



UNIVERSIDAD DE TALCA
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Seguridad Informática

Laboratorio 6

Erik Regla
eregla09@alumnos.otalca.cl

12 de julio de 2020

Índice

1. Actividades	3
1.1. Actividad 1 - NMAP	3
1.2. Actividad 2 - OWASP ZAP	4
1.3. Actividad 3 - NIKTO	7
1.4. Actividad 3 - SQLMAP	10
2. Conclusiones	11

1. Actividades

Elegimos como objetivo disponible en la web la pagina principal de la universidad por motivos legales y de pruebas. Además que ya conocemos algo de información al respecto y estas herramientas no necesariamente pueden encontrar información de otras vulnerabilidades ya conocidas por la forma en la que está hecha la aplicación en si.

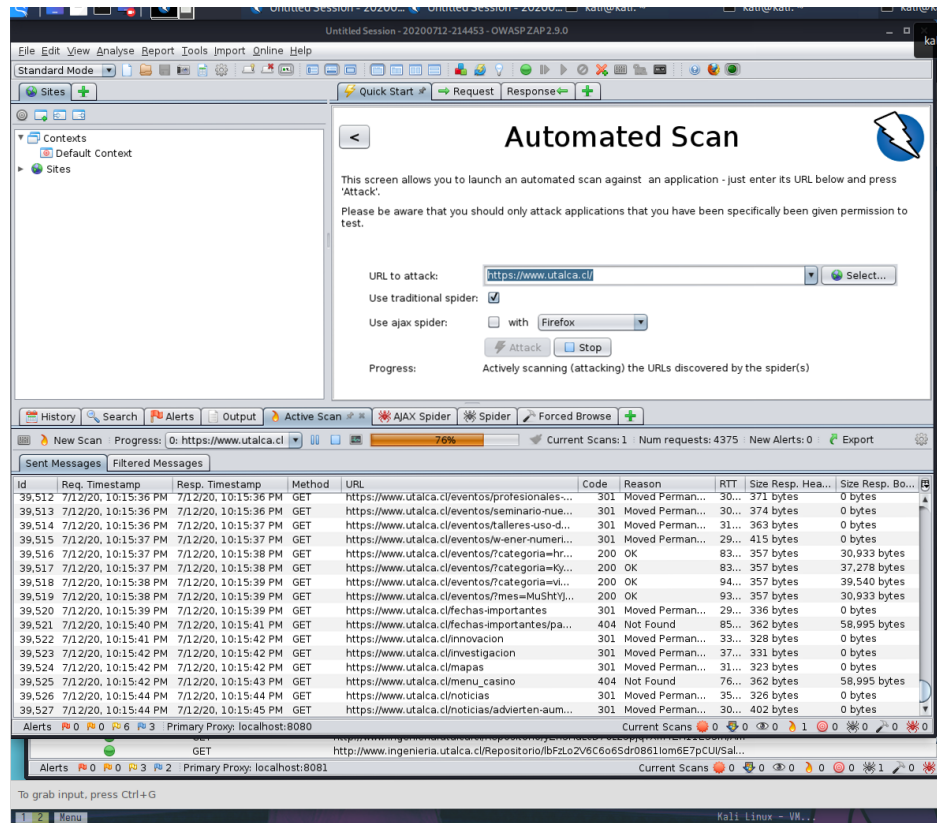
1.1. Actividad 1 - NMAP

```
kali@kali:~$ nmap -sV --version-intensity 5 www.usalca.cl
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 22:29 -04
Nmap scan report for www.usalca.cl (134.209.223.104)
Host is up (0.14s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         nginx 1.15.8
443/tcp   open  ssl/http     nginx 1.15.8
8080/tcp   closed http-proxy
9000/tcp   open  cslistener?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9000-TCP:V=7.80%I=5%D=7/12%Time=5F0BC78A%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,1630,"HTTP/1.1\x20200\x20\r\nX-Frame-Options:\x20SAMEORIGIN\r
SF:\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20n
SF:osniff\r\nCache-Control:\x20no-cache,\x20no-store,\x20must-revalidate\r
SF:\nvary:\x20accept-encoding\r\nContent-Type:\x20text/html;charset=utf-8\
SF:r\nDate:\x20Mon,\x2013\x20Jul\x202020\x2002:31:38\x20GMT\r\nConnection:
```

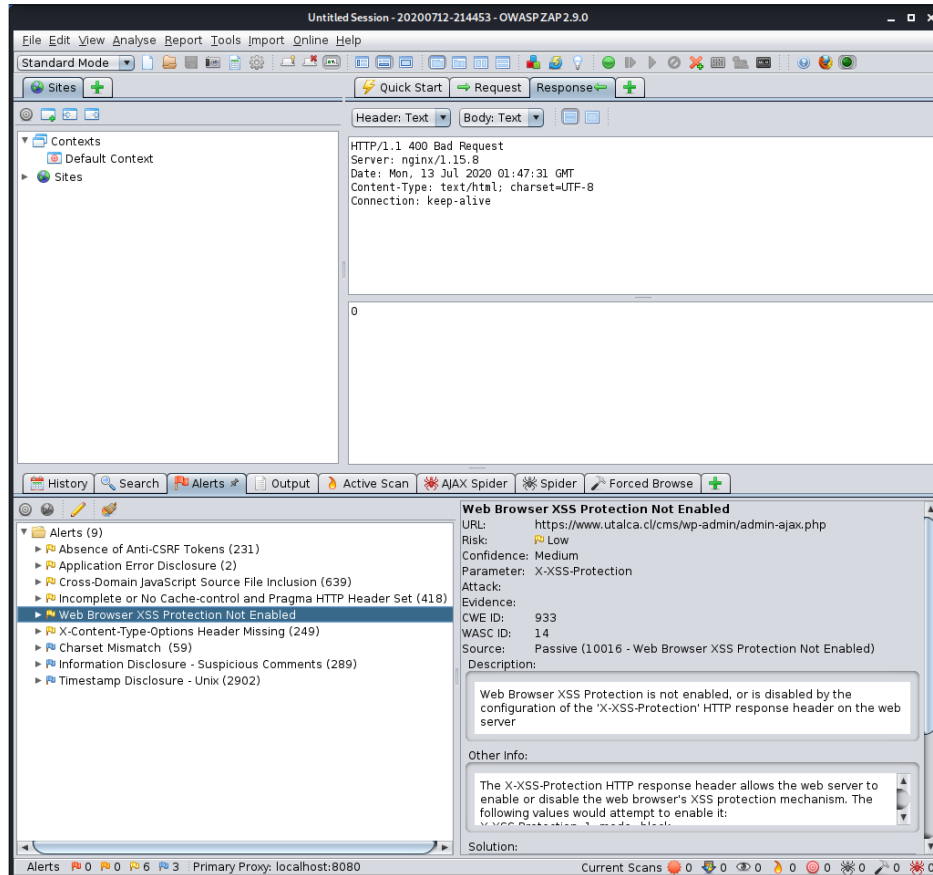
El primer análisis entregado por NMAP no es muy alentador. A diferencia de ocasiones anteriores, en este caso al parecer solo están abiertos los puertos para el consumo de tráfico web y un openssh que está protegido con un acceso solo por llave privada (bien jugado, aprendieron).

Adicionalmente hay un puerto abierto, el 9000 que típicamente en estos casos queda abierto para ser utilizado por sentry, lo cual no debería de ser tan sorprendente.

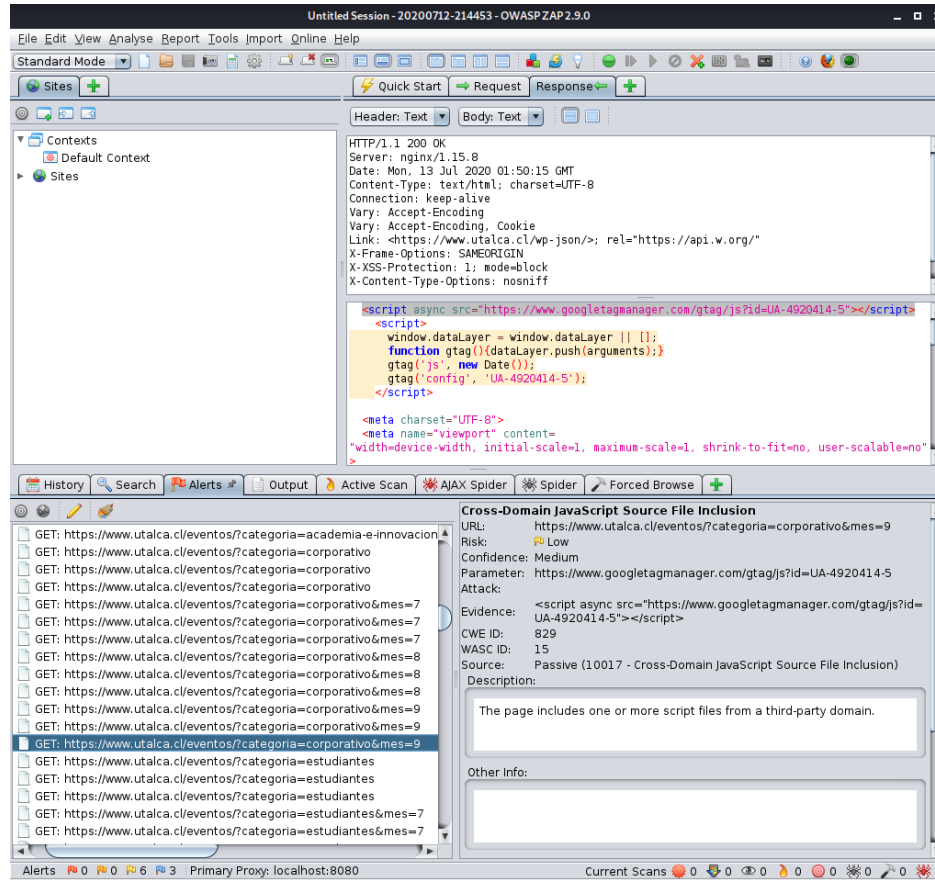
1.2. Actividad 2 - OWASP ZAP



Inicio de la ejecución de OWASP ZAP. Utilizamos los parámetros por defecto el cual ejecuta una búsqueda estandar. No hay necesidad de probar otras arañas ya que la diferencia por headers es nula. Durante esta ejecución es posible apreciar dos procesos principales. La araña que se encarga de buscar la información del sitio y realizar un mapa de este y la ejecución activa de los ataques -aka probing-.



Podemos ver una vez terminada la ejecución de ZAP que no se encuentran mayores vulnerabilidades, aunque llama la atención el número de alertas que son lanzadas por la herramienta en sí.

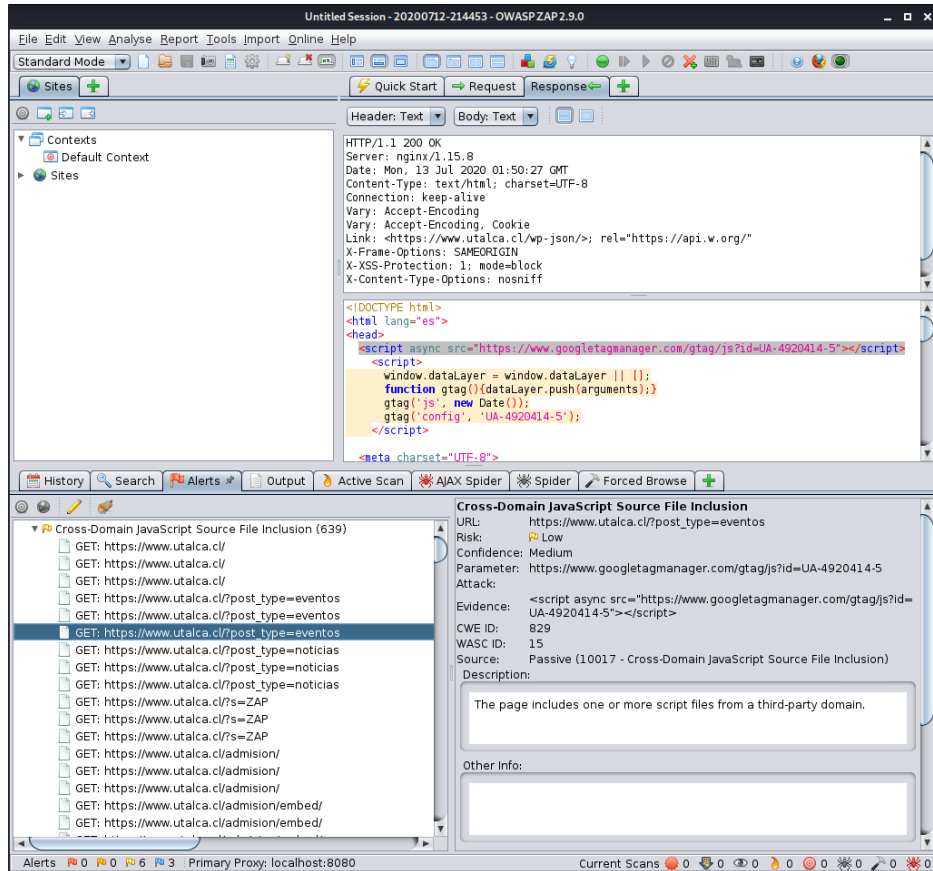


En si, la ejecución de ZAP como muchas herramientas automatizadas para la búsqueda de vulnerabilidades es muy propensa a encontrar falsos positivos. Por ejemplo, tomemos este caso de supuesta ejecución remota.

Podemos apreciar que se incluye un archivo desde google tag manager, por lo que si, es un problema el estar incluyendo archivos de una fuente de terceros. Sin embargo, el objetivo de este laboratorio es encontrar vulnerabilidades dentro de la aplicación en si y esta solo afecta al cliente, por ejemplo, cuando este dominio está pasando por un ataque MITM entonces el cliente puede ser afectado al cargar un script diferente.

Sin embargo, no es un problema propio de la aplicación. De todas maneras, esta información es valiosa al momento de realizar un assesment, ya que nos sugiere que un buen vector de ataque lateral son usuarios que acceden al sitio y posean credenciales y con los que podamos tener contacto dentro de la misma red.

La existencia de estas URL con parámetros nos sugiere un buen punto de partida para probar inyecciones SQL.



Sin embargo, al revisar mas en profundidad las alertas entregadas, además de confirmar los falsos positivos, encontramos que en realidad la razón de la gran cantidad de estos es porque derechamente hay una cantidad enorme de malas prácticas de programación involucradas en el desarrollo del sitio (sin contar que es un wordpress).

1.3. Actividad 3 - NIKTO

Para este caso utilizamos el siguiente comando para almacenar la información dentro de un archivo: `nikto -Display V -o results.html -Format htm -h https://www.ortalca.cl`.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ nikto -Display V -o results_atalca.html -Format htm -h https://www.atalca.cl  
- Nikto v2.1.6  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_parked  
V:Sun Jul 12 23:03:33 2020 - Loaded "Parked Detection" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_clientaccesspolicy  
V:Sun Jul 12 23:03:33 2020 - Loaded "clientaccesspolicy.xml" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_sitefiles  
V:Sun Jul 12 23:03:33 2020 - Loaded "Site Files" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_core  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_paths  
V:Sun Jul 12 23:03:33 2020 - Loaded "Path Search" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_put_del_test  
V:Sun Jul 12 23:03:33 2020 - Loaded "Put/Delete test" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_apache_expect_xss  
V:Sun Jul 12 23:03:33 2020 - Loaded "Apache Expect XSS" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_report_html  
V:Sun Jul 12 23:03:33 2020 - Loaded "Report as HTML" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_headers  
V:Sun Jul 12 23:03:33 2020 - Loaded "HTTP Headers" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_cookies  
V:Sun Jul 12 23:03:33 2020 - Loaded "HTTP Cookie Internal IP" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_dir_traversal  
V:Sun Jul 12 23:03:33 2020 - Loaded "Directory Traversal" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_report_text  
V:Sun Jul 12 23:03:33 2020 - Loaded "Text reports" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_report_sqlg  
V:Sun Jul 12 23:03:33 2020 - Loaded "Generic SQL reports" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_drupal  
V:Sun Jul 12 23:03:33 2020 - Loaded "Drupal Specific Tests" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_cgi  
V:Sun Jul 12 23:03:33 2020 - Loaded "CGI" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_robots  
V:Sun Jul 12 23:03:33 2020 - Loaded "Robots" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_content_search  
V:Sun Jul 12 23:03:33 2020 - Loaded "Content Search" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_ms10_070  
V:Sun Jul 12 23:03:33 2020 - Loaded "ms10-070 Check" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_ssl  
V:Sun Jul 12 23:03:33 2020 - Loaded "SSL and cert checks" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_origin_reflection  
V:Sun Jul 12 23:03:33 2020 - Loaded "CORS Origin Reflection" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_shellshock  
V:Sun Jul 12 23:03:33 2020 - Loaded "shellshock" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_tests  
V:Sun Jul 12 23:03:33 2020 - Loaded "Nikto Tests" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_fileops  
V:Sun Jul 12 23:03:33 2020 - Loaded "File Operations" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_docker_registry  
V:Sun Jul 12 23:03:33 2020 - Loaded "docker_registry" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_strutshock  
V:Sun Jul 12 23:03:33 2020 - Loaded "strutshock" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_dishwasher  
V:Sun Jul 12 23:03:33 2020 - Loaded "dishwasher" plugin.  
V:Sun Jul 12 23:03:33 2020 - Initialising plugin nikto_dictionary_attack
```

Sin embargo nos topamos con un problema fundamental, sin embargo que nos impide utilizar esta herramienta por completo. Al parecer el servidor tiene tiempos de respuesta relativamente altos para las consultas, no a su vez con la resolución de recursos estáticos.


```
kali@kali: ~  
File Actions Edit View Help  
V:Sun Jul 12 23:03:33 2020 - Opening report for "Report as HTML" plugin  
V:Sun Jul 12 23:03:33 2020 - Checking for HTTPS on port www.ortalca.cl:443, using GET  
V:Sun Jul 12 23:03:34 2020 - 200 for GET: /  
V:Sun Jul 12 23:03:35 2020 - 6897 server checks loaded  
V:Sun Jul 12 23:03:35 2020 - Running start for "HTTP Headers" plugin  
V:Sun Jul 12 23:03:35 2020 - Running start for "Directory Traversal" plugin  
V:Sun Jul 12 23:03:35 2020 - Running start for "Drupal Specific Tests" plugin  
V:Sun Jul 12 23:03:35 2020 - Running start for "IBM/Lotus Domino Specific Tests" plugin  
V:Sun Jul 12 23:03:35 2020 - Running start for "Favicon" plugin  
V:Sun Jul 12 23:03:35 2020 - Running start for "Content Search" plugin  
V:Sun Jul 12 23:03:35 2020 - Running start for "Guess authentication" plugin  
V:Sun Jul 12 23:03:36 2020 - 200 for GET: /  
+ Target IP: 134.209.223.104  
+ Target Hostname: www.ortalca.cl  
+ Target Port: 443  
  
+ SSL Info: Subject: /CN=www.ortalca.cl  
Ciphers: ECDHE-RSA-AES256-GCM-SHA384  
Issuer: /C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3  
+ Start Time: 2020-07-12 23:03:35 (GMT-4)  
  
+ Server: nginx/1.15.8  
V:Sun Jul 12 23:03:37 2020 - 200 for GET: /  
+ The site uses SSL and the Strict-Transport-Security header is not defined.  
+ The site uses SSL and Expect-CT header is not present.  
V:Sun Jul 12 23:03:37 2020 - Testing error for file: /TVhv4NIy.cp-1251  
V:Sun Jul 12 23:03:38 2020 - 404 for GET: /TVhv4NIy.cp-1251  
+ Uncommon header 'link' found, with contents: <https://www.ortalca.cl/wp-json/>; rel="https://a  
pi.w.org/"  
V:Sun Jul 12 23:03:38 2020 - Testing error for file: /TVhv4NIy.py  
V:Sun Jul 12 23:03:40 2020 - 404 for GET: /TVhv4NIy.py  
V:Sun Jul 12 23:03:40 2020 - Testing error for file: /TVhv4NIy.csp  
V:Sun Jul 12 23:03:41 2020 - 404 for GET: /TVhv4NIy.csp  
V:Sun Jul 12 23:03:41 2020 - Testing error for file: /TVhv4NIy.jsp+  
V:Sun Jul 12 23:03:43 2020 - 404 for GET: /TVhv4NIy.jsp+  
V:Sun Jul 12 23:03:43 2020 - Testing error for file: /TVhv4NIy.access  
V:Sun Jul 12 23:03:44 2020 - 404 for GET: /TVhv4NIy.access  
V:Sun Jul 12 23:03:44 2020 - Testing error for file: /TVhv4NIy.ca  
V:Sun Jul 12 23:03:45 2020 - 404 for GET: /TVhv4NIy.ca  
V:Sun Jul 12 23:03:45 2020 - Testing error for file: /TVhv4NIy.asa  
V:Sun Jul 12 23:03:47 2020 - 404 for GET: /TVhv4NIy.asa  
V:Sun Jul 12 23:03:47 2020 - Testing error for file: /TVhv4NIy.axd  
V:Sun Jul 12 23:03:48 2020 - 404 for GET: /TVhv4NIy.axd  
V:Sun Jul 12 23:03:48 2020 - Testing error for file: /TVhv4NIy.zip  
V:Sun Jul 12 23:03:49 2020 - 404 for GET: /TVhv4NIy.zip  
V:Sun Jul 12 23:03:49 2020 - Testing error for file: /TVhv4NIy.db  
V:Sun Jul 12 23:03:51 2020 - 404 for GET: /TVhv4NIy.db  
V:Sun Jul 12 23:03:51 2020 - Testing error for file: /TVhv4NIy.pw  
V:Sun Jul 12 23:03:52 2020 - 404 for GET: /TVhv4NIy.pw  
V:Sun Jul 12 23:03:52 2020 - Testing error for file: /TVhv4NIy.SHOW  
V:Sun Jul 12 23:03:53 2020 - 404 for GET: /TVhv4NIy.SHOW  
V:Sun Jul 12 23:03:53 2020 - Testing error for file: /TVhv4NIy.htaccess-  
V:Sun Jul 12 23:03:55 2020 - 404 for GET: /TVhv4NIy.htaccess-  
V:Sun Jul 12 23:03:55 2020 - Testing error for file: /TVhv4NIy.gz
```

Debido a que NIKTO prueba los ataques de manera secuencial, al momento de ejecutar un ataque para poder revisar los archivos disponibles, tenemos un retraso de aproximadamente 500ms a 1600ms. Hay dos hipótesis al respecto, la primera es que toda esta plataforma está bajo un tarpit, la segunda es que el servidor está bajo mucho estrés o bien está mal configurado. Históricamente se ha probado que es mas probable que sea la segunda opción, sin embargo, este problema nos impide resolver el comando dentro de un tiempo relativamente razonable”.

```
kali@kali: ~  
File Actions Edit View Help  
V:Sun Jul 12 22:16:40 2020 - for GET:  
V:Sun Jul 12 22:17:00 2020 - for GET:  
V:Sun Jul 12 22:17:20 2020 - for GET:  
  
V:Sun Jul 12 22:17:40 2020 - for GET:  
V:Sun Jul 12 22:18:00 2020 - for GET:  
V:Sun Jul 12 22:18:20 2020 - for GET:  
V:Sun Jul 12 22:18:40 2020 - for GET:  
V:Sun Jul 12 22:19:00 2020 - for GET:  
V:Sun Jul 12 22:19:20 2020 - for GET:  
V:Sun Jul 12 22:19:41 2020 - for GET:  
V:Sun Jul 12 22:20:01 2020 - for GET:  
V:Sun Jul 12 22:20:21 2020 - for GET:  
V:Sun Jul 12 22:20:41 2020 - for GET:  
V:Sun Jul 12 22:21:01 2020 - for GET:  
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response  
V:Sun Jul 12 22:21:21 2020 - for GET:  
+ Scan terminated: 20 error(s) and 1 item(s) reported on remote host  
+ End Time: 2020-07-12 22:21:21 (GMT-4) (472 seconds)  
  
+ 1 host(s) tested  
V:Sun Jul 12 22:21:21 2020 + 767 requests made in 477 seconds  
kali@kali:~$  
kali@kali:~$  
kali@kali:~$
```

Ahora el problema de esto no es que sea lento el análisis (nikto por naturaleza es lento), si no que el análisis en vez de tomar horas, pasa a tomar días solo por el efecto del tarpit. Incluso paralelizando los análisis, no se obtienen resultados concluyentes ya que no alcanza a realizar todo el trabajo en un tiempo relativamente razonable (digamos, unas 5 horas).

1.4. Actividad 3 - SQLMAP

Para efectos de simpleza solo se muestra una ejecución.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sqlmap -u 'https://www.ugalca.cl/eventos/?categoria=corporativo&mes=9'  
  
[H]  
[+] {1.4.7#stable}  
[+] http://sqlmap.org  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
  
[*] starting @ 22:23:24 /2020-07-12/  
  
[22:23:24] [INFO] testing connection to the target URL  
[22:23:25] [INFO] checking if the target is protected by some kind of WAF/IPS  
[22:23:26] [INFO] testing if the target URL content is stable  
[22:23:26] [INFO] target URL content is stable  
[22:23:26] [INFO] testing if GET parameter 'categoria' is dynamic  
[22:23:27] [WARNING] GET parameter 'categoria' does not appear to be dynamic  
[22:23:28] [WARNING] heuristic (basic) test shows that GET parameter 'categoria' might not be injectable
```

Utilizando la url descubierta en el paso anterior (en realidad se probó con un conjunto de estas), procedemos a ejecutar SQLMAP sobre la dirección. Dado que no estamos necesariamente trabajando con scripts de inyección específicos, no utilizamos mayores argumentos.

```
kali@kali: ~  
File Actions Edit View Help  
[22:23:27] [WARNING] GET parameter 'categoria' does not appear to be dynamic  
[22:23:28] [WARNING] heuristic (basic) test shows that GET parameter 'categoria' might not be injectable  
[22:23:29] [INFO] testing for SQL injection on GET parameter 'categoria'  
[22:23:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[22:23:43] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'  
[22:23:45] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[22:23:49] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'  
[22:23:54] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
[22:23:58] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
[22:24:02] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
[22:24:03] [INFO] testing 'Generic inline queries'  
[22:24:04] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
[22:24:07] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
[22:24:10] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'  
[22:24:14] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[22:24:18] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
[22:24:22] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
[22:24:26] [INFO] testing 'Oracle AND time-based blind'  
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n]
```

Sin embargo en los primeros 10 minutos podemos ver que la ejecución se detiene dentro del modo interactivo indicando que no hay vectores de ataque por inyección por tanto sugiere cambiar la estrategia. A esto se le dice que si y continúa el análisis.

```
kali@kali: ~  
File Actions Edit View Help  
[22:27:07] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'  
[22:27:11] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'  
[22:27:16] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
[22:27:16] [INFO] testing 'Generic inline queries'  
[22:27:17] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'  
[22:27:21] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'  
[22:27:24] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'  
[22:27:28] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'  
[22:27:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
[22:27:36] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'  
[22:27:40] [INFO] testing 'Oracle AND time-based blind'  
[22:27:45] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
[22:27:53] [WARNING] GET parameter 'mes' does not seem to be injectable  
[22:27:53] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'  
[*] ending @ 22:27:53 /2020-07-12/  
kali@kali:~$
```

Sin embargo al cabo de un tiempo, notamos que no arroja mayores resultados. Esto pasó con todas las URL probadas que salieron de la ejecución de la araña de ZAP.

2. Conclusiones

Si bien todas las herramientas fallaron, esto no quiere decir que la aplicación esté libre de fallas. En primer lugar, todas las pruebas fueron ejecutadas desde una máquina en la red, por tanto la situación podría ser diferente al intentarlos dentro de la misma red de la universidad.

Adicionalmente, como se pudo observar durante la ejecución de ZAP, la aplicación en si cuenta con malas prácticas de programación por parte de los módulos de terceros involucrados en esta.

De ejecutarse un análisis, este no solo debe hacerse a nivel de la aplicación en si como lo

especifica el enunciado, se tiene que tomar en cuenta otros sitios los cuales puedan servir como vectores laterales, sitios relacionados, revisar la estructura de la red y los servicios ya que en este caso, resulta que el sitio en cuestion es simplemente un front-end para otra aplicación conectada por detras.

Referencias

- [1] Documentación de sqlmap *sqlmap homepage*. <http://sqlmap.org/>
- [2] Documentación de nmap *nmap homepage*. <https://nmap.org/>
- [3] Documentación de OWASP ZAP *OWASP ZAP project homepage*. <https://owasp.org/www-project-zap/>
- [4] RedTeamTutorials *NIKTO Cheat Sheet*. <https://redteamtutorials.com/2018/10/24/nikto-cheatsheet/>