

OWASP ZAP

Enrique José Rodríguez Martín

Uo257565@uniovi.es

Resumen

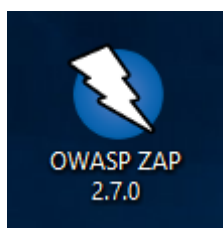
En este trabajo se va a realizar una pequeña introducción al uso de una de las herramientas de pentesting más utilizadas en la actualidad OWASP ZAP, se hablará de su instalación en un sistema Windows y como utilizar sus más básicas funciones siguiendo un tutorial de la web.

1. Introducción

OWASP ZAP se anuncia como una de las herramientas de seguridad de código abierto más utilizadas del mundo, mantenida gracias al esfuerzo de múltiples usuarios de todo el mundo. Entre sus funcionalidades destaca la capacidad de encontrar automáticamente vulnerabilidades en tus aplicaciones web mientras desarrollas y testas las mismas. También es una excelente herramienta para pentesters experimentados que quieren hacer comprobaciones manuales sobre seguridad. ^[1] Esta herramienta está creada en Java por lo que puede ser utilizada desde cualquier sistema operativo y cuando se utiliza como servidor proxy es capaz de otorgar a los usuarios la capacidad de manipular todo el tráfico que pasa a través del proxy, incluido el tráfico del protocolo HTTPS. ^[2] Las siglas ZAP provienen del inglés “Zed Attack Proxy”.

2. Instalación

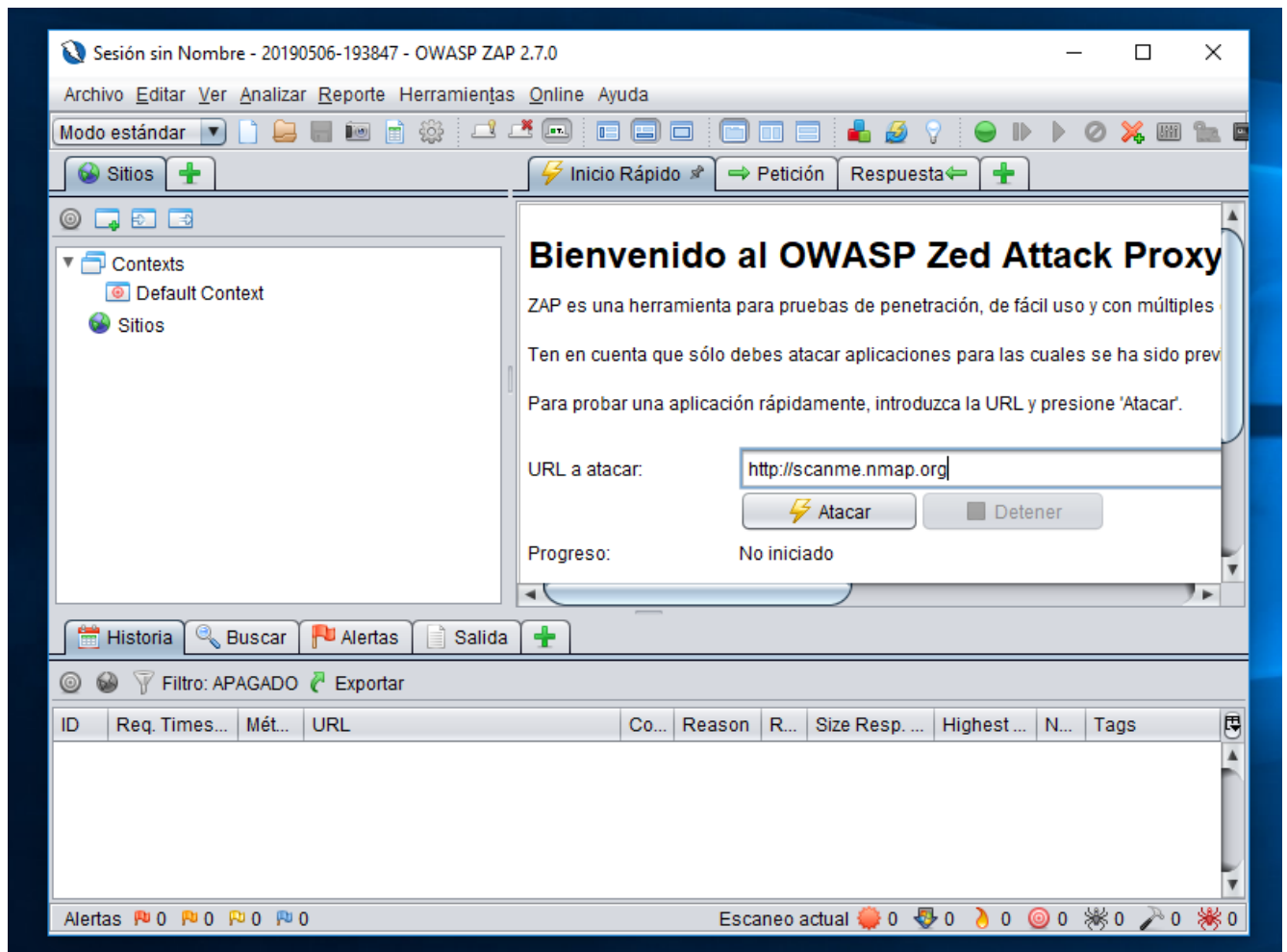
Primero nos dirigimos a su página oficial ^[1], una vez allí pulsamos sobre el botón que nos redirige a su página de descarga, en nuestro caso, vamos a seleccionar el instalador de Windows de 64 bits, una vez con el ejecutable en nuestro poder, procedemos a la instalación, si la instalación se ha completado satisfactoriamente y hemos elegido la instalación estándar, deberíamos tener un nuevo icono de escritorio como este:



Primeros pasos ^[3]

Para este trabajo vamos a seguir el tutorial sobre la herramienta que podemos encontrar en la siguiente página web ^[4]. Iniciamos el programa y siguiendo los pasos del primer apartado del tutorial debemos ingresar la URL a atacar, en nuestro caso será “<http://scanme.nmap.org>”, hay que tener en cuenta que debemos ingresar en el campo del formulario el protocolo con el que se comunica el sitio a atacar ya que de

no hacerse, se nos mostrará diálogo de error. Simplemente tenemos que pulsar el botón atacar de la pestaña inicio rápido.



Podemos detener el escaneo activo cuando queramos e incluso exportar los resultados a un .csv:

ID,Req. Timestamp,Resp. Timestamp,MÃ©todo,URL,Code,Reason,RTT,Size Resp. Header,Size Resp. Body

692,Mon May 06 19:46:01 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons?query=%5Cicons,404,Not Found,176,160,283

693,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=..%2F..%2F..%2F..%2F..

694,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=c%3A%5CWindows%5Csyste

695,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/folder.gif?query=c%3A%2FWindows%2Fsyste

696,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=..%5C..%5C..%5C..%5C..

697,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/folder.gif?query=..%2F..%2F..%2F..%2F..

698,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=%2Fetc%2Fpasswd,200,OK,1

699,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/folder.gif?query=c%3A%5CWindows%5Csyst

700,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=..%2F..%2F..%2F..%2F..

701,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:02 CEST 2019,GET,http://scanme.nmap.org/icons/folder.gif?query=..%5C..%5C..%5C..%5C..

702,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:03 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=c%3A%2F,200,OK,176,227,14

703,Mon May 06 19:46:02 CEST 2019,Mon May 06 19:46:03 CEST 2019,GET,http://scanme.nmap.org/icons/folder.gif?query=%2Fetc%2Fpasswd,200,OK,1

704,Mon May 06 19:46:03 CEST 2019,Mon May 06 19:46:03 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=%2F,200,OK,178,227,148

705,Mon May 06 19:46:03 CEST 2019,Mon May 06 19:46:03 CEST 2019,GET,http://scanme.nmap.org/icons/folder.gif?query=..%2F..%2F..%2F..%2F..

706,Mon May 06 19:46:03 CEST 2019,Mon May 06 19:46:03 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=c%3A%5C,200,OK,176,227,14

707,Mon May 06 19:46:03 CEST 2019,Mon May 06 19:46:03 CEST 2019,GET,http://scanme.nmap.org/icons/folder.gif?query=c%3A%2F,200,OK,171,227,2

708,Mon May 06 19:46:03 CEST 2019,Mon May 06 19:46:03 CEST 2019,GET,http://scanme.nmap.org/icons/blank.gif?query=..%2F..%2F..%2F..%2F..

Sección sin Nombre - 20190506-193847 - OWASP ZAP 2.7.0

Archivo Editar Ver Analizar Reporte Herramientas Online Ayuda

Modo estándar

Sitios

Contexts

Default Context

Sitios

Inicio Rápido

Petición

Respuesta

Ten en cuenta que sólo debes atacar aplicaciones para las cuales se ha sido previamente autorizado.

Para probar una aplicación rápidamente, introduzca la URL y presione 'Atacar'.

URL a atacar: http://scanme.nmap.org

Atacar Detener

Progreso: Detenido manualmente

Para un análisis más en profundidad de la prueba se debe explorar la aplicación mediante pruebas de regresión automática.

Si usted está usando Firefox 24.0 o superior puede usar 'Plug-n-Hack' para configurar su navegador.

Historia Buscar Alertas Salida Spider(Araña) Escaneo Activo

Nuevo escaneo : Progreso: 1: http://scanme.nmap.org 5%

Escaneo actual: 0 Número de peticiones: 1112 Exportar

ID	Req. Timestamp	Resp. Timestamp	Método	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1.681	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/images/tople...	200	OK	168 ...	228 bytes	266 bytes
1.682	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.683	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	180 ...	171 bytes	2.300 bytes
1.684	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.685	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	168 ...	190 bytes	2.300 bytes
1.686	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.687	6/05/19 19:47:45	6/05/19 19:47:46	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	180 ...	171 bytes	2.300 bytes
1.688	6/05/19 19:47:46	6/05/19 19:47:46	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.689	6/05/19 19:47:45	6/05/19 19:47:46	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	352 ...	171 bytes	2.300 bytes
1.690	6/05/19 19:47:46	6/05/19 19:47:46	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.691	6/05/19 19:47:46	6/05/19 19:47:46	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	176 ...	171 bytes	2.300 bytes

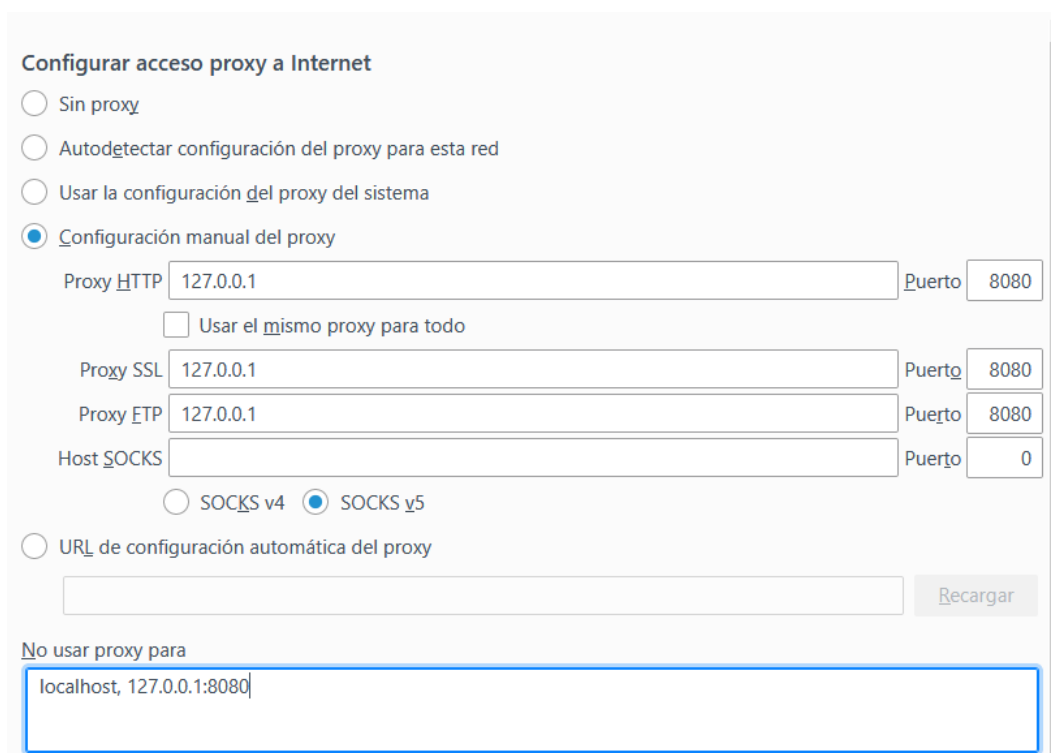
Alertas 0 2 3 0

Escaneo actual 0 0 0 0 0 0 0 0 0 0

Esto nos permite analizar con mayor detenimiento los datos obtenidos incluso realizar una serie de filtrados posteriores utilizando otras herramientas que nos pueden esclarecer o precisar la búsqueda.

Interceptación por proxy: ^[5]

Para poder realizar este apartado modificaremos nuestra configuración, para ello vamos a utilizar el navegador Firefox ya que es un navegador más cómodo a lo que editar la configuración se refiere:



Configurar acceso proxy a Internet

☐ Sin proxy

☐ Autodetectar configuración del proxy para esta red

☐ Usar la configuración del proxy del sistema

☒ Configuración manual del proxy

Proxy HTTP: 127.0.0.1 Puerto: 8080

☐ Usar el mismo proxy para todo

Proxy SSL: 127.0.0.1 Puerto: 8080

Proxy FTP: 127.0.0.1 Puerto: 8080

Host SOCKS: Puerto: 0

☐ SOCKS v4 ☒ SOCKS v5

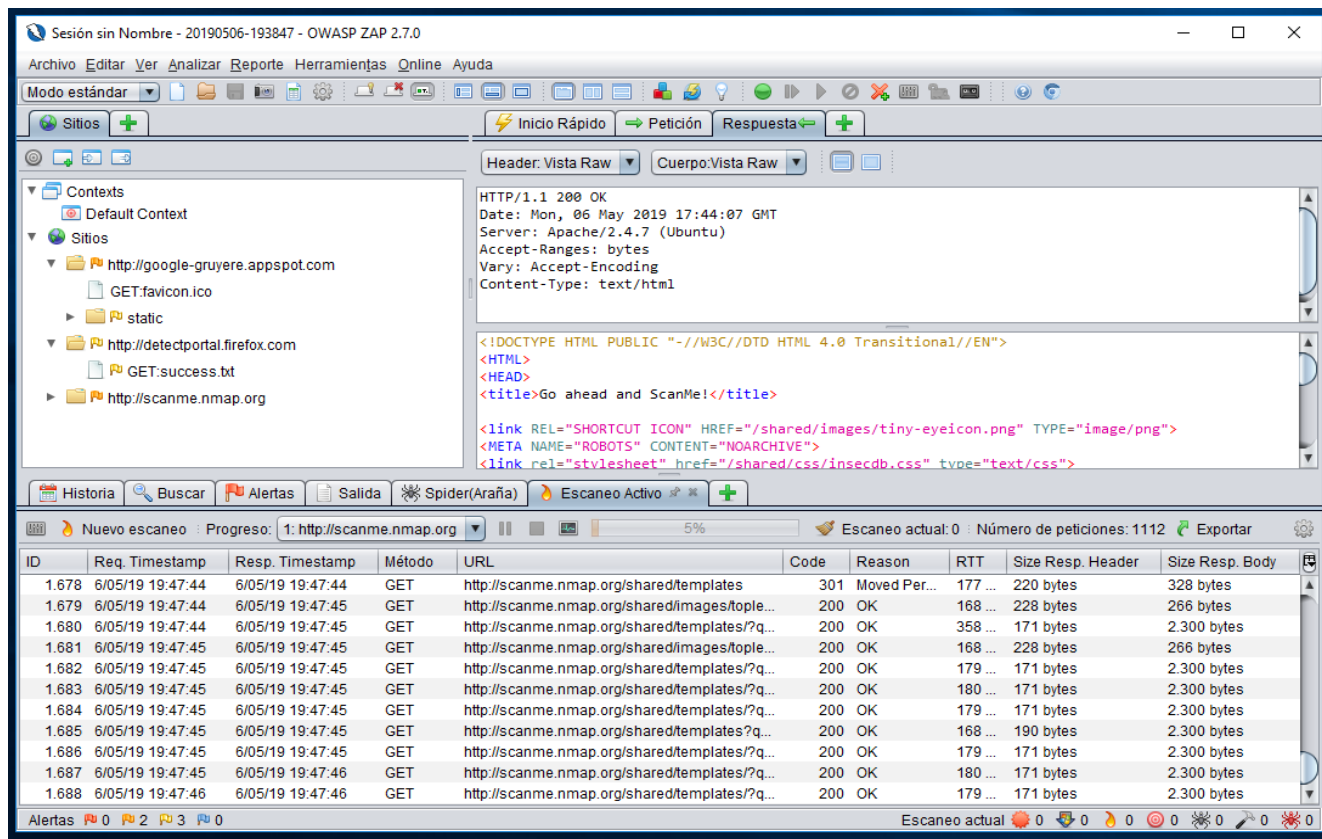
☐ URL de configuración automática del proxy

Recargar

No usar proxy para

localhost, 127.0.0.1:8080

Ahora accedemos a “Google Gruyere” ^[6] desde Firefox. Si teníamos previamente ZAP abierto deberíamos apreciar varios cambios ya que ZAP ha comenzado a analizar los sitios que hemos visitado, pudiendo nosotros observar el contenido de las peticiones y respuestas entre nuestro navegador y el servidor que aloja la web.



Sesión sin Nombre - 20190506-193847 - OWASP ZAP 2.7.0

Archivo Editar Ver Analizar Reporte Herramientas Online Ayuda

Modo estándar

Sitios

- Contexts
 - Default Context
- Sitios
 - http://google-gruyere.appspot.com
 - GET:favicon.ico
 - static
 - http://detectportal.firefox.com
 - GET:success.txt
 - http://scanme.nmap.org

Header: Vista Raw

Cuerpo: Vista Raw

```
HTTP/1.1 200 OK
Date: Mon, 06 May 2019 17:44:07 GMT
Server: Apache/2.4.7 (Ubuntu)
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
<title>Go ahead and ScanMe!</title>
<link REL="SHORTCUT ICON" HREF="/shared/images/tiny-eyeicon.png" TYPE="image/png">
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
<link rel="stylesheet" href="/shared/css/insecd.css" type="text/css">
```

Historia Buscar Alertas Salida Spider(Araña) Escaneo Activo

Nuevo escaneo Progreso: 1: http://scanme.nmap.org 5%

Escaneo actual: 0 Número de peticiones: 1112 Exportar

ID	Req. Timestamp	Resp. Timestamp	Método	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1.678	6/05/19 19:47:44	6/05/19 19:47:44	GET	http://scanme.nmap.org/shared/templates	301	Moved Per...	177 ...	220 bytes	328 bytes
1.679	6/05/19 19:47:44	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/images/tople...	200	OK	168 ...	228 bytes	266 bytes
1.680	6/05/19 19:47:44	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	358 ...	171 bytes	2.300 bytes
1.681	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/images/tople...	200	OK	168 ...	228 bytes	266 bytes
1.682	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.683	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	180 ...	171 bytes	2.300 bytes
1.684	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.685	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	168 ...	190 bytes	2.300 bytes
1.686	6/05/19 19:47:45	6/05/19 19:47:45	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes
1.687	6/05/19 19:47:45	6/05/19 19:47:46	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	180 ...	171 bytes	2.300 bytes
1.688	6/05/19 19:47:46	6/05/19 19:47:46	GET	http://scanme.nmap.org/shared/templates/?q...	200	OK	179 ...	171 bytes	2.300 bytes

Alertas 0 2 3 0

Escaneo actual 0 0 0 0 0 0 0 0 0 0

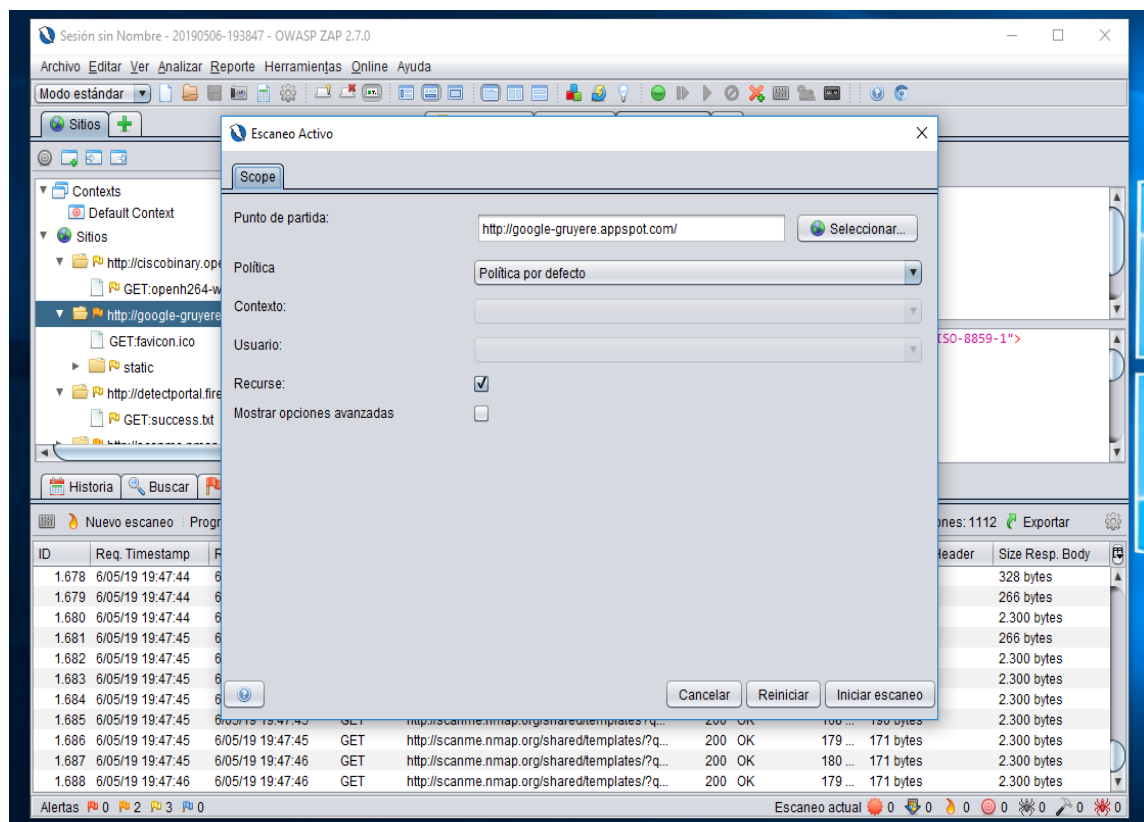
ZAP nos permite en este momento analizar el tráfico con este sitio o con otros si queremos simultáneamente analizar varios sitios, nos permite, por ejemplo comprobar cómo se envían las credenciales a nuestro servidor para así evitar exponer a nuestros usuarios, nos permite filtrar las peticiones con el sitio para tener un entorno de trabajo más organizado o simplemente queremos afinar nuestra búsqueda, también podemos utilizar las funciones de “breakpoints” es decir podemos detener peticiones antes de enviarlas para un análisis paso a paso más exhaustivo, esta funcionalidad nos permite modificar las peticiones y comprobar como reaccionaría un sistema en caso de ataque.

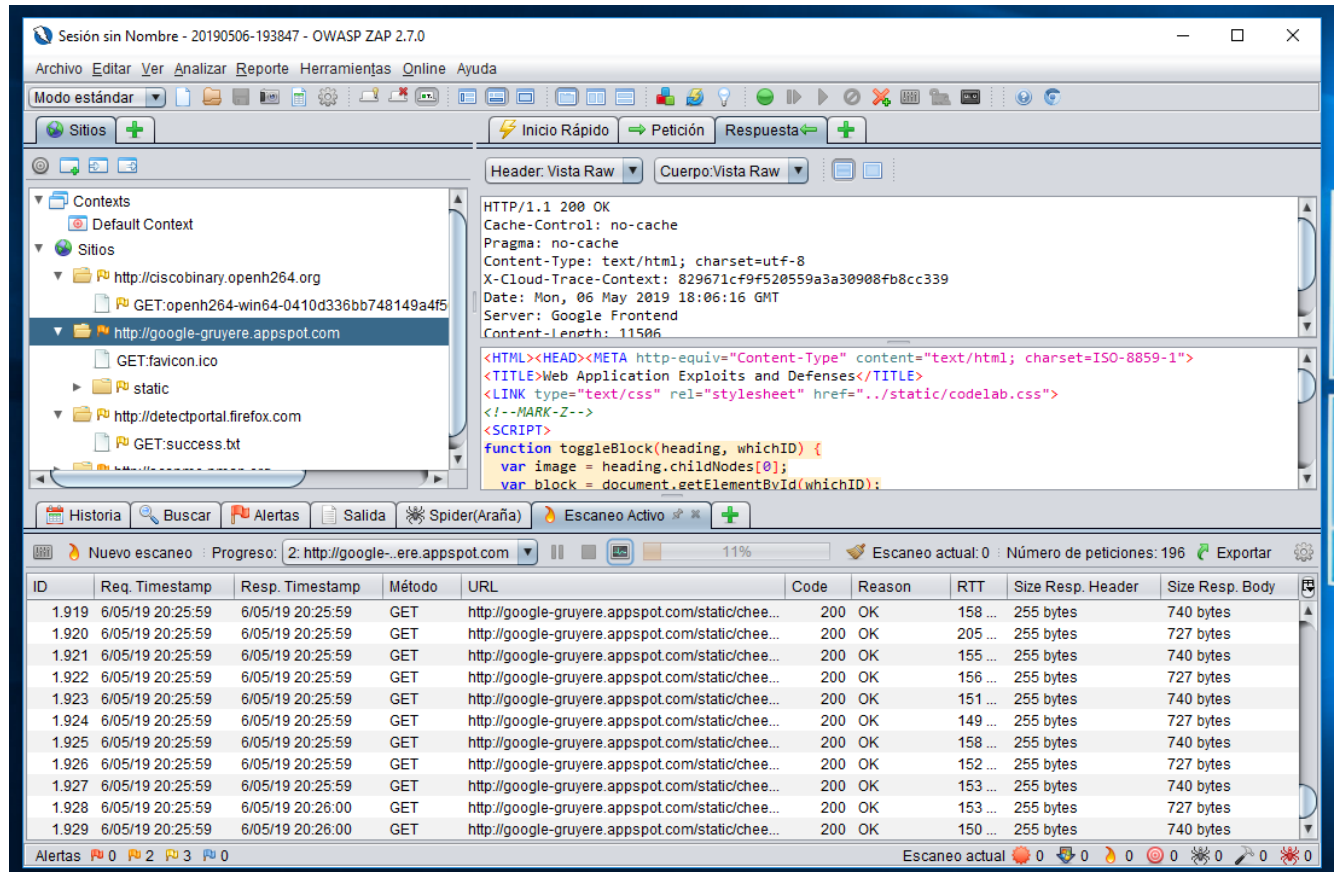
Escaneo pasivo con ZAP ^[7]

ZAP nos permite escanear de forma pasiva las respuestas del servidor de forma no intrusiva, podemos definir las reglas que utiliza usando la ventana de ajustes, pudiendo añadir, modificar y eliminar dichas reglas. Esto nos permite analizar con muchísima más precisión la interacción de nuestro buscador con el servidor. Estas reglas tienen múltiples funcionalidades como detectar comentarios, direcciones de correo, cookies entre otros elementos de interés para nuestro análisis.

Escaneo activo con ZAP ^[7]

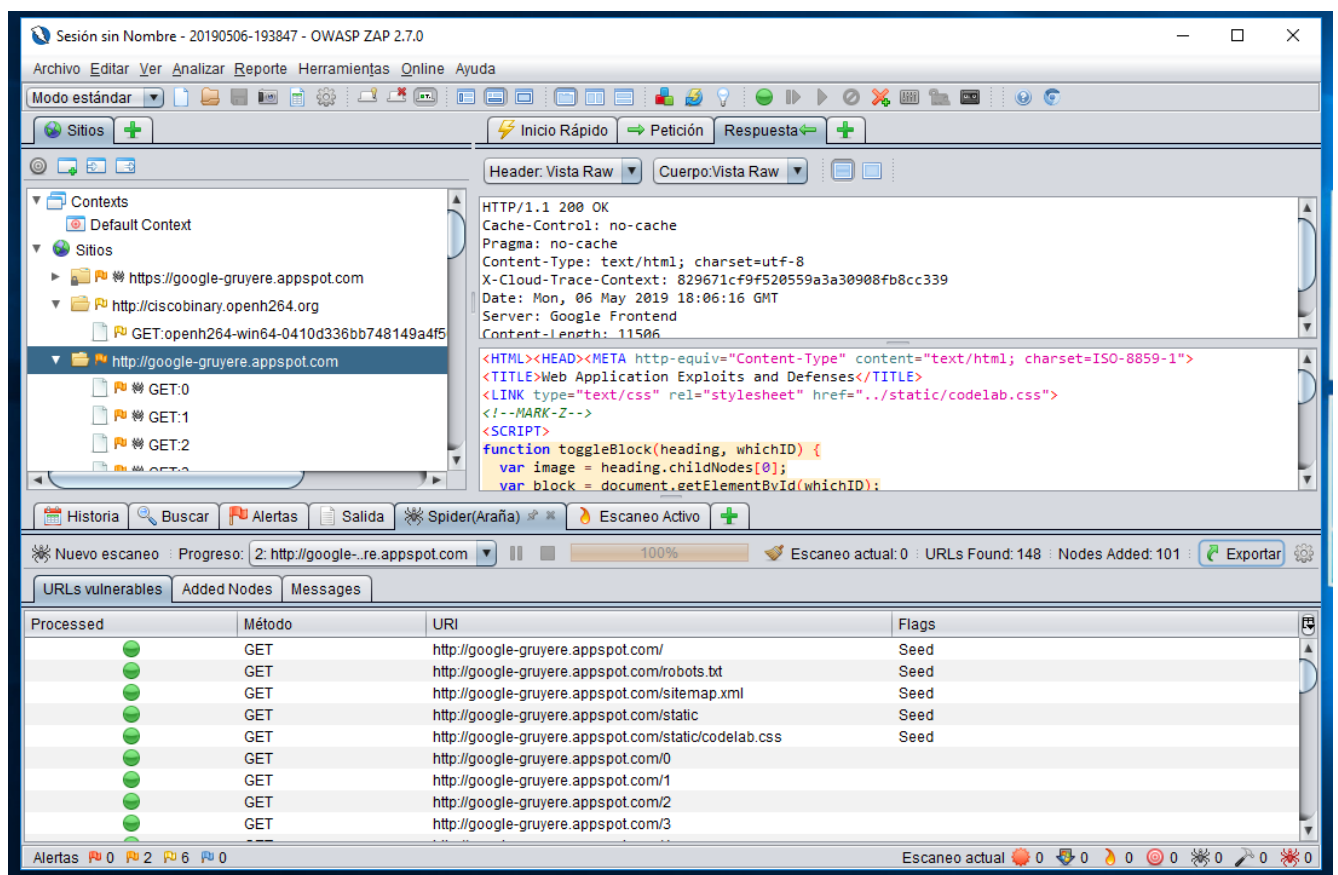
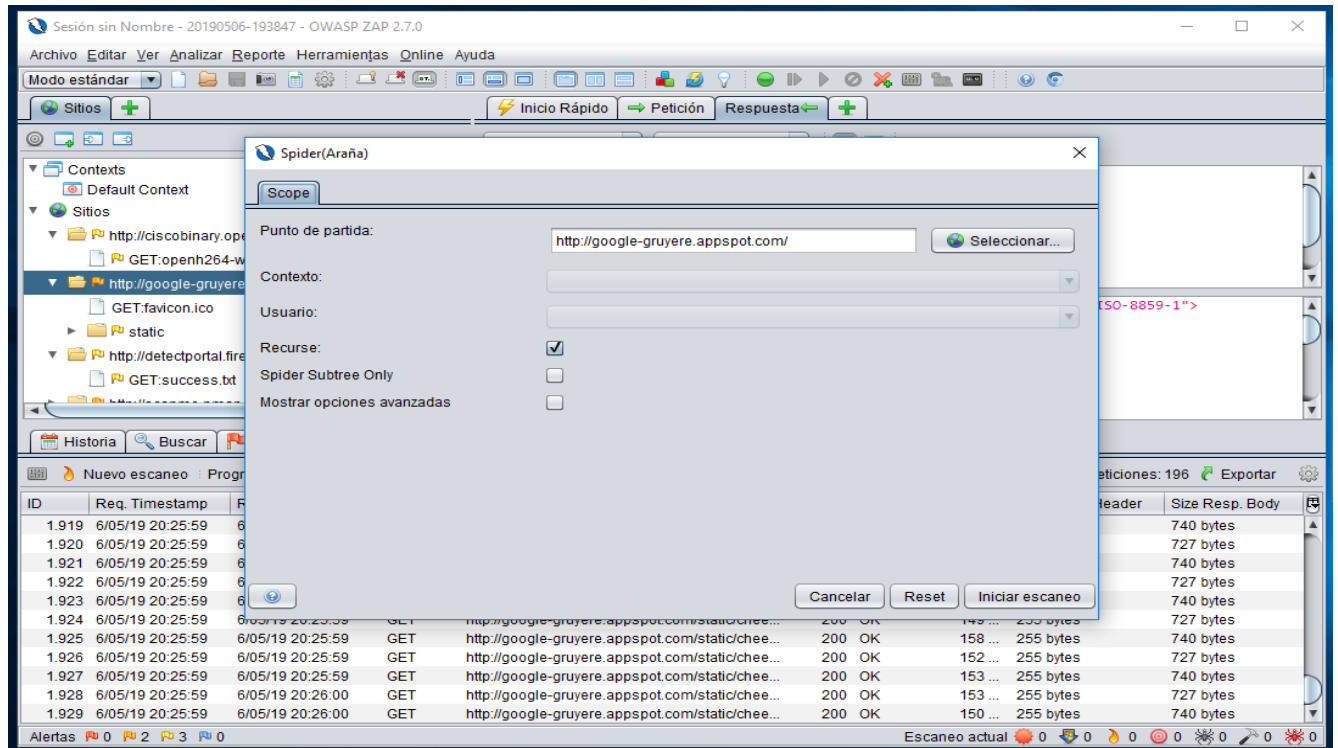
De la misma forma que hemos realizado con anterioridad un escaneo pasivo podemos realizarlo de manera activa contra un sitio, para ello solo tenemos que haber visitado la página, es decir, tenerla en nuestra pestaña de sitios y mediante clic derecho -> atacar -> Iniciar escaneo ... el programa iniciará el escaneo. Se recomienda antes de realizar un escaneo activo haber realizado con anterioridad un escaneo pasivo aumentando la granularidad de nuestro ataque.





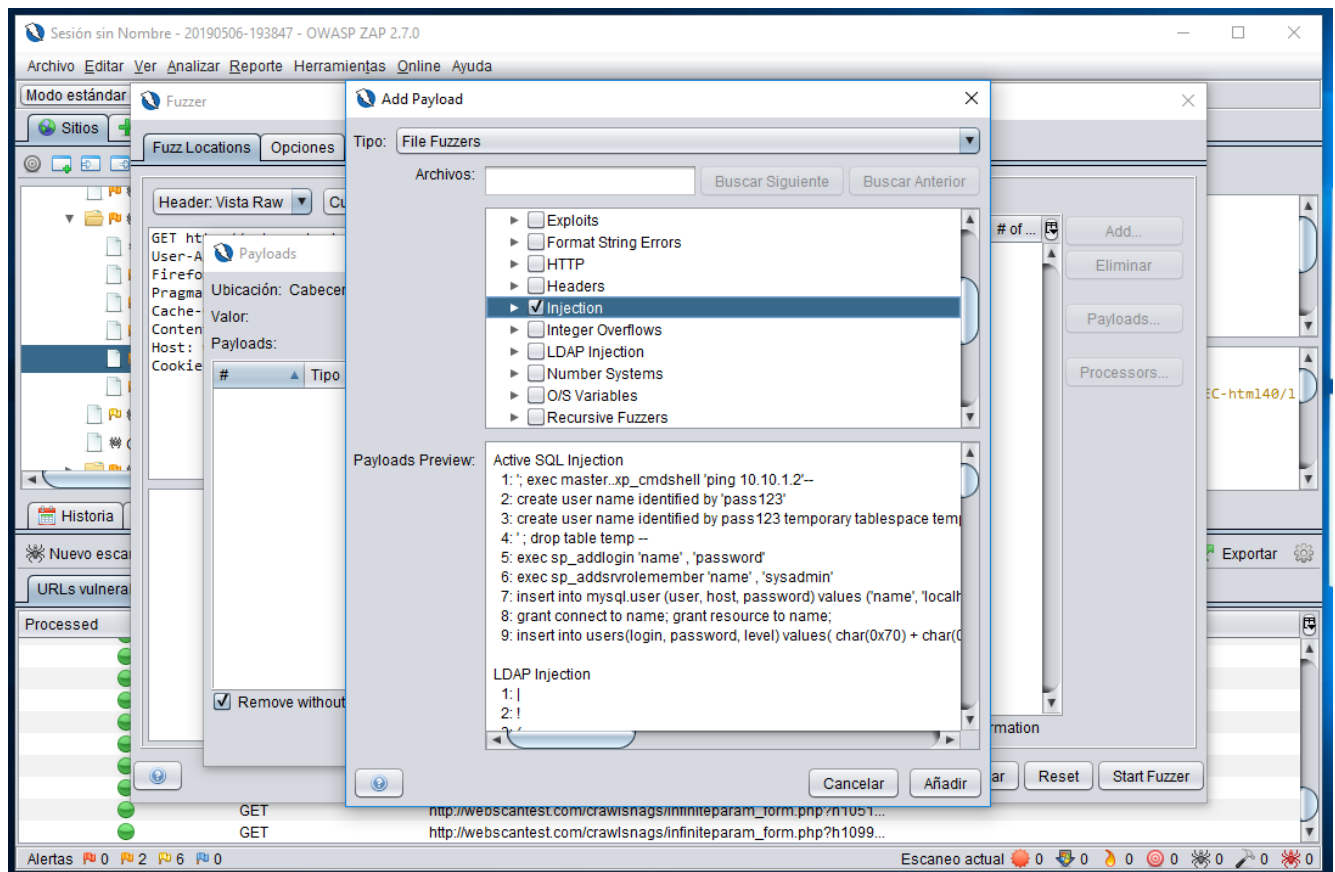
ZAP web crawling ^[8]

ZAP cuenta con funcionalidades de web crawling, esto nos permite identificar los enlaces que están presentes en un sitio web, con esto conseguimos analizar cómo se compone nuestro sitio web y desentrañar cómo se estructuran tanto los directorios como posibles archivos existentes en los cuales podemos centrar nuestra auditoría, el web crawler de ZAP funciona de forma recursiva, eso quiere decir que cada vez que encuentra un nuevo enlace lo va siguiendo, identificando los elementos; existe la posibilidad de una mayor granularidad que puede ser definida en la ventana de configuración; de esta forma iremos afinando aún más nuestra búsqueda y otorgándonos datos de mayor relevancia para nuestro análisis. Si buscamos un análisis general del sitio solo tenemos que realizar un escaneo pasivo y dirigirnos a la pestaña de sitios -> clic derecho -> Spider URL. Para una mayor precisión se recomienda usar el resto de las funciones Spider.

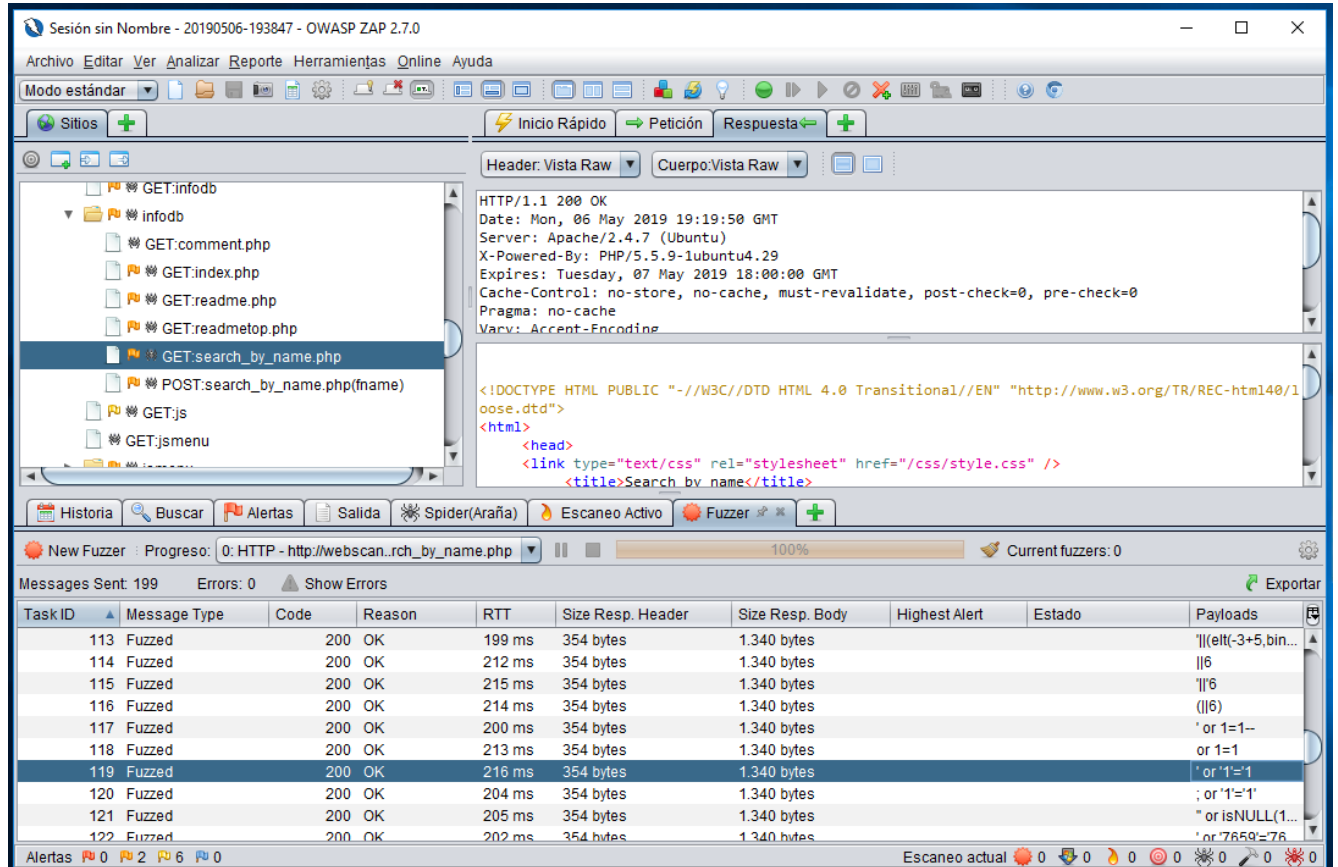


Fuzzing ^[9]

El fuzzing son las diferentes técnicas que permiten generar y enviar datos aleatorios y secuenciales a una aplicación con el fin de conocer sus vulnerabilidades ^[10], estas técnicas previenen a nuestras aplicaciones por ejemplo de ser susceptibles a ataques de inyección SQL al permitirnos comprobar con anterioridad al despliegue si es nuestro software vulnerable a este tipo de ataques. Vamos a realizar un ataque de inyección SQL contra el sitio "<http://webscantest.com>". Después de realizar un ataque con la herramienta de web crawling antes descrita procedemos a analizar los posibles puntos débiles de la aplicación. Si nos fijamos en el árbol post análisis del sitio veremos en la carpeta "infodb" un método GET con el nombre "search by name". Ahora pasaremos al ataque con las funciones de fuzzing para realizar una inyección SQL. Para ello realizamos clic derecho -> atacar fuzz -> Add ... -> File Fuzzers -> jbrofuzz -> injection.



Una vez configurado el fuzz simplemente seleccionamos la opción Start fuzz de la primera ventana de fuzzing.



Sesión sin Nombre - 20190506-193847 - OWASP ZAP 2.7.0

Archivo Editar Ver Analizar Reporte Herramientas Online Ayuda

Modo estándar

Sitios

Inicio Rápido Petición Respuesta

Header: Vista Raw Cuerpo: Vista Raw

GET:infodb

infodb

GET:comment.php

GET:index.php

GET:readme.php

GET:readmetop.php

GET:search_by_name.php

POST:search_by_name.php(fname)

GET:js

GET:jsmenu

HTTP/1.1 200 OK

Date: Mon, 06 May 2019 19:19:50 GMT

Server: Apache/2.4.7 (Ubuntu)

X-Powered-By: PHP/5.5.9-1ubuntu4.29

Expires: Tuesday, 07 May 2019 18:00:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Vary: Accept-Encoding

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">

<html>

<head>

<link type="text/css" rel="stylesheet" href="/css/style.css" />

<title>Search by name</title>

Historia Buscar Alertas Salida Spider(Araña) Escaneo Activo Fuzzer

New Fuzzer Progreso: 0: HTTP - http://webscan.rch_by_name.php 100% Current fuzzers: 0

Messages Sent: 199 Errors: 0 Show Errors Exportar

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Estado	Payloads
113	Fuzzed	200	OK	199 ms	354 bytes	1.340 bytes			(elt(-3+5,bin...
114	Fuzzed	200	OK	212 ms	354 bytes	1.340 bytes			6
115	Fuzzed	200	OK	215 ms	354 bytes	1.340 bytes			6
116	Fuzzed	200	OK	214 ms	354 bytes	1.340 bytes			6
117	Fuzzed	200	OK	200 ms	354 bytes	1.340 bytes			' or 1=1--
118	Fuzzed	200	OK	213 ms	354 bytes	1.340 bytes			or 1=1
119	Fuzzed	200	OK	216 ms	354 bytes	1.340 bytes			' or '1'='1
120	Fuzzed	200	OK	204 ms	354 bytes	1.340 bytes			, or '1'='1
121	Fuzzed	200	OK	205 ms	354 bytes	1.340 bytes			" or isNULL(1...
122	Fuzzed	200	OK	202 ms	354 bytes	1.340 bytes			' or 7659=76

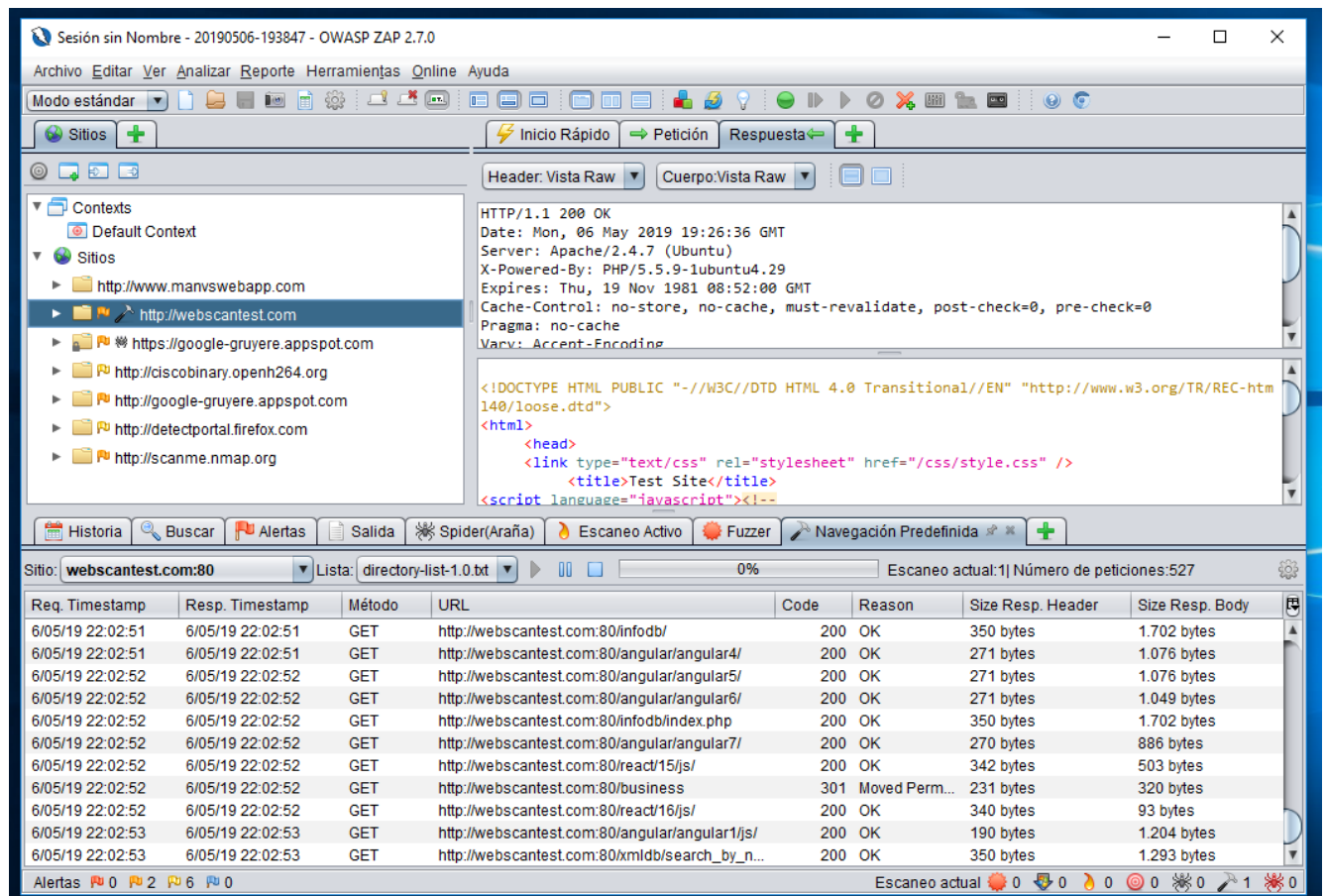
Alertas 0 0 2 6 0 Escaneo actual 0 0 0 0 0 0 0 0 0 0

Comprobamos que en este caso nos retorna un código OK la sentencia SQL que nos mostraría el contenido completo de nuestra base de datos. Comprobamos que el ZAP está en lo correcto dirigiéndonos al sitio con nuestro navegador e introduciendo manualmente la cadena maliciosa.

Forced Browse ^[11]

Entendemos por forced browsing por el ataque que se centra en enumerar los accesos a recursos que no son referenciados por una aplicación ^[12], es decir, elementos que no son accesibles desde el uso normal de una web por un usuario, pero que conociendo la URL pueden ser accedidos con una intencionalidad maliciosa, es por ello por lo que es muy importante mantener la estructura de directorios limpia para evitar este tipo de ataques.

ZAP nos permite realizar este tipo de ataques, simplemente una vez visitado el sitio, clic derecho -> Atacar ... -> Sitio de navegación predefinida. Cuando termine deberíamos obtener algo similar a esto.



Header: Vista Raw

Cuerpo: Vista Raw

```
HTTP/1.1 200 OK
Date: Mon, 06 May 2019 19:26:36 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accent-Encoding

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">
<html>
<head>
<link type="text/css" rel="stylesheet" href="/css/style.css" />
<title>Test Site</title>
<script language="javascript"><!--
```

Historia | Buscar | Alertas | Salida | Spider (Araña) | Escaneo Activo | Fuzzer | Navegación Predefinida

Sitio: webscantest.com:80 | Lista: directory-list-1.0.bt | 0% | Escaneo actual: 1 | Número de peticiones: 527

Req. Timestamp	Resp. Timestamp	Método	URL	Code	Reason	Size Resp. Header	Size Resp. Body
6/05/19 22:02:51	6/05/19 22:02:51	GET	http://webscantest.com:80/infodb/	200	OK	350 bytes	1.702 bytes
6/05/19 22:02:51	6/05/19 22:02:51	GET	http://webscantest.com:80/angular/angular4/	200	OK	271 bytes	1.076 bytes
6/05/19 22:02:52	6/05/19 22:02:52	GET	http://webscantest.com:80/angular/angular5/	200	OK	271 bytes	1.076 bytes
6/05/19 22:02:52	6/05/19 22:02:52	GET	http://webscantest.com:80/angular/angular6/	200	OK	271 bytes	1.049 bytes
6/05/19 22:02:52	6/05/19 22:02:52	GET	http://webscantest.com:80/infodb/index.php	200	OK	350 bytes	1.702 bytes
6/05/19 22:02:52	6/05/19 22:02:52	GET	http://webscantest.com:80/angular/angular7/	200	OK	270 bytes	886 bytes
6/05/19 22:02:52	6/05/19 22:02:52	GET	http://webscantest.com:80/react/15/js/	200	OK	342 bytes	503 bytes
6/05/19 22:02:52	6/05/19 22:02:52	GET	http://webscantest.com:80/business	301	Moved Perm...	231 bytes	320 bytes
6/05/19 22:02:52	6/05/19 22:02:52	GET	http://webscantest.com:80/react/16/js/	200	OK	340 bytes	93 bytes
6/05/19 22:02:53	6/05/19 22:02:53	GET	http://webscantest.com:80/angular/angular11/js/	200	OK	190 bytes	1.204 bytes
6/05/19 22:02:53	6/05/19 22:02:53	GET	http://webscantest.com:80/xmldb/search_by_n...	200	OK	350 bytes	1.293 bytes

Alertas 0 0 2 6 0 0 | Escaneo actual 0 0 0 0 0 0 1 0

Es posible realizar un ataque más granular con las funciones que nos otorga la propia herramienta si queremos por ejemplo conocer qué esconde un directorio concreto.

3. Conclusión

Podemos concluir que esta aplicación es fundamental en la “caja de herramientas” de todo pentester, sus funcionalidades descritas en los apéndices anteriores son muy variadas y versátiles, además cuenta con un elevado nivel de personalización que permiten al usuario, no solo analizar los datos obtenidos, sino que además permite realizar ataques y exploraciones de forma precisa y rápida; ofrece una variedad de opciones por defecto que cumplirán los requisitos mínimos que podamos requerir y debido a su buen diseño, esta

herramienta puede ser mejorada gracias a addons realizados por la comunidad, los cuales permiten expandir las posibilidades de la herramienta aumentando su versatilidad.

4. Referencias

1. https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
2. https://es.wikipedia.org/wiki/OWASP_ZAP
3. <https://www.sniferl4bs.com/2015/07/owasp-zaproxy-i-introduccion-zaproxy.html>
4. <https://blog.segu-info.com.ar/2015/09/tutorial-de-uso-owasp-zaproxy.html>
5. <https://www.sniferl4bs.com/2015/07/owasp-zaproxy-ii-intercept-proxy.html>
6. <http://google-gruyere.appspot.com/>
7. <https://www.sniferl4bs.com/2015/08/owasp-zaproxy-iii-escaneos-pasivo-y.html>
8. <https://www.sniferl4bs.com/2015/08/owasp-zaproxy-iv-zap-web-crawling.html>
9. <https://www.sniferl4bs.com/2015/08/owasp-zaproxy-v-fuzzing-con-zap.html>
10. <https://blog.segu-info.com.ar/2007/08/qu-es-fuzzing.html>
11. <https://www.sniferl4bs.com/2015/09/owasp-zaproxy-vi-zap-forced-browse.html>
12. https://www.owasp.org/index.php/Forced_browsing