

Tutorial - Demo 3 - Uso de OWASP para análisis de un sitio o aplicación web

Se considera **pre-requisito** contar con la imagen de Docker correspondiente, sea a partir de la copia realizada en clase o mediante una descargada desde Docker Hub¹.

Pasos a seguir para realizar un análisis con la herramienta:

1. Iniciar la ejecución del contenedor:
 - a. Si fuera con la imagen distribuida en clase, ejecutar (es una única línea):

```
docker run -u zap -p 8080:8080 -p 8090:8090 -i <<IP-REPOSITORIO>>:5000/demo3owasp zap-webswing.sh
```

- b. Si fuera con la imagen de Docker Hub, ejecutar (es una única línea):

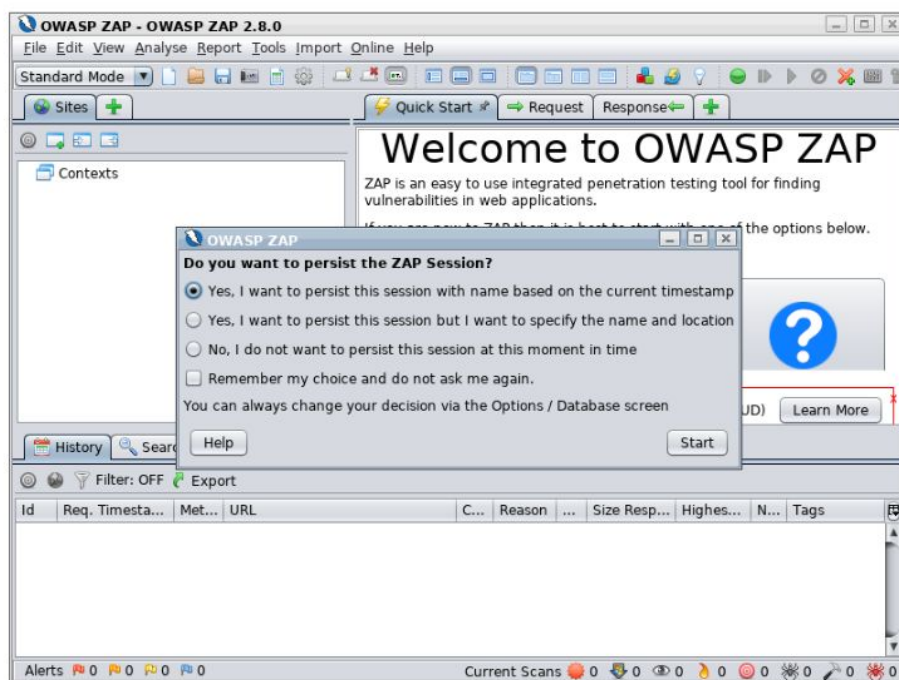
```
docker run -u zap -p 8080:8080 -p 8090:8090 -i owasp/zap2docker-stable zap-webswing.sh
```

2. En el navegador web acceder a la siguiente dirección <http://localhost:8080/zap>, se verá una pantalla de carga como la siguiente:

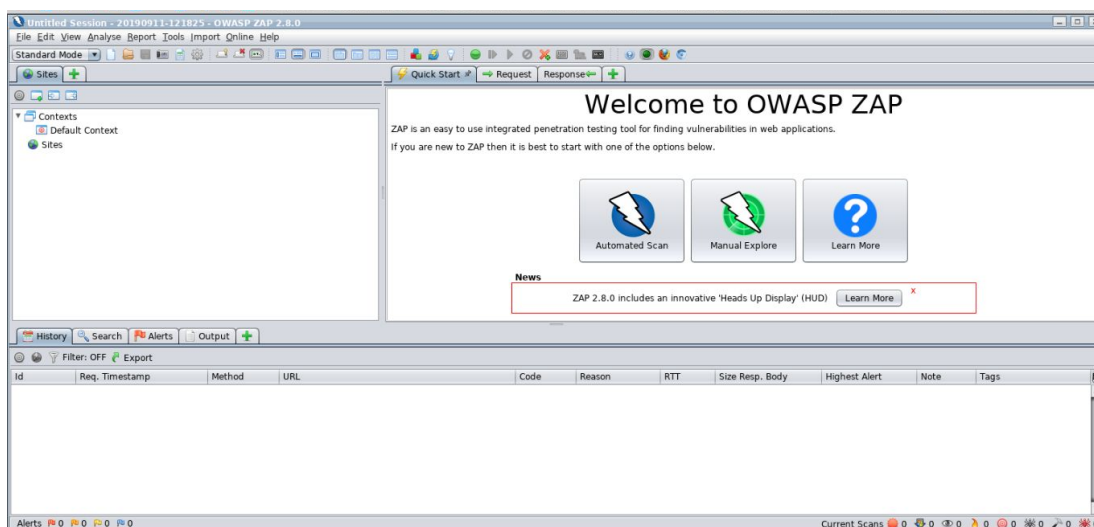


¹ Si este fuera el caso se deberá **ejecutar**: `docker pull owasp/zap2docker-stable`

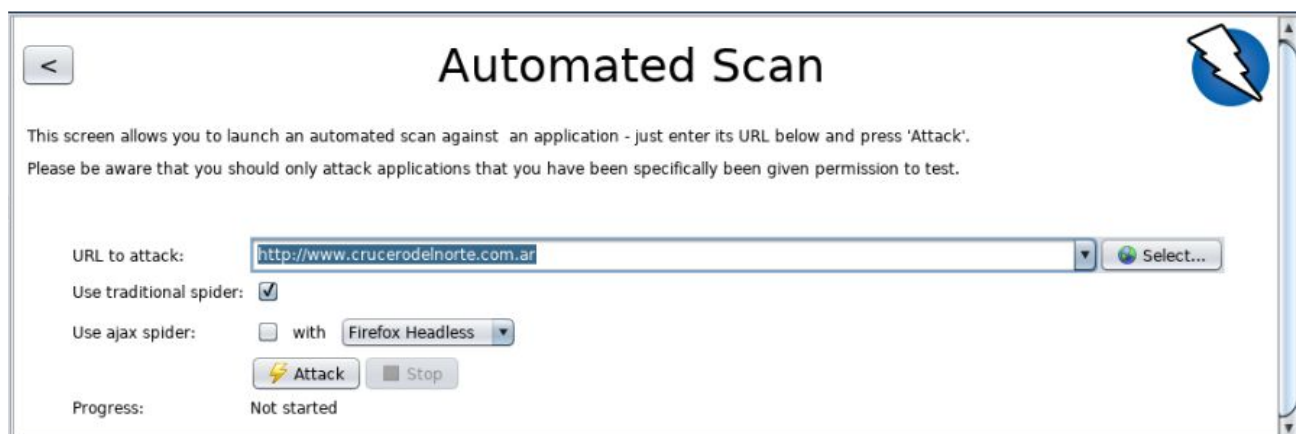
- Una vez que inicia la herramienta se solicitará definir el método de almacenamiento de la sesión actual, se selecciona una opción y se hace clic en **Start**.



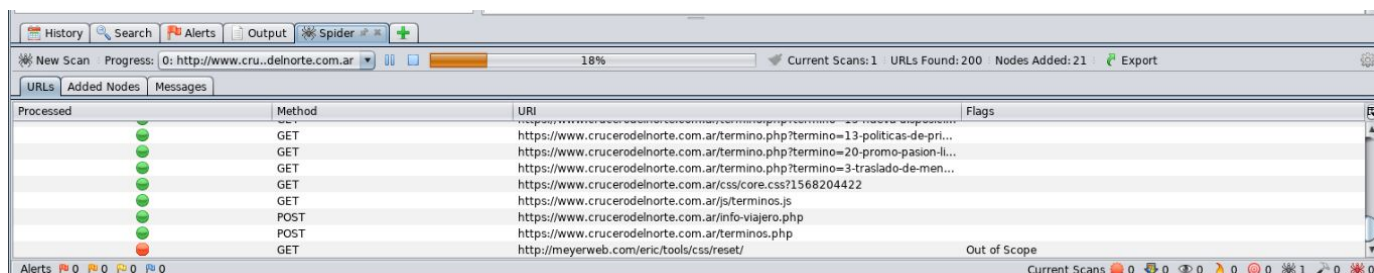
- En este punto la herramienta se habrá iniciado completamente y estará en condiciones de comenzar con la ejecución de un análisis.



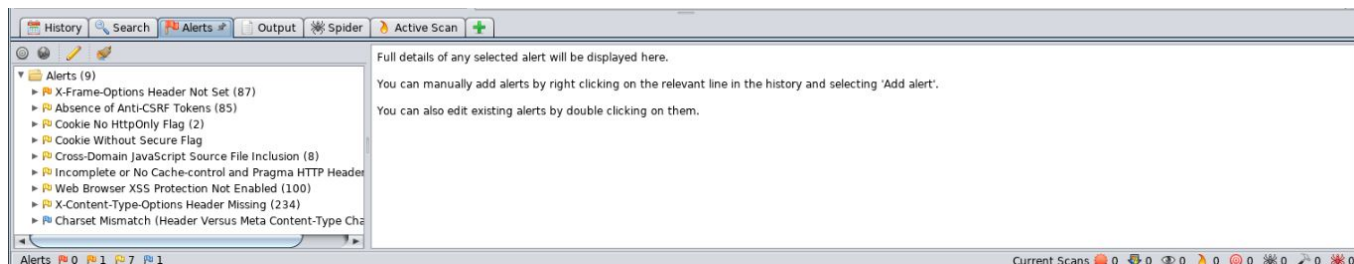
5. Haciendo clic en la opción “**Automated Scan**” se podrá ingresar la URL del objetivo de análisis y se iniciará con el botón “**Attack**”. En este caso se realizará el análisis sobre <http://www.cruceroelnorte.com.ar/>.



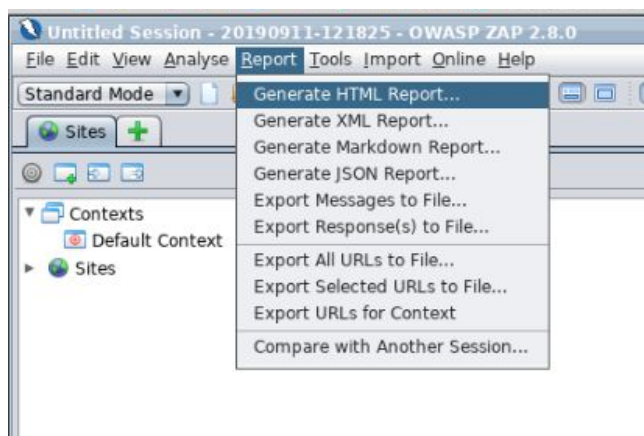
6. Mientras que el análisis se encuentra en ejecución se podrá seguir su avance desde la consola inferior.




7. Una vez que se completan todos los pasos del análisis se puede obtener el reporte de resultados desde la pestaña “**Alerts**” de la sección inferior de la pantalla.



8. El conjunto de resultados obtenidos se puede exportar en diferentes formatos desde el menú “**Reports**”, en este caso se utilizará la opción “**Generate HTML Report...**” para poder visualizarlo posteriormente en un navegador web.



9. Este archivo generado será abierto a continuación en el navegador para su lectura.



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	11
Informational	1

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://www.cruceroelnorte.com.ar/mods/cliente/login.php
Method	GET
Parameter	X-Frame-Options
URL	https://www.cruceroelnorte.com.ar/termino.php?termino=4-equipaje
Method	GET
Parameter	X-Frame-Options
URL	https://www.cruceroelnorte.com.ar/boleterias.php
Method	POST
Parameter	X-Frame-Options
URL	https://www.cruceroelnorte.com.ar/info-viajero.php
Method	POST
Parameter	X-Frame-Options

10. En este ejemplo se pueden llegar a destacar algunos de los siguientes aspectos:

- Por ejemplo, se puede observar que la falta de opciones de configuración del sitio podrían permitir ataques de tipo “ClickJacking”. Si se estuviera ejecutando una auditoría de la seguridad o calidad del producto analizado, aún cuando no se trata de un problema de alta gravedad según la herramienta se podría presentar como hallazgo por

X-Frame-Options Header Not Set	
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.	
https://www.cruceodelnorte.com.ar/mods/cliente/login.php	
GET	
X-Frame-Options	
https://www.cruceodelnorte.com.ar/termino.php?termino=4-equipaje	
GET	
X-Frame-Options	
https://www.cruceodelnorte.com.ar/boleterias.php	
POST	
X-Frame-Options	

- Otro caso podría ser el que se observa a continuación donde se informa que la protección contra ataques de tipo XSS (*cross-site scripting*) no se encuentra habilitada, lo que podría dar lugar a vulnerabilidades del lado del usuario.

Web Browser XSS Protection Not Enabled	
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server	
https://www.cruceodelnorte.com.ar/terminos.php	
GET	
X-XSS-Protection	
https://www.cruceodelnorte.com.ar/ventas/mods/cliente/login.php?err=104	
GET	
X-XSS-Protection	
https://www.cruceodelnorte.com.ar/boleterias.php	

Con esta estrategia se podrán analizar diferentes aspectos de la seguridad / integridad