RADAR -> TIENDA.FLEX.CL

INFORME EJECUTIVO DE PENTESTING

ESTADO ACTUAL – RESULTADOS – RECOMENDACIÓN

PENTESTER
LILIO TAPIA
DIRECTOR DE DESARROLLO
AGENCIA RADAR

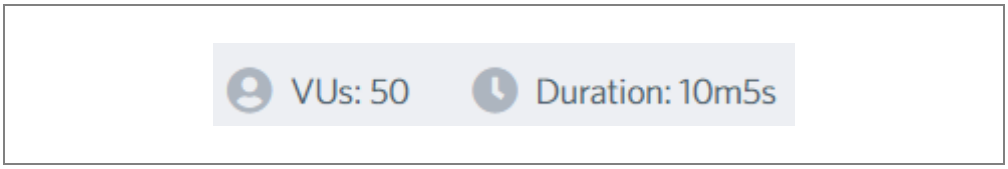
SERVIDOR

ESTADO ACTUAL DEL SERVIDOR

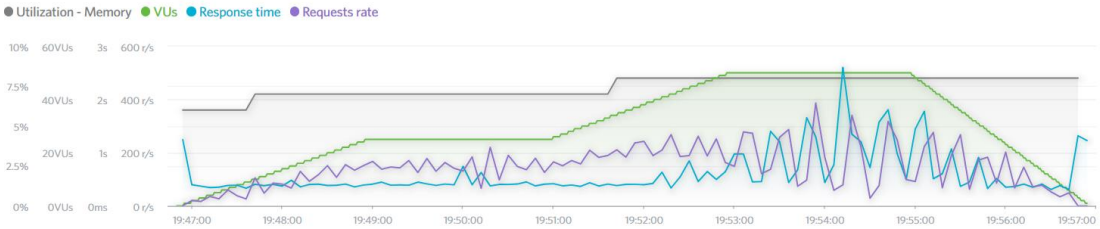
IP: 200.29.32.224 – PCKG 32B T=14MS TTL=51

El servidor fue sometido a un estrés simulado con un máximo de 50 VUs (virtual users) con el fin de no ocasionar caídas en el servicio real y de esta forma obtener un resultado estimado real.

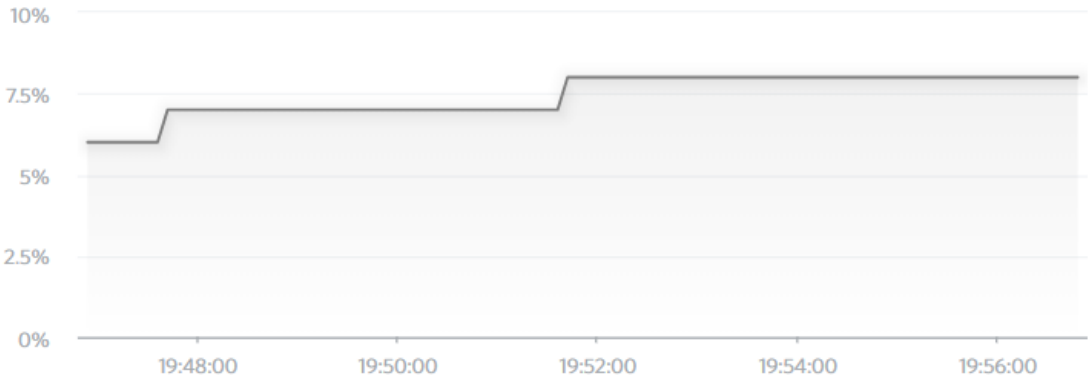
El procedimiento tuvo una duración total de 10 minutos y para ello se usó un servidor de Amazon preparado y configurado especialmente para esto con ubicación en Columbus.



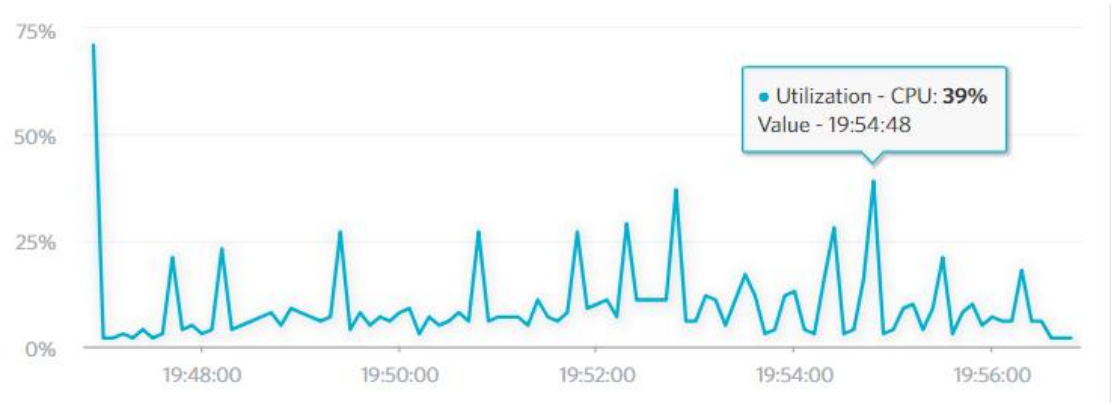
General:



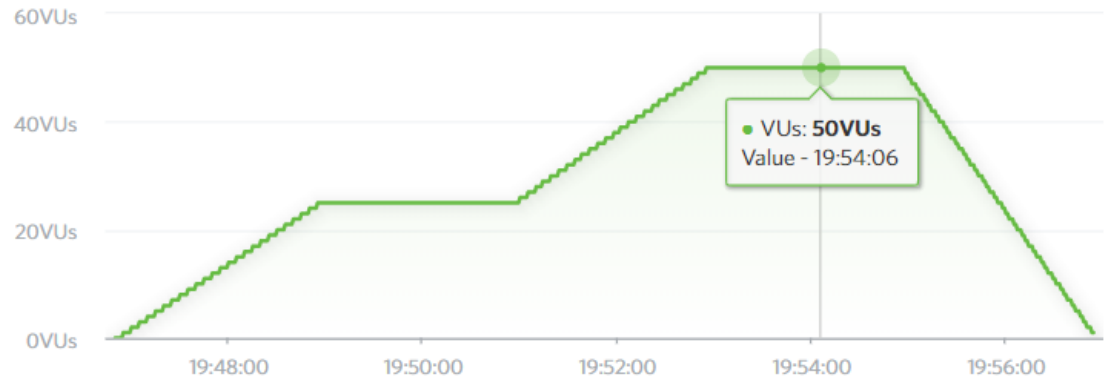
Memory:



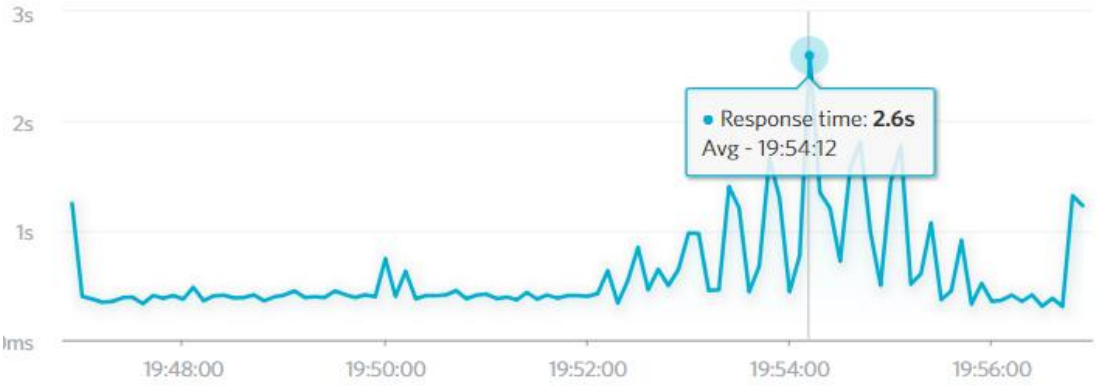
CPU:



VUs:



Response time:



LECTURA DE LOS DATOS

1. MEMORIA:

    a. La memoria total instalada en el servidor es suficiente para que 630 usuarios se conecten de forma simultánea y realicen un máximo de 550 request.

    b. El uso de la memoria es importante pero no es suficiente si no se utiliza en conjunto a la CPU.

2. CPU:

    a. El uso de CPU rinde hasta 180 Usuarios apróx en paralelo. Si bien la memoria es suficiente, no podrían llegar hasta 630 usuarios porque la cpu solo permite conectar a 180 apróx. Esto, bajo una ecuación usada comúnmente en el estrés de servidores, da un average de 260 usuarios de forma simultánea. Esto puede variar dependiendo de otros factores como la conexión del servidor y saturación de la red al momento del evento por lo cual puede aumentar y/o bajar un 20% en los números entregados.

SQL INJECTION + BRUTEFORCE

Se realizó una prueba de SQL injection al servidor DB y se extrajeron datos sin mayor valor del servidor. No obstante, al realizarse un bruteforce en conjunto con sql injection, se descubrió que está activa una vulnerabilidad muy presente en Magento y se pudo inyectar datos en los siguientes paths:

- /catalog/product/frontend_action_synchronize
- /catalog/product_frontend_action/synchronize

Esta vulnerabilidad, si bien está presente en las versiones 1.9, no es comúnmente explotada por cualquier hacker y tampoco representaría una amenaza real para flex, a menos que sea un blanco directo. En aquel caso y bajo ese contexto, esta vulnerabilidad se convierte en primordial y solamente se puede solucionar cambiando el sitio a su versión 2.3 ya que está actualizada y contiene un parche especial para evitar la inyección de datos.

Se adjunta link acerca del parche que liberó Magento en marzo 2019.

https://magento.com/security/patches/magento-2.3.1-2.2.8-and-2.1.17-security-update

SOBRE EL PENTESTING

- Las herramientas usadas son de completa autoría del pentester.
- Los datos pueden ser usados por el dueño del dominio como estimen convenientes.
- Para verificar el script usado en el estrés del servidor, se adjunta repositorio en gitHub.

  https://github.com/liliotapia/flex-EH-may-2019/
  dudas o consultas at lilio.tapia@radar.cl