginas web

### Archivos excel

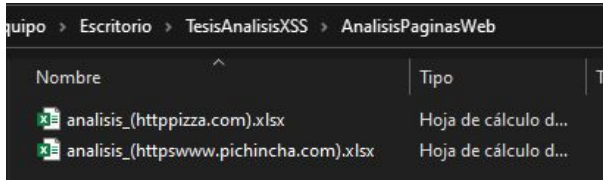
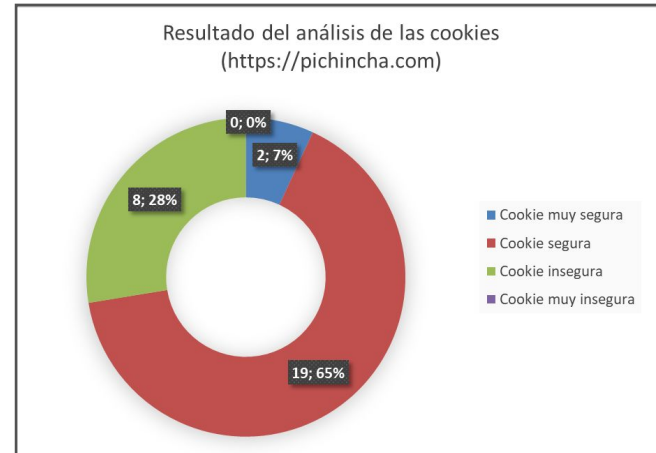


Tabla de resultados

	A	B	C	D	E	F	G
1	DominioCookie	Segura	HttpOnly	FechaCreacion	FechaExpiracion	NumeroAños	AnalisisCookies
2	.doubleclick.net	1	1	2022-07-30	2022-07-30	0	Cookie muy segura
3	.doubleclick.net	1	1	2022-07-30	2024-07-29	2	Cookie muy segura
4	.pizza.com	0	0	2022-07-30	2023-08-24	1.0685	Cookie insegura
5	.pizza.com	0	0	2022-07-30	2023-08-24	1.0685	Cookie insegura
6	.pizza.com	0	0	2022-07-30	2024-07-29	2	Cookie insegura
7	.pizza.com	0	0	2022-07-30	2022-07-30	0	Cookie insegura
8	.pizza.com	0	0	2022-07-30	2022-07-30	0	Cookie insegura
9	.pizza.com	0	0	2022-07-30	2023-01-28	0.4986	Cookie insegura
10	.pizza.com	0	0	2022-07-30	2024-07-29	2	Cookie insegura

### Análisis de las cookies

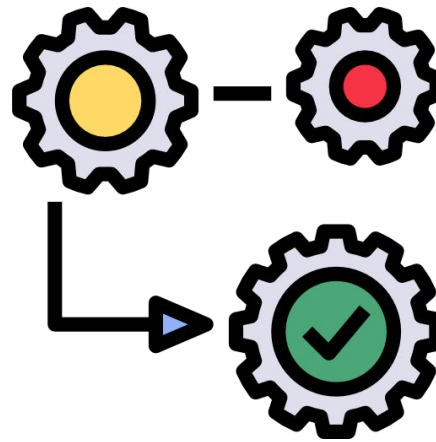




# RESULTADOS

Tiempo de ejecución del bot en base a los dominios analizado

Número de páginas web	Tiempo aproximado
1 página web	38 seg.
2 páginas web	76 seg. (1.26 min.)
10 páginas web	380 seg. (6.33 min)
100 páginas web	3800 seg. (1 hr.)



# RESULTADOS

## Resultados de la solución para el análisis de las cookies del historial de navegación

Archivo CSV del historial

```

C:\Users\JORDA\Desktop\Tesis Analisis XSS Analisis Historial\History.csv - Notepad++
Archivo  Editar  Buscar  Vista  Codificación  Lenguaje  Configuración  Herramientas  Macro  Ejecutar  Plugins  Ventana  ?
History.csv [3]
1 http://haja1ogratia.com/
2 http://haja1ogratia.com/descargar-externas-latino-2.html
3 http://cnn.com/activate
4 http://edition.cnn.com/
5 http://edition.cnn.com/activate
6 http://edition.cnn.com/activate/
7 http://elcomercio.es/
8 http://espa.com/
9 http://howoverlapsuspicious.com/vgeakav4?idiw=100&refer=http%3A%2F%2Fcoincidental.fan%2
10 http://howoverlapsuspicious.com/vgeakav4?key=0f22c1fd609f13cb7547c8cabfe1a90d&submetric
11 http://pichincha.com/
12 http://pizza.com/
13 http://redid.org/
14 http://redid.org/index.php/es/
15 http://warlyaggregation.com/nwtxcun1?key=0f22c1fd609f13cb7547c8cabfe1a90d&submetric=167
16 http://warlyaggregation.com/nwtxcun1?sfzryvs=54&refer=http%3A%2F%2Fwww3.anime.fly.net%2
17 http://www.cnn.com/activate
18 http://xml.fantdm.com/click?i=1&IQXpeJVM1_0
19 https://accounts.google.com/cr/accounts/Signin?asdc=1&sid=2AMU2cyygrTW&uhoqfkiN8FddGh
20 https://accounts.google.com/CheckCookieContinue?http%3A%2F%2Fwww.google.com%2Fsearch%3
21 https://accounts.google.com/ServiceLogin?hl=es-419&passive=true&continue=https://www.goo
22 https://accounts.google.com/signin/v2/challenge/dp?hl=es-419&passive=true&continue=https
23 https://accounts.google.com/signin/v2/challenge/pwd?hl=es-419&passive=true&continue=http
24 https://accounts.google.com/signin/v2/identify?hl=es-419&passive=true&continue=https%3
25 https://accounts.youtube.com/accounts/SetSID?asdc=1&sid=2AMU2cyygrTW&uhoqfkiN8FddGh
26 https://adclick.g.doubleclick.net/pcs/click?xai=AKAQ;auUSOERT_7?oP1OW5-QM4WXR58xMiahXV
27 https://affiliate.igbroker.com/redirect?af=194306&instrument=Options&aff_model=cpa
28 https://allicalidad.si/
29 https://allicalidad.si/!YTUGx8Smc
30 https://amazon.com/
    
```

Tabla de resultados

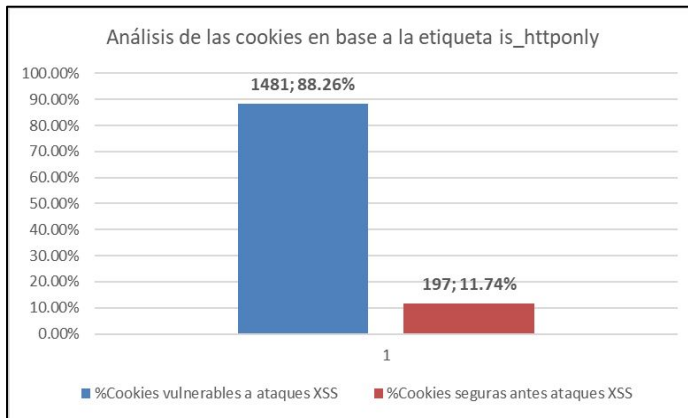
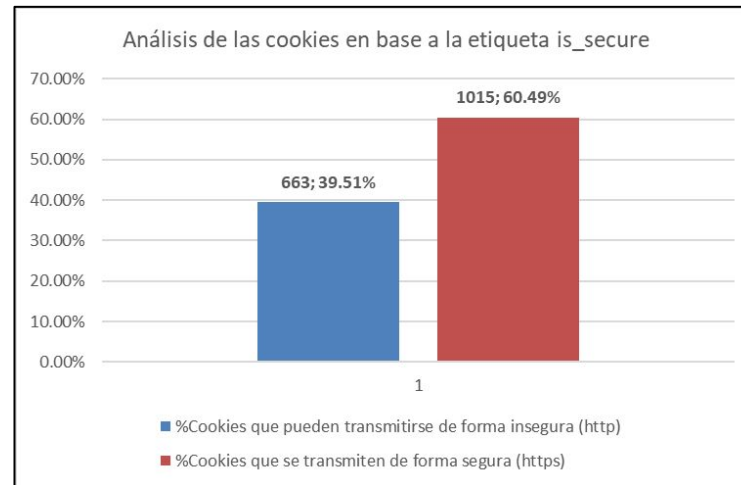
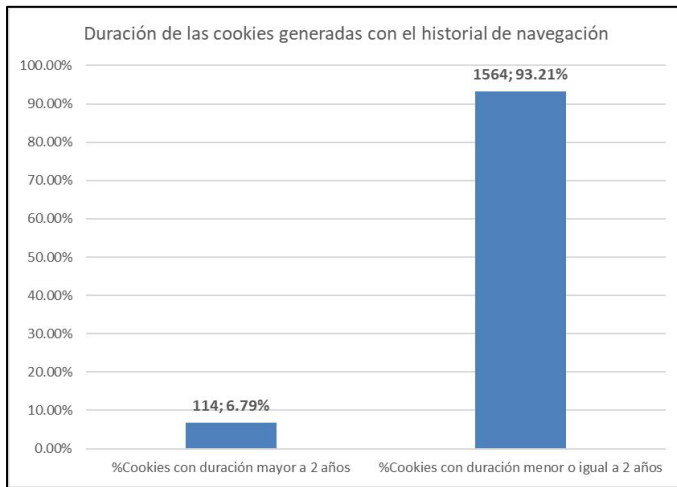
	A	B	C	D	E	F	G
59	.tiktok.com	0	1	2022-07-24	2022-07-24	0	Cookie segura
60	.tiktok.com	0	0	2022-07-24	2022-07-25	0.0027	Cookie insegura
61	.instagram.com	1	1	2022-07-24	2024-07-23	2	Cookie muy segura
62	.instagram.com	1	0	2022-07-24	2023-07-24	1	Cookie segura
63	.instagram.com	1	0	2022-07-24	2024-07-23	2	Cookie segura
64	.tiktok.com	1	1	2022-07-24	2023-07-24	1	Cookie muy segura
65	.twitter.com	0	0	2022-07-23	2024-07-23	2.0027	Cookie muy insegura
66	.twitter.com	0	0	2022-07-24	2022-07-25	0.0027	Cookie insegura
67	.app.link	1	0	2022-07-23	2023-07-24	1.0027	Cookie segura
68	.instagram.com	1	0	2022-07-24	2023-07-23	0.9973	Cookie segura
69	.twitter.com	1	0	2022-07-24	2022-07-25	0.0027	Cookie segura
70	.twitter.com	0	0	2022-07-24	2023-01-20	0.4932	Cookie insegura
71	www.tiktok.com	0	0	2022-07-24	2022-10-22	0.2466	Cookie insegura
72	.youtube.com	1	1	2022-07-24	2024-07-23	2	Cookie muy segura
73	.espe.edu.ec	0	0	2022-07-24	2024-07-23	2	Cookie insegura
74	.espe.edu.ec	0	0	2022-07-24	2022-07-24	0	Cookie insegura
75	.espe.edu.ec	0	0	2022-07-24	2022-07-24	0	Cookie insegura
76	.ww1.cuevana3.me	0	0	2022-07-24	2022-07-24	0	Cookie insegura
77	.espe.edu.ec	0	0	2022-07-24	2023-01-23	0.5014	Cookie insegura
78	.cuevana.email	0	0	2022-07-24	2024-07-23	2	Cookie insegura
79	.cuevana.pro	0	0	2022-07-24	2028-12-31	6.4438	Cookie muy insegura
80	.cuevana.email	0	0	2022-07-24	2022-07-24	0	Cookie insegura
81	.cuevana.email	0	0	2022-07-24	2022-07-25	0.0027	Cookie insegura
82	.arrooget-sanges.icu	1	1	2022-07-24	2022-07-25	0.0027	Cookie muy segura
83	ww3.cuevana.nro	0	0	2022-07-24	2022-07-26	0.0055	Cookie insegura

## Análisis de las cookies



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# RESULTADOS



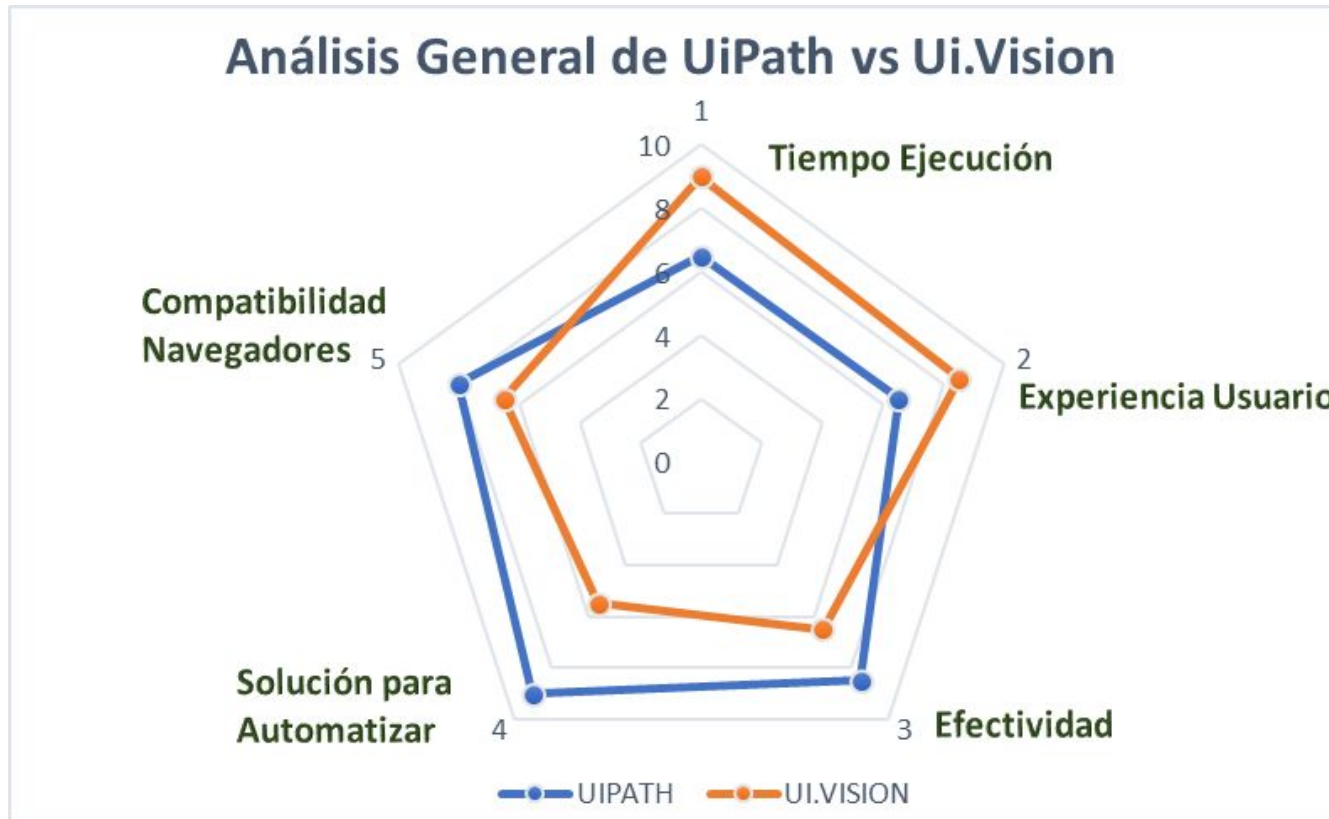
## Tiempo de ejecución del bot para análisis del historial

Número de páginas web	Tiempo aproximado
Historial con 1 URL	27 seg.
Historial con 10 URLs	108 seg. (1.8 min)
Historial con 100 URLs	918 seg. (15.3 min)
Historial con 1000 URLs	9018 seg. (150.3 min)



# RESULTADOS

## Comparativa de las herramientas RPA UiPath y Ui.Vision



# CAPÍTULO V

## CONCLUSIONES Y RECOMENDACIONES



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# CONCLUSIONES

- Se concluye que las técnicas más utilizadas para vulnerar este tipo de medidas de seguridad son los sistemas de reconocimiento de caracteres (OCR), los sistemas de reconocimiento de habla y los analizadores sintácticos, cuya función es intentar resolver los desafíos y simular la interacción de un humano.
- En base al análisis comparativo de las herramientas RPA planteado en este estudio, se determinó que UiPath es una de las soluciones más completas y accesibles del mercado. Su versión Community Edition, a pesar de ser limitada, ofrece las opciones suficientes para implementar una automatización funcional.
- Se cumplió con el objetivo de desarrollar un bot para vulnerar los desafíos de los sistemas CAPTCHA, se utilizó como referencia el mostrado en la página web [www.map24.com](http://www.map24.com) (revista online francesa) que corresponde a un tipo hCapcha, se ha integrado con la API de Google Cloud Vision, proporcionando las técnicas de visión artificial para el análisis de imágenes.
- Cross-site scripting (XSS) se considera como una vulnerabilidad que aprovecha las fallas de seguridad para que los atacantes puedan inyectar scripts ejecutables y maliciosos en aplicaciones o sitios web. Existen tres tipos de ataques, almacenado, reflejado y basado en DOM. Se concluye entonces que el ataque más peligroso es el almacenado porque el atacante inyecta el código malicioso en el servidor web una sola vez y luego afecta a todos los usuarios web que lo visiten.
- Empleando la herramienta UI.Vision se implementó un bot que analiza vulnerabilidades de tipo XSS de una manera rápida y sencilla. A través del estudio de los atributos (nombre, is\_secure, is\_httponly, fecha de creación y fecha de expiración) de las cookies generadas, se observó que los sitios web que utilizan el protocolo HTTP tienden a generar cookies inseguras a comparación de las que usan HTTPs.



# RECOMENDACIONES

- La constante actualización del sistema de visión artificial con las nuevas imágenes que se proporcionan en los desafíos, ya que como se demostró en el presente proyecto, a un bot se le hace más difícil vulnerar imágenes con texturas o patrones incrustados.
- El bot puede llegar a fallar en ciertas ocasiones debido a que las imágenes del CAPTCHA pueden presentar texturas, patrones y/o distorsiones que dificultan el análisis. Para que la detección logre un 100% de efectividad, es recomendable la incorporación de nuevas imágenes con estas características en un dataset propio y actualizado.
- La capacidad de ejecución del bot de análisis de vulnerabilidades XSS realizado en UI.Vision es un punto que se puede mejorar, ya que presenta limitantes relacionadas con el uso de comandos (XClick, XType y XMove) en una misma ejecución. La solución más viable a esta limitante es con la obtención de una licencia para la Edición Personal de UI.Visión RPA XModules.
- Para mejorar la protección de los sistemas de información dentro de la web, se recomienda complementar nuestra propuesta con un verificador de cookies de terceros, ya que estas podrían obtener información confidencial del usuario que visita dicha página.
- Si se va a automatizar un proyecto complejo se recomienda la implementación del software UiPath. Por otro lado, si se desea implementar una automatización sencilla y repetitiva, la utilización de UI.Vision es una muy buena opción, no solo por su facilidad para automatizar, sino también por su portabilidad.





**MUCHAS  
GRACIAS**



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA