



Introducción a ZAP



Pablo Gómez – OWASP Logroño – La Rioja

Mayo 2025



Pablo Gómez Sánchez

- Padre de 2
- Co-Fundador @ Redsauce
- Co-Líder de OWASP Logroño - La Rioja
- Desarrollador, QA automation, cybersec...
- En el Ebro, con la familia o los amigos



✉ pgomez@redsauce.net

🔗 <https://www.linkedin.com/in/pablogomezsanchez/>



¿Qué es ZAP (Zed Attack Proxy)?

Herramienta Open-Source



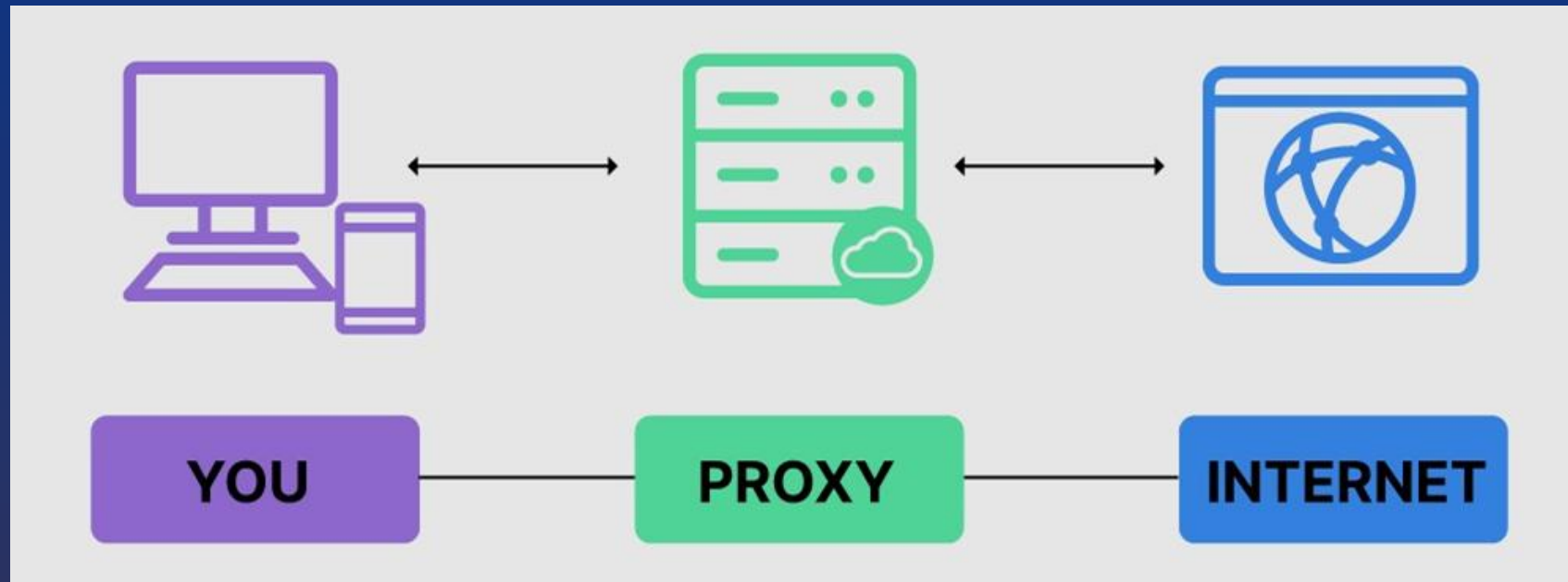
Encuentra
vulnerabilidades



Análisis web manual y
automatizado



Entendiendo el Proxy



Navegador
HTTP/HTTPS

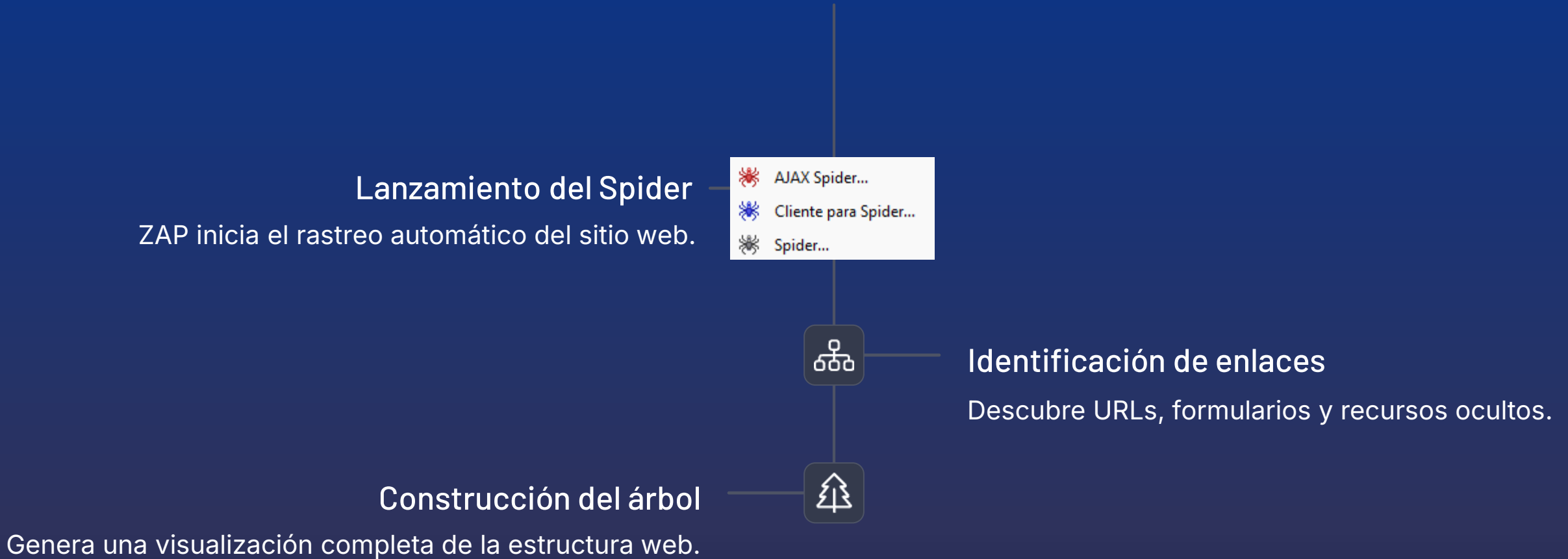
ZAP
Intercepta, analiza
y registra

Servidor Web
Responde a las
peticiones procesadas



Caso de uso 1: mapeo del sitio

Descubrimiento de la estructura

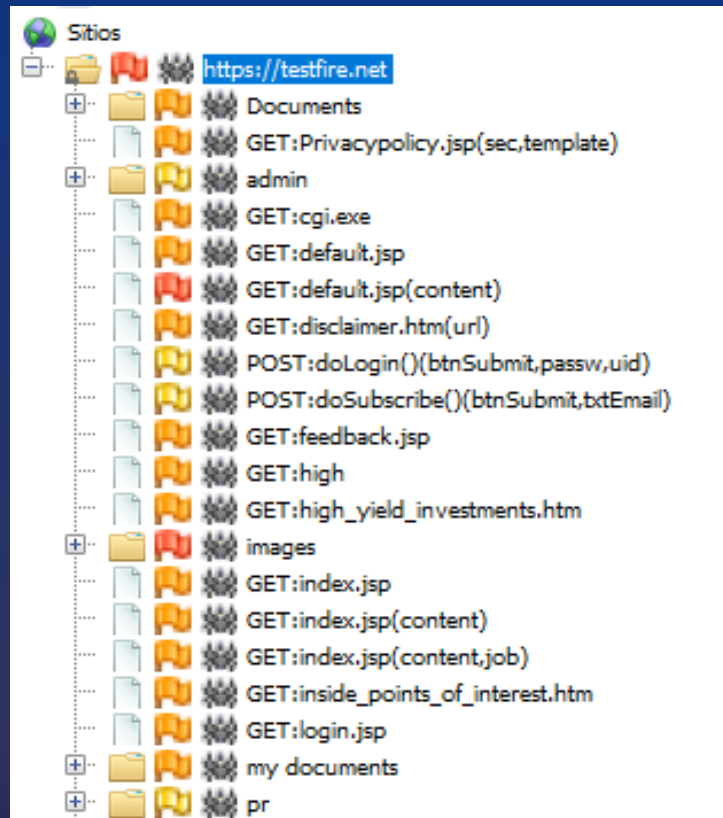




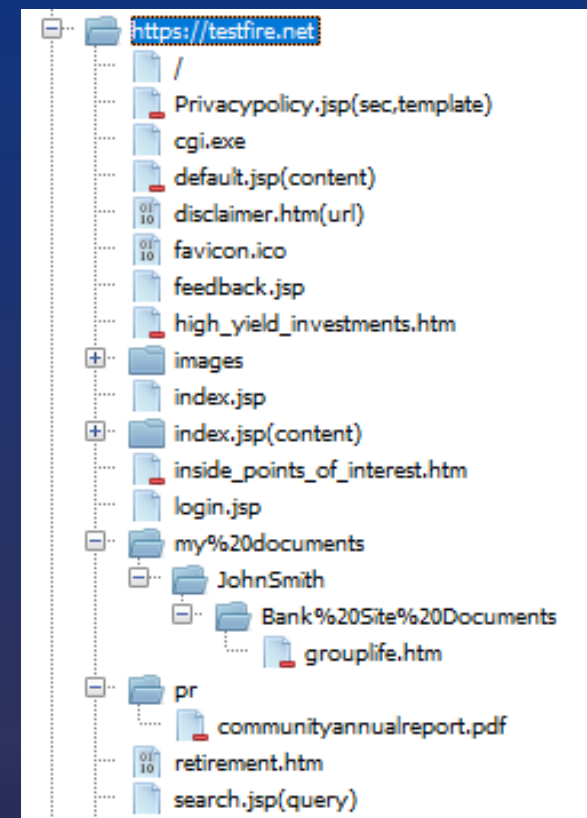
Caso de uso 1: mapeo del sitio

Descubrimiento de la estructura

Spider y AJAX Spider



Client Spider





Caso de uso 2: escaneo activo

Encontrando debilidades ocultas (y sus vulnerabilidades asociadas)





Caso de uso 2: escaneo activo

Encontrando debilidades ocultas (y sus vulnerabilidades asociadas)

The screenshot displays a security scanner interface. On the left, a tree view under 'Alertas (29)' lists various vulnerabilities, with 'Cross Site Scripting (Reflected) (2)' selected. The right pane provides details for this vulnerability:

- Evidencia:** `</p><script>alert(1);</script><p>`
- CWE ID:** 79
- WASC ID:** 8
- Origen:** Activo (40012 - Cross Site Scripting (Reflected))
- Vector de Entrada:** Consulta de formulario
- Descripción:** Cross_site Scripting (XSS) es una técnica de ataque que comprende hacer eco del código que fue proporcionado por el atacante en la instancia del navegador de un usuario. Una instancia de navegador puede ser un cliente de navegador web corriente, o un objeto de navegador integrado e un producto de
- Otra información:**
- Solución:**
 - Fase:** Arquitectura y Diseño
 - Utilizar una biblioteca o framework verificado y confiable que evite esta vulnerabilidad o proporcione elementos que faciliten evitarla.

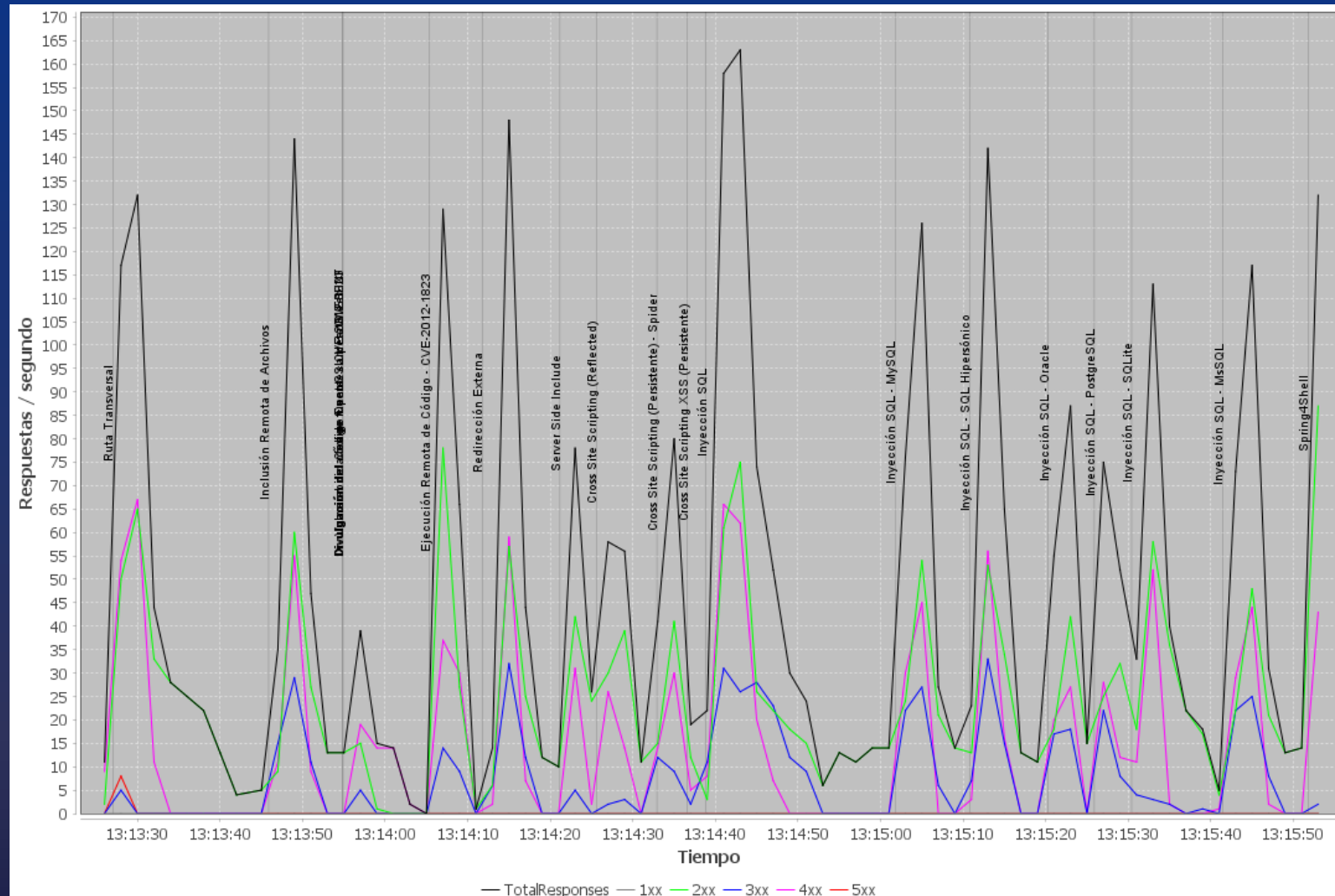


Progreso						
Tabla de respuesta						
Sitio:			http://testfire.net			
	Fuerza	Progreso	Transcurrido	Peticiones	Alertas	Estado
Analizador			00:02.069	12		
Plugin						
Ruta Transversal	Medio		00:18.865	381	0	✓
Inclusión Remota de Archivos	Medio		00:08.987	240	0	✓
Divulgación del código fuente: carpeta /WEB-INF	Medio		00:06.473	43	0	✓
Vulnerabilidades de OpenSSL HeartBleed	Medio		00:10.497	3	0	✓
Divulgación del Código Fuente - CVE-2012-1823	Medio		00:10.496	17	0	✓
Ejecución Remota de Código - CVE-2012-1823	Medio		00:06.389	188	0	✓
Redirección Externa	Medio		00:09.396	216	0	✓
Server Side Include	Medio		00:04.419	96	0	✓
Cross Site Scripting (Reflected)	Medio		00:05.758	114	2	✓
Cross Site Scripting (Persistente) - Prime	Medio		00:01.577	24	0	✓
Cross Site Scripting (Persistente) - Spider	Medio		00:03.699	94	0	✓
Cross Site Scripting XSS (Persistente)	Medio		00:02.229	0	0	✓
Inyección SQL	Medio		00:22.954	565	2	✓
Inyección SQL - MySQL	Medio		00:09.000	240	0	✓
Inyección SQL - SQL Hipersónico	Medio		00:09.488	240	0	✓
Inyección SQL - Oracle	Medio		00:05.606	144	0	✓
Inyección SQL - PostgreSQL	Medio		00:01.022	30	0	⏮
Inyección SQL - SQLite	Medio			0	0	⏮
Sitio cruzado de Scripting (Basado en DOM)	Medio			0	0	⏮
Inyección SQL - MsSQL	Medio			0	0	⏮
Log4Shell	Medio			0	0	⏮



Caso de uso 2: escaneo activo

Encontrando debilidades ocultas (y sus vulnerabilidades asociadas)



Caso de uso 1 y 2: comparativa



En resumen:

Función	Spider	Escaneo Activo
¿Qué hace?	Descubre estructura	Busca vulnerabilidades
¿Lanza ataques?	 No	 Sí
¿Afecta a la app?	 Mínimamente	 Potencialmente destructivo
¿Cuándo usarlo?	Antes de escanear o manual	Tras mapear, para auditar seguridad



Caso de uso 3: escaneo automatizado

El “Modo fácil”: lanzar, esperar y revisar.

Spider(s) + Escaneo activo

- ✗ No se muestran detalles de la ejecución
- ✗ No es posible pausar ni revisar en tiempo real
- ✓ Sencillo y rápido de usar
- ✓ No requiere configuración ni personalización

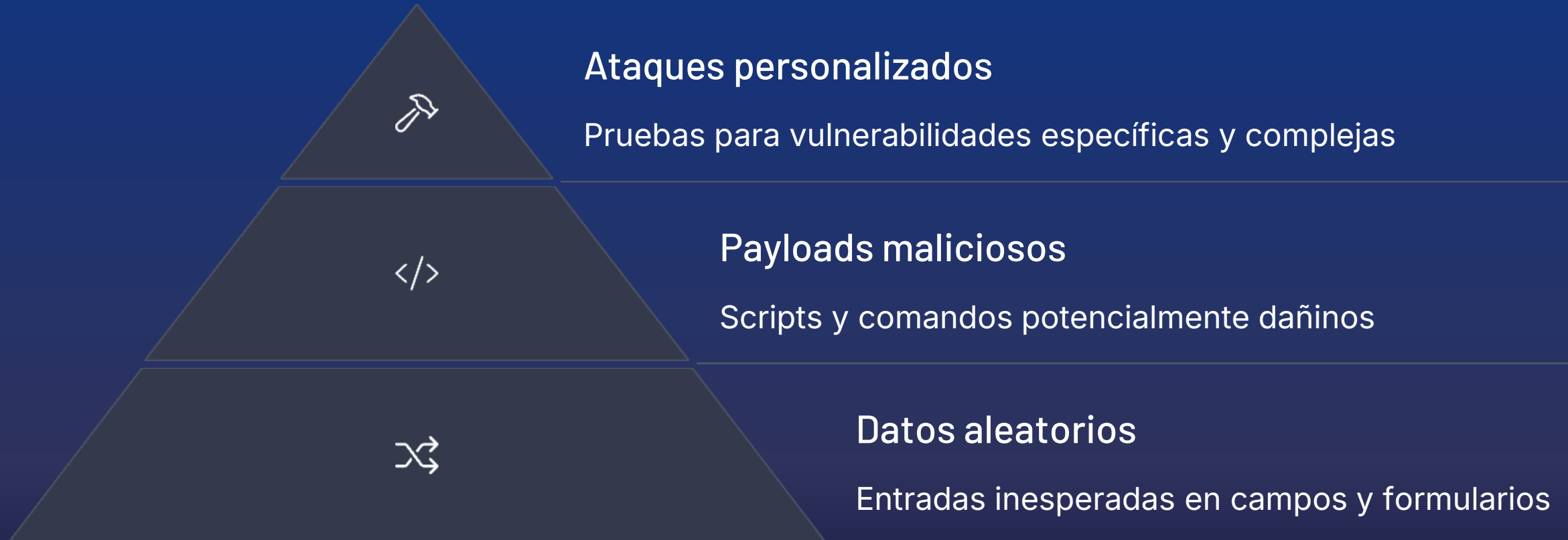
Caso de uso 2 y 3: comparativa



Característica	Escaneo Automatizado	Escaneo Activo
¿Diseñado para...?	Simplicidad / principiantes	Control / usuarios técnicos
¿Feedback en tiempo real?	✗ No	✓ Sí
¿Control de parámetros?	✗ Automático	✓ Total
¿Visible en árbol de sitios?	✗ Limitado	✓ Completo
¿Personalización de reglas?	✗ No	✓ Sí

Caso de uso 4: fuzzing

Probando los límites del sistema





The screenshot displays the Fuzzer application interface. In the background, the 'Ubicaciones de Fuzzeo' (Fuzzing Locations) window is open, showing a list of URLs and a table of fuzzing results. The table has columns for 'Fuzzed', 'Status', 'Time', and 'Size'. The results show multiple successful fuzzing attempts on the URL 'https://testfire.net HTTP/1.1'.

In the foreground, the 'Añadir Carga Útil' (Add Payload) dialog box is open. The 'Tipo' (Type) is set to 'Fuzzers de archivo' (File Fuzzers). The 'Archivos' (Files) section shows a tree view of available payloads. The 'Format String Payloads' option is selected. The 'Vista previa de cargas' (Payload Preview) section displays a list of 13 payloads, including 'Format String Payloads' and 'Format String Errors'.

The 'Format String Payloads' list includes:

- 1: %s%p%x%d
- 2: .1024d
- 3: %.2049d
- 4: %p%p%p%p
- 5: %x%x%x%x
- 6: %d%d%d%d
- 7: %s%s%s
- 8: %s%s%s%s
- 9: %08x
- 10: %*20d
- 11: %*20n
- 12: %*20x
- 13: %*20s



Caso de uso 4: fuzzing

Probando los límites del sistema

Cabecera: Vista R...

Cuerpo: Vista R...

Editar

GET https://testfire.net HTTP/1.1

host: testfire.net

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

sec-ch-ua: "Chromium";v="136", "Google Chrome";v="136", "Not.A/Brand";v="99"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Language: es-ES,es;q=0.9

Ubicaciones de Fuzzeo:

	Posi...	Valor	# de ...	# de ...	
	Cabe...	GET	15	0	
	Cabe...	Mozill...	29	0	
	Cabe...	es-ES...	19	0	

No pedir confirmación al eliminar de la lista ☒



Caso de uso 4: fuzzing

Probando los límites del sistema

Nuevo Fuzzer Progreso: 3: HTTP - https://testfire.... 18 % Fuzzers actuales: 1						
Mensajes enviados: 1503 Errores: 2 ⚠ Mostrar errores						
Identificación de pestaña	Tipo de mensaje	Código	Razón	RTT	Tamaño de la Cabecera de Respuesta	Respuesta (Tamaño del cuerpo)
1.488	Fuzzed	200	OK	472milisegundos	232bytes	0bytes
1.489	Fuzzed	200	OK	447milisegundos	232bytes	0bytes
1.490	Fuzzed	200	OK	472milisegundos	232bytes	0bytes
1.491	Fuzzed	200	OK	472milisegundos	232bytes	0bytes
1.492	Fuzzed	200	OK	472milisegundos	232bytes	0bytes
1.493	Fuzzed	200	OK	433milisegundos	232bytes	0bytes
1.494	Fuzzed	200	OK	433milisegundos	232bytes	0bytes
1.495	Fuzzed	200	OK	416milisegundos	232bytes	0bytes
1.496	Fuzzed	200	OK	453milisegundos	232bytes	0bytes
1.497	Fuzzed	200	OK	428milisegundos	232bytes	0bytes
1.498	Fuzzed	200	OK	451milisegundos	232bytes	0bytes
1.499	Fuzzed	200	OK	419milisegundos	232bytes	0bytes



Caso de uso 4: fuzzing

Probando los límites del sistema

Contextos

Contexto predeterminado

Sitios

```
trace https://testfire.net HTTP/1.1
host: testfire.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
sec-ch-ua: "Chromium";v="136", "Google Chrome";v="136", "Not.A/Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
```

Historial

Buscar

Alertas

Output

Spider(Araña)

AJAX Spider

Escaneo Activo

WebSockets

Fuzzer

+

Nuevo Fuzzer

Progreso: 3: HTTP - https://testfire....

100 %

Fuzzers actuales: 0

Mensajes enviados: 8264

Errores: 2

Mostrar errores

Exportar

Identificación de pestaña	Tipo de mensaje	Código	Razón	RTT	Tamaño de la Cabecera de Respuesta	Respuesta (Tamaño del cuerpo)	Alerta mayor	Estado	Cargas Útiles
2.806	Fuzzed	405	Method Not A...	149milisegundos	134bytes	0bytes			trace, User-Agent...
2.807	Fuzzed	405	Method Not A...	138milisegundos	134bytes	0bytes			trace, User-Agent...
2.808	Fuzzed	405	Method Not A...	137milisegundos	134bytes	0bytes			trace, User-Agent...
2.809	Fuzzed	405	Method Not A...	148milisegundos	134bytes	0bytes			trace, User-Agent...
2.810	Fuzzed	405	Method Not A...	147milisegundos	134bytes	0bytes			trace, User-Agent...
2.811	Fuzzed	405	Method Not A...	147milisegundos	134bytes	0bytes			trace, User-Agent...
2.812	Fuzzed	405	Method Not A...	145milisegundos	134bytes	0bytes			trace, User-Agent...
2.813	Fuzzed	405	Method Not A...	143milisegundos	134bytes	0bytes			trace, User-Agent...
2.814	Fuzzed	405	Method Not A...	143milisegundos	134bytes	0bytes			trace, User-Agent...
2.815	Fuzzed	405	Method Not A...	142milisegundos	134bytes	0bytes			trace, User-Agent...
2.816	Fuzzed	405	Method Not A...	139milisegundos	134bytes	0bytes			trace, User-Agent...



Caso de uso 5: exploración manual

Análisis silencioso del tráfico



Análisis sin intrusión



Reducción de falsos positivos



Detección de fallos lógicos



Útil en acciones complejas (autenticación)



Exploración manual VS Escaneo activo

Tipo de escaneo	Manual	Automático / Activo
Intrusión	✗ No	☑ Sí
Seguridad para producción	☑ Alta	✗ Arriesgado
Detecta configuración insegura	☑ Sí	☑ Sí
Detecta vulnerabilidades técnicas (XSS, SQLi, etc.)	✗ No	☑ Sí
Carga sobre el servidor	⦿ Nula	⦿ Alta
Cobertura completa	⦿ Limitada	☑ Amplia (si se configura bien)



Caso de uso 6: integración continua

Seguridad desde tu CI/CD

Desarrollo
Programadores escriben nuevo código

Despliegue
Código seguro en producción



Control de Versiones

Cambios enviados al repositorio

ZAP Automático

Disparo del escaneo de seguridad

<https://plugins.jenkins.io/zap/>

<https://github.com/zaproxy/action-baseline/tree/master>

<https://gitlab.com/gitlab-org/security-products/dependencies/zaproxy>

ZAP Proxy (@ zaproxy.org)



100%

Gratuito

Código abierto y accesible para todos

1.000+

Casos de uso

Desde desarrollo hasta auditorías profesionales

24/7

Comunidad

Soporte global y actualizaciones constantes



¡Gracias a nuestro colaborador!

SDi Digital
Group

...por invitarnos a sus instalaciones.



OWASP

LOGROÑO - LA RIOJA