Máster interuniversitario en Seguridad de las Tecnologías de la Información y las Comunicaciones (MISTIC)

Prueba de penetración de caja gris realizada a la solución Redborder versión cloud

Estudiante: Yesenia Guadalupe Trejo Alfaro

Directores del TFM:

Dra. Helena Rifà Pous (UOC)

Carlos Jiménez Barranco (Redborder)

Empresa: Redborder -ENEO Tenología

Junio 2017

Agradecimientos

Agradezco a todos aquellos que me apoyaron en la realización de este trabajo final de máster y en especial a la empresa Eneo Tecnología por permitirme analizar su solución Redborder y por la orientación recibida para poder llevar a cabo la prueba de penetración.

Pero sobre todo, agradezco enormemente al consorcio ISC^2 por otorgarme la beca Women's scholarship y así poder realizar los estudios de máster que me han permitido llegar hasta la realización de este trabajo.

Resumen

En el presente documento se hace una descripción de la empresa Eneo Tecnología, la plataforma a auditar, el alcance de la prueba de penetración, la metodología empleada, fases y resultados de cada una de estas, así como las conclusiones y recomendaciones para mitigar las vulnerabilidades encontradas.

Abstract

This document provides a description of: Eneo Tecnologia company, the platform to be audited, scope of the penetration test, the methodology used, the phases and results of each one of them, as well as the conclusions and recommendations to mitigate the discovered vulnerabilities.

Índice de contenido

Índice de figuras

Índice de tablas

1. Introducción

Cada día las empresas se encuentran ante el enorme desafío de cuidar sus activos de cibercriminales, por tal motivo es importante que estas dentro del marco de sus Sistemas de Gestión de la Seguridad de la Información (SGSI) implementen controles que permitan evaluar la seguridad real de la organización. Uno de estos controles son las pruebas de intrusión de caja gris, puesto que simulan la acción de un atacante externo con un mínimo de información y permiten evaluar el nivel de exposición al riesgo al que se enfrentan los sistemas objetos de estudio para determinar el grado de seguridad ante un ataque real.

Durante una prueba de intrusión se utilizan diferentes métodos y herramientas con la finalidad de identificar las vulnerabilidades existentes. Este tipo de pruebas nos proporcionan información detallada sobre las vulnerabilidades encontradas en los sistemas, las amenazas correspondientes que podrían explotarlas y orientación sobre medidas correctivas apropiadas.

El presente trabajo describe la metodología, fases y resultados de las pruebas de intrusión realizadas a la plataforma Redborder versión cloud producto de la empresa ENEO Tecnología. Además, en la fase relativa al informe se incluye un apartado de recomendaciones con la finalidad de ayudar a la empresa a mitigar las vulnerabilidades encontradas.

1.1. Acerca de la empresa Eneo Tecnología

Es una empresa de **ciberseguridad** y análisis de tráfico de red (NTA) de origen Español, cuya sede principal está ubicada en Sevilla.

ENEO Tecnología S.L. es una compañía que nació en 2003 con el objetivo de desarrollar soluciones para un mercado complejo que requería la consolidación de infraestructuras avanzadas de red para hacerlas más rápidas, seguras, fiables y fáciles de gestionar.

Actualmente posee una cartera de clientes nacionales e internacionales como CISCO, el Banco Santander, Aena, la Junta de Andalucía, entre otros.

ENEO Tecnología ofrece una solución **Open Source** basada en tecnología **Big Data** para el análisis de las redes de datos y la ciberseguridad activa llamada Redborder. Es una solución **escalable** apta para dar respuesta en entornos críticos en los que es necesario analizar, explotar y securizar un gran volumen de datos e información procedente de distintas fuentes: flujos de red, usuarios, eventos, logs, etc. Este producto se puede desplegar bajo demanda o como un servicio cloud.

1.2. Acerca de la solución Redborder versión cloud

Redborder es una solución de Big Data de código abierto que permite la visibilidad, análisis de datos y ciberseguridad la cual es escalable a las necesidades de las redes empresariales y de los proveedores de servicios.

Redborder es una plataforma con aplicaciones (apps) y sondas (módulos independientes que se ejecutan fuera de la plataforma) que pueden recopilar datos de forma activa en la red y aplicar políticas.

Cada app de Redborder, a través de sensores o sondas externas, recoge cierto tipo de información que se consolida en el núcleo del mánager para su inmediato análisis y visualización de la misma. Los sensores que alimentan al mánager pueden ser propios de Redborder o de terceros, es decir, la solución permite una amplia integración con otros fabricantes.

Redborder puede emplear información enviada por terceros, como pueden ser dispositivos routers, switches o controladores de red Wi-Fi o recibir información de sus propias herramientas como el sensor Redborder IPS, que realiza una inspección del tráfico de red y envía eventos al mánager.

La versión de Redborder cloud a analizar cuenta con la siguiente app:

Traffic: esta aplicación es capaz de realizar una gran ingesta de los flujos de red de cualquier organización, para es necesario configurar los distintos elementos de red como routers, switches, Wireless LAN Controllers (Cisco WLC), etc. y redirigir sus flujos al mánager de Redborder. Soporta los siguientes protocolos: NetFlow v5, NetFlow v9, IPFIX, FNF, etc. Permite geolocalizar los puntos de acceso, comprobar el estado de los mismos y controlar los valores de otros parámetros interesantes de la red. Por medio de esta app se puede conocer qué aplicaciones se están usando actualmente en la organización, cuál es el ancho de banda consumido en cada momento, compararlo con el día anterior, contar con un histórico del número de usuarios conectados a la red de la organización, ver qué dispositivos consumen más ancho de banda, con quién se comunican, países de los que se está recibiendo más tráfico, entre otros datos.

1.3. Objetivo

El objetivo principal de esta prueba de intrusión fue evaluar los niveles de seguridad de la plataforma Redborder con la finalidad de detectar y mitigar vulnerabilidades y/o amenazas que pudieran poner en riesgo el funcionamiento normal de la misma, integridad/confidencialidad de los datos almacenados y la imagen-reputación de la empresa.

1.4. Alcance

Se realizaron pruebas de intrusión a nivel de **aplicación web y** de **red** al los siguientes hosts: https://live.redborder.com y https://cloud-01.redborder.com

1.5. Metodología

La metodología que se utilizó para el desarrollo de las pruebas se basó en PTES (Penetration Testing Execution Standard) que comprende las siguientes fases.:

1. Interacción contractual
2. Reconocimiento
3. Modelado de amenazas
4. Análisis de vulnerabilidades
5. Explotación
6. Post-explotación
7. Reporte

1.5.1. Interacción contractual

Durante esta fase se definieron las condiciones para realizar las diferentes pruebas de intrusión, comprendió: definición del alcance, tiempo estimado de duración del test de intrusión, fecha de inicio y finalización, rangos IP y dominios a analizar, metas, tipos de pruebas a realizar (ingeniería social, DDOS,..), establecimiento de líneas de comunicación, información de contacto en caso de emergencia, proceso de notificación de incidentes, cronogramas, locaciones, manejo de evidencia, horarios para realizar las pruebas, consideraciones legales y algunas otras preguntas que el cliente -Eneo Tecnología- tuvo que responder para que el alcance del contrato pudiera ser estimado apropiadamente.

1.5.2. Reconocimiento

Esta fase consistió en recopilar la mayor cantidad de información posible para ser utilizada durante las fases de evaluación y explotación de las vulnerabilidades. Cuanta más información se pudo reunir durante esta fase, más vectores de ataque se pudieron utilizar en el resto de etapas.

En esta fase se usaron herramientas OSINT de tipo pasivo, semi pasivo y activo para encontrar, seleccionar y adquirir información de fuentes públicas y analizarla para producir inteligencia accionable. Además, se hizo recolección de información externa, también conocida como footprinting, que consiste en la interacción con el objetivo para obtener información desde una perspectiva externa a la organización.

Y además, como parte de esta fase se realizó la identificación de mecanismos de protección con la intención de maximizar la eficiencia de los ataques y minimizar el ratio de detección.

1.5.3. Modelado de amenazas

En esta fase se definió un enfoque de modelado de amenazas para la correcta ejecución de la prueba de penetración. El modelado se centró en dos elementos clave: activos y atacante (comunidad de amenazas / agente). Cada uno de ellos se desglosó en activos y procesos de la solución, y en amenazas y capacidades.

En este caso, al ser una prueba de penetración de caja gris, donde no se tuvo ninguna información previa sobre la organización, se creó un modelo de amenazas basado en el punto de vista del atacante.

1.5.4. Análisis de vulnerabilidades

Esta fase consistió en descubrir fallas en el sistema y aplicaciones que pudieran ser aprovechadas por un atacante. Se realizaron pruebas activas y pasivas, validación de las vulnerabilidades, correlación de hallazgos, y una vez que estas fueron corroboradas en el sistema objetivo, se determinó la exactitud sus ID's(p.Ej, CVE) y se investigó la potencial explotabilidad de las vulnerabilidades dentro del alcance de la prueba de penetración.

1.5.5. Explotación

Esta etapa se centró únicamente en establecer el acceso a un sistema o recurso al evitar las restricciones de seguridad a través del uso de exploits. El enfoque principal fue identificar el punto de entrada principal en la organización e identificar activos de valor alto.

1.5.6. Post-explotación

Durante esta fase se determinó el valor de la máquina comprometida y se definieron propuestas para mantener el control de esta para su uso posterior. El valor de la máquina estuvo determinado por la sensibilidad de los datos almacenados en ella y la utilidad de las máquinas para comprometer aún más la red. Los métodos descritos en esta fase estuvieron diseñados para ayudar a identificar y documentar datos confidenciales, identificar configuraciones, canales de comunicación y relaciones con otros dispositivos de red que se pudieron utilizar para obtener más acceso a la red y configurar uno o más métodos para acceder a la máquina en un momento posterior.

1.5.7. Informe

El informe se dividió en dos secciones principales: informe ejecutivo e informe técnico, con el fin de comunicar a diferentes audiencias los objetivos, métodos, resultados de las pruebas realizadas y recomendaciones de mitigación.

1.6. Cronograma

A continuación se muestra el cronograma aceptado por la organización:

Actividades	Marzo				Abril				Mayo				Junio		
	Semana de 6 al 12 de marzo	Semana del 13 al 19 de marzo	Semana del 20 al 26 de marzo	Semana del 27 de marzo al 2 de abril	Semana del 3 al 9 de abril	Semana del 10 al 16 de abril	Semana del 17 al 23 de abril	Semana del 24 al 30 de abril	Semana del 1 al 7 de mayo	Semana del 8 al 14 de mayo	Semana del 15 al 21 de mayo	Semana del 22 al 28 de mayo	Semana del 29 de mayo al 4 de junio	Semana del 5 al 11 de junio	Semana del 12 de junio
Fase 1: Interacción contractual															
Fase 2: Reconocimiento															
Fase 3: Modelado de amenazas															
Fase 4: Análisis de vulnerabilidades															
Fase 5: Explotación															
Fase 6: Post-explotación															
Fase 7: Informe															
Entrega de TFM y presentación en video															

Tabla 1. Cronograma

2. Interacción contractual

Durante esta fase se definieron las condiciones para realizar las diferentes pruebas de intrusión, se envió un cuestionario al equipo de Redborder(Eneo Tecnología) el cual comprendió las siguientes secciones:

- Preguntas generales: para definir la motivación de la empresa al solicitar la prueba de penetración, horarios y días de preferencia para llevar a cabo las fases 4 y 5 (análisis de vulnerabilidades y explotación).
- Network penetration test: para delimitar las direcciones IP a analizar, acciones permitidas durante la fase de explotación y post-explotación.
- Web application penetration test: para precisar los tipos de ataques y escaneos permitidos.
- DDos testing: para especificar si existirá algún entorno de pruebas para realizar dichos test.
- Terceras partes: para garantizar que se tengan los permisos por parte de terceros que pudieran estar involucrados en la plataforma a auditar.
- Líneas de comunicación: para establecer los canales de comunicación y formato de los ficheros.
- Consideraciones legales: para solicitar la firma por parte del representante de la empresa y garantizar la aprobación de las condiciones estipuladas en el plan de trabajo, así como de las condiciones que se manifiestan en el propio cuestionario.

2.1. Cuestionario

El cuestionario y las respuestas proporcionadas por la empresa se listan a continuación:

Preguntas generales

1. ¿La prueba de penetración se necesita para un requisito de cumplimiento específico? O ¿cuál es la meta de la empresa al solicitar la prueba de penetración?
   El objetivo principal es evaluar los niveles de seguridad de la plataforma y detectar vulnerabilidades y/o amenazas en la misma que pudieran poner en riesgo su funcionamiento normal, la integridad/confidencialidad de los datos contenidos y la imagen de la empresa.

2. ¿En qué días de la semana y horarios prefieren que se realice la fase de escaneo?
   Preferiblemente, de lunes a jueves de 18:00h a 8:00h (España), viernes a partir de las 18:00h (España) y fin de semana en cualquier momento. En caso de tratarse de escaneos activos, susceptibles de provocar algún tipo de degradación/alteración del servicio, se debería consensuar con la empresa.

3. ¿En qué días de la semana y horarios prefieren que se realice la fase de explotación?
   Preferiblemente, de lunes a jueves de 18:00h a 8:00h (España), viernes a partir de las 18:00h (España) y fin de semana en cualquier momento. En caso de tratarse de acciones susceptibles de provocar algún tipo de degradación/alteración del servicio, se debería consensuar con la empresa.

Network Penetration Test

1. ¿Desean que se prueben todas las IP vinculadas al dominio live.Redborder.com? Se han identificado dos: 54.86.84.150 y 52.0.168.54
   Sí.

2. En el caso de que se penetre un sistema,

   a. ¿cómo se deberá proceder?

   Una vez penetrado un sistema y, por tanto, confirmado una vulnerabilidad, no será preciso seguir indagando a partir de esa vulnerabilidad para ver si se pueden atacar otros sistemas. Es preferible recopilar toda la información relativa a esa penetración (e incluirla en el informe final), para poder reproducirla en caso que fuera preciso, y en caso de ser considerado crítico, reportarlo a la empresa a través del tutor.

   b. Para la fase de post-explotación, ¿permitirán realizar una evaluación de vulnerabilidad local en la máquina comprometida?

   Por defecto, no se deberían realizar tareas de post-explotación, entendiéndose que el objetivo de esas tareas sería mantener algún tipo de acceso al sistema para poder acceder a posteriori, p. ej. Para evaluar vulnerabilidad. No obstante, antes de llevar a cabo esa post-explotación, se deberá consensuar con la empresa para cada una de las vulnerabilidades.

   c. ¿Se podrá llevar a cabo intentos para obtener los privilegios más altos (root en máquinas Unix, SYSTEM o Administrator en equipos Windows) en la máquina comprometida?

   Sí, siempre y cuando no se provoque denegación/degradación del servicio. Se deberá notificar a la empresa del resultado de dichas pruebas, especialmente en los casos en que se consiga dicha escalada de privilegios.

   d. ¿Se podrá realizar ataques de diccionario, fuerza bruta, o ataques de contraseña exhaustiva contra hashes de contraseña local obtenido(por ejemplo, /etc/shadow en máquinas Linux)?

   Sí.

3. ¿Hay sistemas en la red que la empresa no posea, que puedan requerir aprobación adicional para probar?

Sí. De hecho, unos días antes de finalizar la fase de recopilación de información se deberá notificar a la empresa para que ésta informe a terceras partes de esta auditoría.

Web Application Penetration Test

1. ¿Se podrán realizar ataques de fuerza bruta contra el formulario de inicio de sesión?
   Sí, aunque no es el objetivo principal de esta auditoría.

2. Para realizar un análisis más completo se llevarán a cabo escaneos con credenciales ¿están de acuerdo con ello?
   Sí.

3. ¿Existen secciones de la aplicación web que puedan caracterizarse como frágiles?
   Al tratarse de un entorno en producción, toda la plafatorma (no sólo web) se puede considerar frágil o sensible. De hecho, uno de los objetivos del auditor será el evaluar y detectar posibles secciones/tecnologías que, debido a su fragilidad, puedan suponer un eslabón débil que comprometa la seguridad de todo el sistema.

DDos Testing

1. ¿Las pruebas de Denegación de Servicio se realizarán sobre algún entorno de pruebas o quedan completamente descartadas?
   A priori quedan descartadas. No obstante, llegado el caso se deberán evaluar con la empresa a través del tutor.

2. Si se realizará sobre un entorno controlado de pruebas, especificar la dirección URL:
   Por determinar, en base a lo indicado en pregunta anterior (ya no se realizaron prueba de DDOS por tanto ya no se determinó una dirección URL)

Tercera partes

1. ¿El proveedor de servicios en la nube(Amazon) está alertado sobre las pruebas y concede los permisos a la organización para realizar el test? Algunos proveedores de la nube tienen procedimientos específicos para los penetration testers que deben seguir, y pueden requerir formularios de solicitud, programación o permiso explícito de ellos antes de que la prueba pueda comenzar. Por ejemplo: https://aws.amazon.com/es/security/penetration-testing/

La empresa es conocedora de ello y está trabajando con terceras partes.

Líneas de comunicación

1. ¿El equipo de respuestas a incidentes (en caso de existir) está informado sobre la prueba de penetración?
   Algunas personas (tutores).

2. ¿Las comunicaciones de información sensible deberán ser cifradas?
   Con los tutores no será preciso, pero de cara a la elaboración de informes (parciales/finales) que fueran susceptibles de ser compartidos con otros miembros de la empresa sí será preciso que se cifre u oculte de alguna forma la información sensible, p.ej. credenciales.

3. ¿El envío de informes se realizará sobre el portal de la UOC o se utilizará algún buzón seguro, o el fichero se cifrará?
   El envío formal de informes correspondientes a las entregas evaluables se realizará sobre el portal de la UOC, dentro del aula de TFM, en el apartado de evaluación continua. Otro tipo de comunicaciones que puedan contener información sensible se realizarán al buzón del tutor. A priori, no será preciso cifrar los ficheros, salvo que se incluyan ficheros con credenciales u otra información sensible que realmente se deba visualizar para evaluar/confirmar p. ej. una vulnerabilidad.

4. En caso de que se necesite un medio cifrado ¿Qué herramienta se utilizará? ¿GPG o archivos cifrado por AES p. ej. con Vera Crypt?
   En ese caso, se deberá consensuar con la empresa, a través del tutor.

Consideraciones legales

1. Con la finalidad de que el proceso se apegue a un entorno real, así como para complementar la documentación ¿podrían firmar este cuestionario y la copia del plan de trabajo como manifiesto de aprobación del test de intrusión, por favor?
   La empresa firmó el cuestionario y el plan de trabajo como manifiesto de aprobación del test de intrusión

3. Reconocimiento

En esta fase se recopiló la mayor cantidad de información posible con el propósito de conocer mejor el objetivo y de esta forma tener una visión más completa al momento de llevar a cabo las demás fases.

En esta etapa se emplearon herramientas OSINT de tipo pasivo, semi pasivo y activo para encontrar, seleccionar y adquirir información de fuentes públicas y analizarla para producir inteligencia accionable. Además, se recolectó información externa (footprinting), que consiste en la interacción con el objetivo para obtener información desde una perspectiva fuera de la organización.

Para una mejor comprensión de la información recopilada, esta se aglutinó en las siguientes categorías:

3.1. Dominios

Se encontró que los dominios asociados a los hosts live.redborder.com y cloud-01.redborder.com son:

- redborder.com
- redborder.net
- redborder.org

Los dos últimos siempre redireccionan al primero.

3.2. Direcciones IP

Se detectaron dos direcciones IP asociadas al host live.redborder.com: **52.0.168.54 y 54.86.84.150 y** dos direcciones IP asociadas al host cloud-01.redborder.com: **52.207.51.160 y 54.86.155.29.**

3.3. Subdominio

Se detectó un subdomino asociado al host live.Redborder.com: **data.live.redborder.com.**

3.3.1. Direcciones IP

Se detectaron dos direcciones IP asociadas al subdomino data.live.redborder.com: **52.86.216.10 y 52.4.45.25**

3.3.2. Ubicación

El host está alojado en servidores de amazon AWS y está ubicado en Seattle, Estados Unidos.

3.3.3. Servicios encontrados

Están abiertos los puertos 80 y 443, pero solamente está funcionando el servicio de https(443).

3.4. Ubicación

Se detectó que utilizan los servicios de amazon AWS para alojar los sitios web. redborder.com se encuentra ubicado en Virginia, Estados Unidos mientras que live.redborder.com y cloud-01.redborder.com están en Seattle, EE.UU.

3.5. Sistema operativo y servidor web

La herramienta who.is menciona que la solución está montada sobre un servidor Apache y un S.O. Ubuntu, sin embargo, nmap arroja que se utiliza el servidor web nginx versión 1.8.1 y la documentación encontrada en el punto 3.9 menciona que Redborder está basado en la distribución Linux CentOS 6.5.

3.6. Dispositivos intermedios

Al realizar pruebas desde el centro de auditorías (México) se observó que fueron necesarios 18 saltos para llegar al destino, es decir, existen 16 dispositivos intermedios entre la IP desde donde se realizaron las pruebas de penetración y el objetivo. Y en los anexos entregados a la empresa se puede ver la ubicación geográfica de cada dispositivo involucrado, los dispositivos clave y posibles proveedores de red.

3.7. Servicios encontrados

live.redborder.com y cloud-01.redborder.com tienen habilitados los puertos 80 y 443, estos puertos están asociados a los servicios HTTP y HTTPS.

3.8. Direcciones URL interesantes

A través de google Hacking y la herramienta SpiderFoot se detectaron varias URL que podrían resultar de interés para la fase de análisis de vulnerabilidades.

URL para registro del sensor en Redborder versión cloud

- https://live.redborder.com/api/v1/sensors

Registros publicados por certificatedetails.com :

- https://certificatedetails.com/5f60cf619055df8443148a602ab2f57af44318ef/235d2ebac5abb3b662b94c1bc92233b7/data.live.Redborder.com que indica que en live.redborder.com existe otro subdominio: data.live.Redborder.com

URL's obtenidas de analizar distintos archivos js

- https://live.redborder.com/assets/"+this.url_+"
- https://live.redborder.com/dashboard/sensors/'+t.id+'/overview
- https://live.redborder.com/dashboard/sensors/'+t.sensor_id+'/overview
- https://live.redborder.com/reports/{{report}}/remove_page/{{page}}
- https://live.redborder.com/reports/{{report}}/widgets/list?page={{page}}
- https://live.redborder.com/sensors/'+$(this).data(
- https://live.redborder.com/sensors/'+h.id+'/view
- https://live.redborder.com/sensors/'+t.id+'/edit

Repositorio de Github de Redborder

- https://github.com/Redborder/

3.9. Documentos que contienen información sensible

A través de Google se localizaron los siguientes documentos que contienen información sobre la tecnología y arquitectura de Redborder:

Despliegue y plataformado en entornos Cloud - Universidad de Sevilla

- http://bibing.us.es/proyectos/abreproy/90419/fichero/Despliegue+y+plataformado+en+entornos+Cloud.PDF

Monitorización de servidores Cloud - idUS - Universidad de Sevilla

- https://idus.us.es/xmlui/handle/11441/44261

3.10. Metadatos de documentos

Se analizaron los metadatos de los documentos del área de Recursos https://redborder.com/resources pero no se detectaron datos relevantes.

3.11. Tecnologías detectadas

A través de una revisión del portal redborder.com y de documentación listada en el punto 3.9 se detectó que live.redborder.com utiliza las siguientes tecnologías:

- **Amazon WebServices (EC2, VPC, S3, RDS, Route 53)**
- **Apache Kafka**
- **Apache Samza**
- **Bootstrap**
- **ChefServer**
- **Druid**
- **Hadoop /HDFS**
- **Http2k (ver respositorio de Github)**
- **JQuery**
- **PostgreSQL**
- **PUMA**
- **Ruby on Rails**
- **S3**
- **Zookeper**

Durante la fase de análisis de vulnerabilidades se confirmaron o descartaron alguna de estas.

3.12. Arquitectura de Redborder

En la documentación encontrada en la sección 3.9 se describe la posible infraestructura de Reborder:

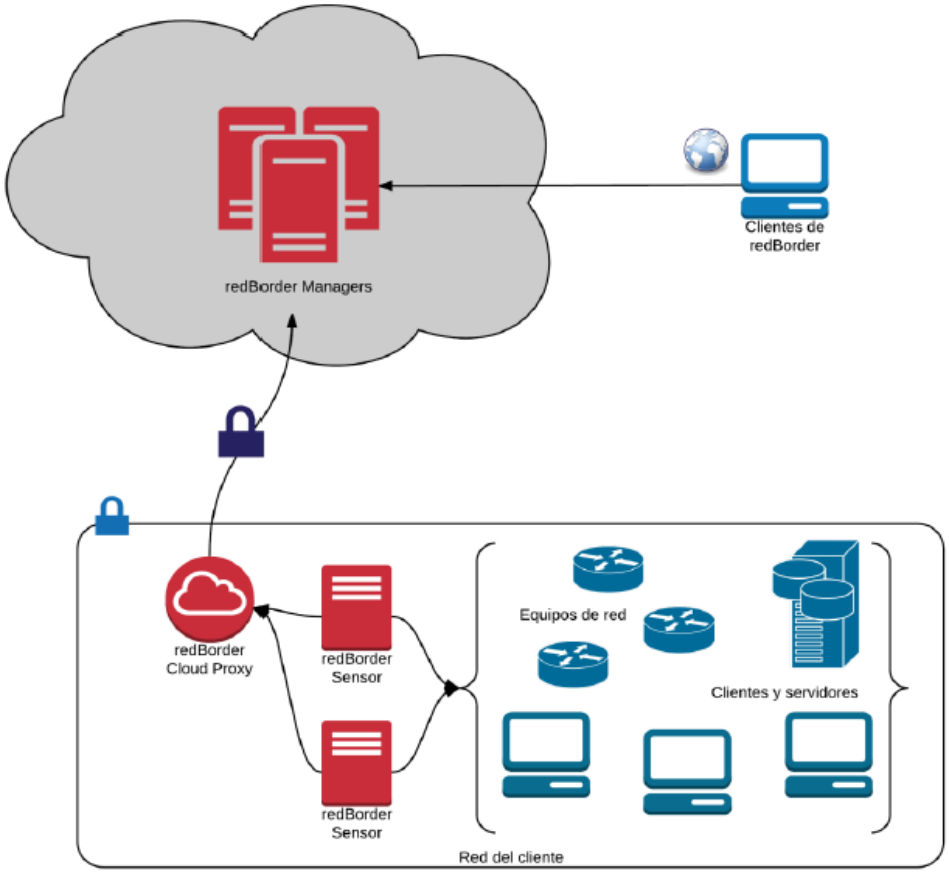


Figura 1. Arquitectura de Redborder

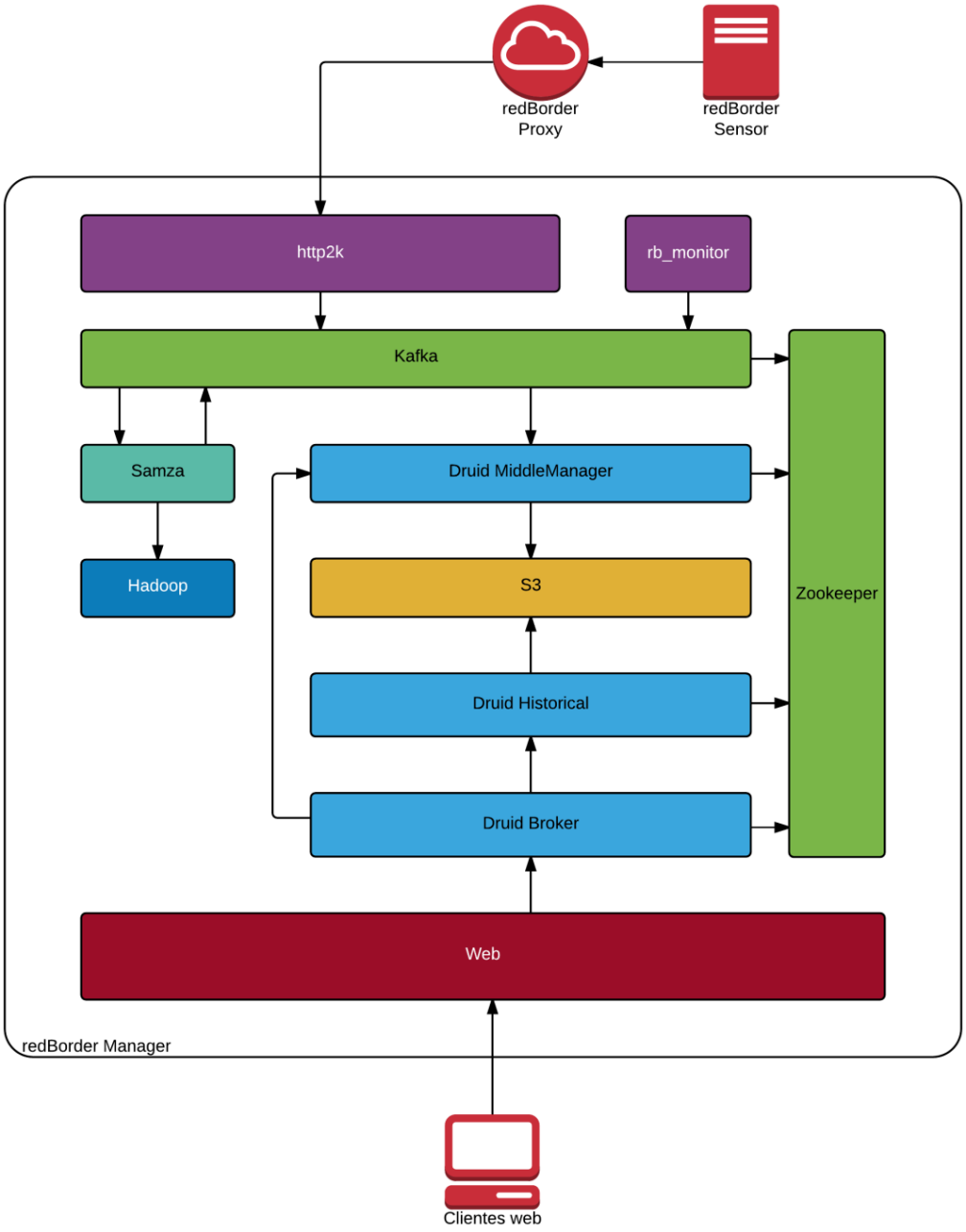


Figura 2. Arquitectura de Redborder- versión extendida

Como se puede apreciar, existen dos vías para interactuar con la plataforma Redborder versión cloud: a través del cliente web y a través de un sensor, la primera es ingresando a las direcciones URL http://live.redborder.com/ y http://cloud-01.redborder.com y la segunda a través de las URL https://live.redborder.com/api/v1/sensors (encontrada en la sección 3.8) y en https://cloud-01.redborder.com/api/v1/sensors

3.13. Empleados que trabajan en Redborder(Eneo tecnología)

Se localizó el listado de empleados, cargos, actividades que realizan, dirección de correo electrónico y enlaces a sus perfiles en las redes sociales como twitter o linkedin. Estos resultan de gran utilidad cuando se desean mezclar técnicas de ingeniería social.

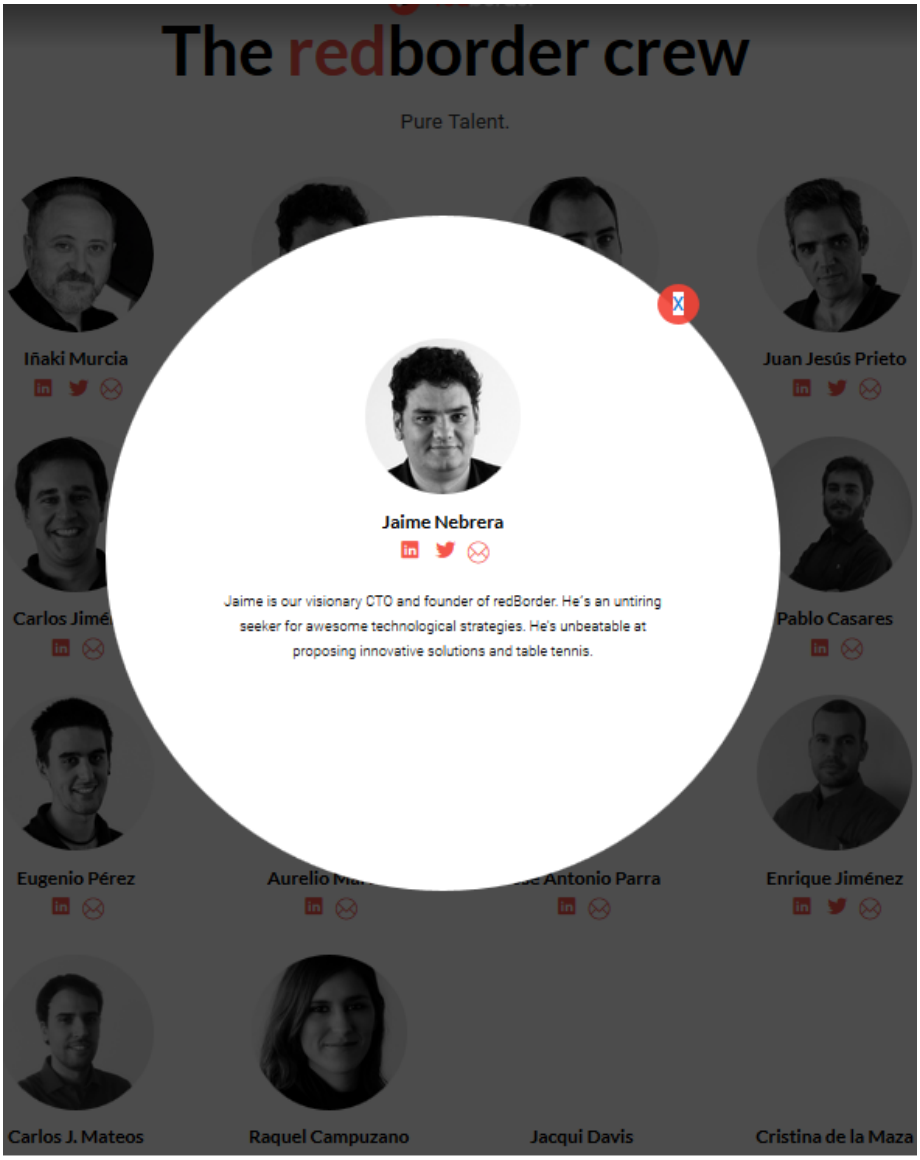


Figura 3. Equipo Redborder

3.14. Clientes

Desde el sitio de redborder.com se pudo ver el listado de compañías que han probado el producto, estas son: Grupo Santander, CISCO, aena, Junta de Anadalucía y produban. Posiblemente en este momento sean más, pero no estuvieron listadas en el sitio. Esta información fue muy valiosa puesto que estas podrían salir afectadas, es decir, a través de una vulnerabilidad crítica en Redborder se puede llegar a comprometer información de estos clientes.

3.15. Fuerza humana en el área de seguridad

Se descubrió la existencia de un equipo de CSIRT dentro de la organización que gestiona los incidentes en seguridad detectados por el equipo interno y por usuarios de Redborder. Esta información fue localizada en http://support.redborder.com/hc/en-us

3.16. Acceso a la platafarmo Redborder versión cloud

Para tener acceso Redborder versión cloud el usuario se debe registrar en el sitio de Redborder https://redborder.com/trial y solicitar una cuenta Redborder para cloud.

3.17. Mecanismos de protección

El servidor redirigió siempre a su versión cifrada, es decir, al servicio https.

Se comprobó que el servidor utiliza un certificado RSA de 2048 bits emitido por Amazon el 26 de marzo de 2017 y expirará el 27 de abril del 2018.

El servidor soporta cifrado: TLS v1.0. TLS v1.1, TLS v1.2 .

4. Modelado de amenazas

Para el siguiente modelado de amenazas de la solución Redborder versión cloud se utilizó la metodología de categorización de amenazas STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege por sus siglas en inglés) y fue realizado con el apoyo de la herramienta Microsoft Threat Modeling Tool 2016.

4.1. Metodología empleada

Se llevaron a cabo los siguientes pasos:

a. **Descomposición de la solución:** se profundizó en el conocimiento de la aplicación y se determinó cómo interactúa con entidades externas. Esta fase consistió en determinar puntos de entrada dónde un potencial atacante puede interactuar con la aplicación y se realizó la identificación de activos. Para este caso se generó el siguiente diagrama de flujo de datos (DFDs) -El DFD en alta definición se incluye en el anexo E-.

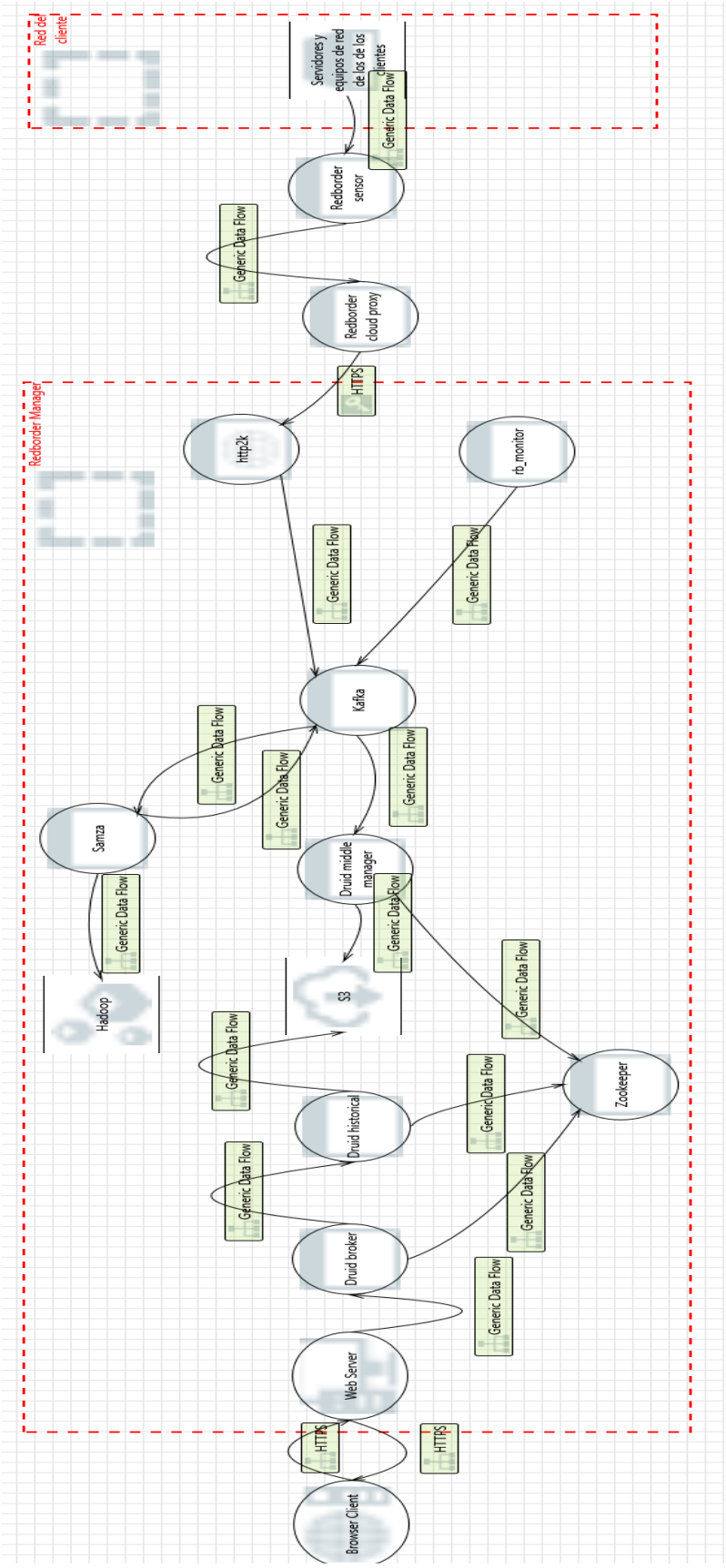


Figura 4. Diagrama de flujo- redborder versión cloud

b. **Determinación y jerarquización de amenazas:** la identificación de amenazas críticas se realizó utilizando la metodología de categorización de amenazas STRIDE. Y el riesgo de seguridad para cada amenaza se determinó usando el modelo de evaluación de riesgos DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability por sus siglas en inglés).

Se utilizó la siguiente tabla de valores:

Puntuación	Alto(3)	Medio(2)	Bajo(1)
Damage potential (Daño potencial)	El atacante podría tener acceso completo, actuar en un contexto privilegiado o subir contenido.	Divulgación de información sensible	Divulgación de información trivial
Reproducibility (Reproducibilidad)	El ataque es fácilmente reproducible.	El ataque se podría reproducir, pero sólo en condiciones muy concretas	Ataque difícil de reproducir, incluso conociendo la naturaleza del fallo.
Exploitability (Explotabilidad)	Requiere pocas habilidades. Novato	Requiere moderadas habilidades.	Requiere un nivel de habilidad muy alto. Experto.
Affected users (Usuarios afectados)	Todos los usuarios y clientes clave.	Algunos usuarios	Pocos usuarios afectados
Discoverability (Descubrimiento)	Existe información pública que explica el ataque. Vulnerabilidad presente en una parte de la aplicación muy utilizada	La vulnerabilidad afecta a una parte de la aplicación que casi no se utiliza. No es muy probable que sea descubierta	El fallo está oculto, no es muy probable que los usuarios puedan utilizarlo para causar un daño potencia

Tabla 2. Tabla de valores

Y la siguiente escala de puntuación del riesgo:

Extremo	13-15
Alto	10-12
Elevado	7-9
Moderado	4-6
Bajo	1-3

Tabla 3. Escala de puntuación del riesgo

Los pasos anteriores dieron como resultado la siguiente tabla de amenazas y riesgos:

No.	Amenaza	Categoría	Descripción	D	R	E	A	D	Total	Riesgo
1	Bloqueo o parada del Redborder manager	Denial Of Service	El Redborder manager puede sufrir un bloqueo, detención o ejecución lenta; en todos los casos violando una métrica de disponibilidad.	3	2	2	3	3	13	Extremo
2	Elevación cambiando el flujo de ejecución del navegador	Elevation Of Privilege	Un atacante puede pasar datos al navegador para cambiar el flujo de ejecución de la plataforma Redborder	3	2	2	3	3	13	Extremo
3	Memoria de procesos del servidor web alterada	Tampering	Si el Servidor Web tiene acceso a la memoria, como la memoria compartida o los punteros, o se le da la capacidad de controlar lo que ejecuta el Cliente del Explorador (por ejemplo, pasar un puntero de función), el	3	2	2	3	3	13	Extremo

			Servidor Web puede alterar el Cliente del Explorador.								
4	Spoofing del servidor Web	Spoofing	El servidor Web puede ser falsificado por un atacante, provocando que las credenciales y navegadores de los clientes se vean comprometidos	3	2	2	3	3	13	Extremo
5	Cross Site Scripting	Tampering	El servidor web 'Servidor Web' podría ser objeto de un ataque XSS porque no sanitiza las entradas	2	3	3	3	1	12	Extremo
6	Elevación cambiando el flujo de ejecución en el sensor Redborder	Elevation Of Privilege	Un atacante podría pasar datos al sensor Redborder para cambiar su flujo de ejecución	3	2	1	2	2	10	Alto
7	Control de acceso débil para un recurso	Information Disclosure	La protección de datos inadecuada de los Servidores y equipos de red de los clientes puede permitir que un atacante lea información no destinada a la divulgación	2	2	2	1	3	10	Alto
8	Elevación con suplantación de identidad	Elevation Of Privilege	El servidor web puede ser capaz de suplantar el contexto del cliente del navegador para obtener privilegios adicionales.	3	1	2	3	1	10	Elevado

9	Almacén de datos inaccesible	Denial Service	Of	Un agente externo podría impedir el acceso a un servidor de almacenamiento o base de datos	3	1	1	3	1	9	Elevado
10	Elevación con suplantación de identidad	Elevation Privilege	Of	El navegador puede ser capaz de suplantar el contexto del servidor Web para obtener privilegios adicionales.	3	1	1	3	1	9	Elevado
11	Proceso de bloqueo o parada del cliente del navegador	Denial Service	Of	El navegador se puede bloquear, detener o se ejecuta lentamente; en todos los casos violando una métrica de disponibilidad.	1	2	2	3	1	9	Elevado
12	Falsificar el cliente del navegador	Spoofing		El cliente del navegador puede ser falsificado por un atacante y esto puede conducir a un acceso no autorizado al Web Server.	3	1	1	3	1	9	Elevado
13	Modificación del Redborder cloud proxy	Tampering		Si al proxy Redborder cloud proxy se le da la capacidad de controlar lo que http2k ejecuta, el proxy podría interferir con http2k	3	1	1	3	1	9	Elevado
14	Spoofing del Redborder cloud proxy	Spoofing		El proxy Redborder cloud proxy puede ser falsificado por un atacante y esto puede conducir a un acceso no	3	1	1	3	1	9	Elevado

			autorizado a http2k.								
15	consumo excesivo de recursos por parte de S3 y el resto de componentes	Denial Of Service	¿S3 y el resto de componente de Redborder Manager toman medidas explícitas para controlar el consumo de recursos? Los ataques de consumo de recursos pueden ser difíciles de tratar, y hay veces que tiene sentido dejar que el sistema operativo haga el trabajo. Tenga cuidado de que sus solicitudes de recursos no bloqueen, y que lo hacen el tiempo de espera.	2	1	1	3	1	8	Elevado
16	Repudio de datos por parte del sensor Redborder	Repudiation	El sensor de Redborder puede afirmar que no recibió datos de los servidores y equipos de red de los clientes.	3	1	1	2	1	8	Elevado
17	El flujo de datos HTTPS puede ser interrumpido	Denial Of Service	Un agente externo puede interrumpir los datos que fluyen a través del navegador y el web server del Redborder manager	2	1	1	3	1	8	Elevado

18	Spoofing del almacén de datos de destino S3	Spoofing	S3 puede ser suplantado por un atacante y esto puede llevar a que los datos se escriban en el servidor del atacante en lugar del S3 verdadero	1	1	1	3	1	7	Elevado
19	Spoofing del almacén de datos de destino Hadoop	Spoofing	Hadoop puede ser falsificado por un atacante y esto puede conducir a que los datos se escriban en el servidor del atacante en lugar de Hadoop	1	1	1	3	1	7	Elevado
20	El sensor de Redborder puede estar sujeto a elevación de privilegios mediante la ejecución remota de código	Elevation Of Privilege	Los servidores y equipos de red de los clientes podrían ser capaces de ejecutar código remotamente a través del sensor Redborder.	2	1	1	2	1	7	Elevado
21	Spoofing de los Servidores y equipos de red de los clientes	Spoofing	Servidores y equipos de red de los clientes pueden ser falsificados por un atacante y esto puede conducir a datos incorrectos entregados al sensor Redborder.	2	1	1	1	2	7	Elevado
22	Spoofing del sensor de Redborder	Spoofing	El sensor de Redborder puede ser falsificado por un atacante y esto puede dar lugar a la divulgación de información	2	1	1	1	2	7	Elevado

			proporcionada por los Servidores y equipos de red de los clientes							
23	Posible rechazo de datos por el cliente del navegador	Repudiation	El navegador puede afirmar que no recibió datos del servidor web	3	1	1	1	1	7	Elevado
24	Elevación cambiando el flujo de ejecución en el servidor Web	Elevation Of Privilege	Un atacante puede pasar datos al servidor Web para cambiar el flujo de ejecución de la plataforma Redborder	3	1	1	1	1	7	Elevado
25	Elevación cambiando el flujo de ejecución en http2k	Elevation Of Privilege	Un atacante puede pasar datos en http2k para cambiar su flujo de ejecución dentro del Redborder Manager	2	1	1	2	1	7	Elevado
26	Repudio de datos por http2k	Repudiation	Http2k podría afirmar que no recibió datos del proxy de Redborder	2	1	1	2	1	7	Elevado

Tabla 4. Amenazas y riesgos

5. Análisis de vulnerabilidades

Con base en la información obtenida en la fase de reconocimiento se llevaron a cabo pruebas activas y pasivas en búsqueda de vulnerabilidades, se validaron cada una de éstas, se efectuó la correlación de hallazgos, se clasificaron por Zero Day o ID asociado y finalmente, por cada vulnerabilidad se definió el potencial de explotabilidad con base en el sistema CVSS 3.0.

El análisis de vulnerabilidades fue manual y automatizado utilizando herramientas open source como Nessus Free y de pago como OWASP Burp Suite. Todo lo anterior, con el objetivo de encontrar el mayor número de vulnerabilidades para llevar con éxito el resto de las fases de la prueba de intrusión.

Para una mejor comprensión de la información recopilada las vulnerabilidades se aglutinaron en las siguientes categorías:

5.1. En el dominio cloud-01.Redborder.com

5.1.1. Obtención del listado y configuración de todos los dominios y sondas

Se detectaron vulnerabilidades de tipo “web parameter tampering” que permiten tener acceso a toda la estructura de Redborder.

- Modificando la URL https://cloud-01.Redborder.com/sensors /?/export_tree que se encuentra como enlace de la opción Export Tree de cada uno de los menús de los dominios (sección Sensors) fue posible obtener toda la estructura y configuración de dominios, subdominios y sondas.

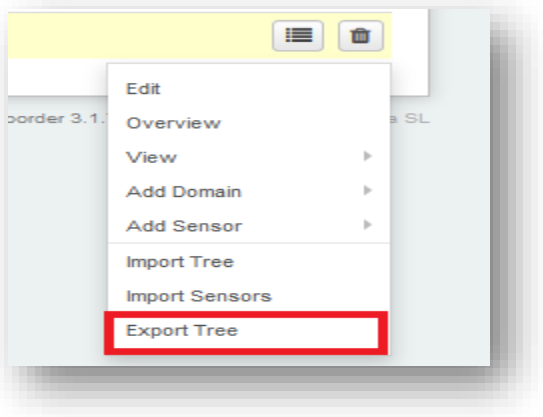


Figura 5. Opción Export Tree del menú de un dominio –sección Sensors-

Sustituyendo ? por el numero 1, se pudo obtener acceso a toda la estructura de dominios y sondas de Redborder, puesto que 1 corresponde

al dominio root de Redborder versión cloud. Al hacer clic en Expor Tree se desacrgó un fichero de extensión tar.gz con toda la estructura de dominios y sondas (Anexo F).

Figura 6. Estructura de dominios y sondas contenida en el fichero tar.gz

- Modificando la URL https://cloud-01.Redborder.com/dashboard/sensors/?/children que se encuentra en los ficheros javascript de la sección Sensors fue posible conocer toda la estructura de dominios y subdominos de la solución.

```
$.ajax({
  async: false, // Must be false, otherwise loadBranch happens after showChildren?
  url: "/sensors/" + sensor.id + "/children",
  success: function(html){
    // Session may expire and, in that case, the login HTML page will be returned.
    // This is because devise redirects to login page on session expiral and this is an HTML
    // request, not a JS one; so the browser will automatically redirect the request
    // and return 200 OK with the login HTML.
    if ($(html).find('form[action="/users/login"]').length > 0) {   // Session has expired
      location.href = "/sensors/tree";
    } else {
      var rows = $(html).filter("tr");
      $('span#loading_sensor').remove();

      if($('#tree').data('admin') == true){
```

Figura 7. Código javascript de la solución Redborder

Por ejemplo, modificando el valor de ? por el número 3 se puedo ver el contenido de un dominio que a su vez contiene a los subdominios arodriguez-office y UOC. Para conocer toda la estructura se repitió el ejercicio con otros números.

Figura 8. Subdominio arodriguez-office

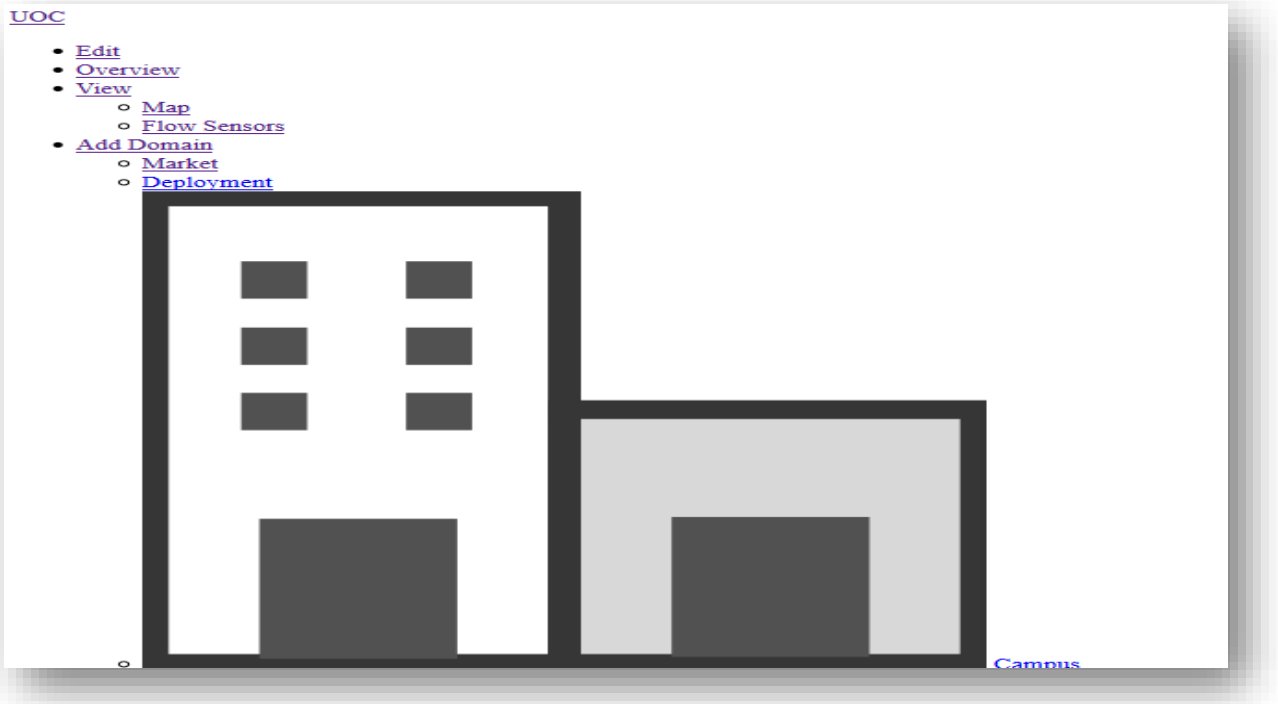


Figura 9. Subdominio UOC

- También modificando la URL https://cloud-01.Redborder.com/dashboard/sensors/?/overview que se encuentra como enlace de la opción Overview de cada uno de los menús de los dominios (sección Sensors) fue posible conocer toda la estructura de dominios y subdominos de Redborder versión cloud.

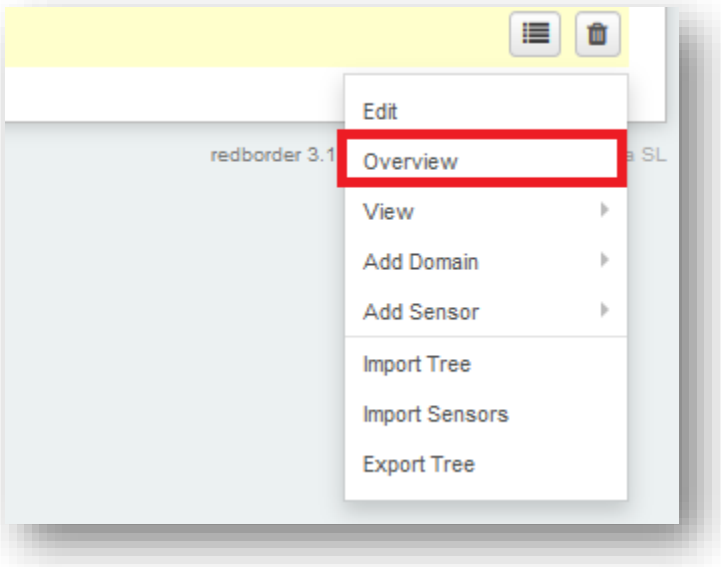


Figura 10. Opción Overview del menú de un dominio –sección Sensors-

Por ejemplo, al sustituir el valor de ? por el ID 63 se logró observar una sonda perteneciente al dominio UOC que a su vez también pertenece al dominio Redborder.

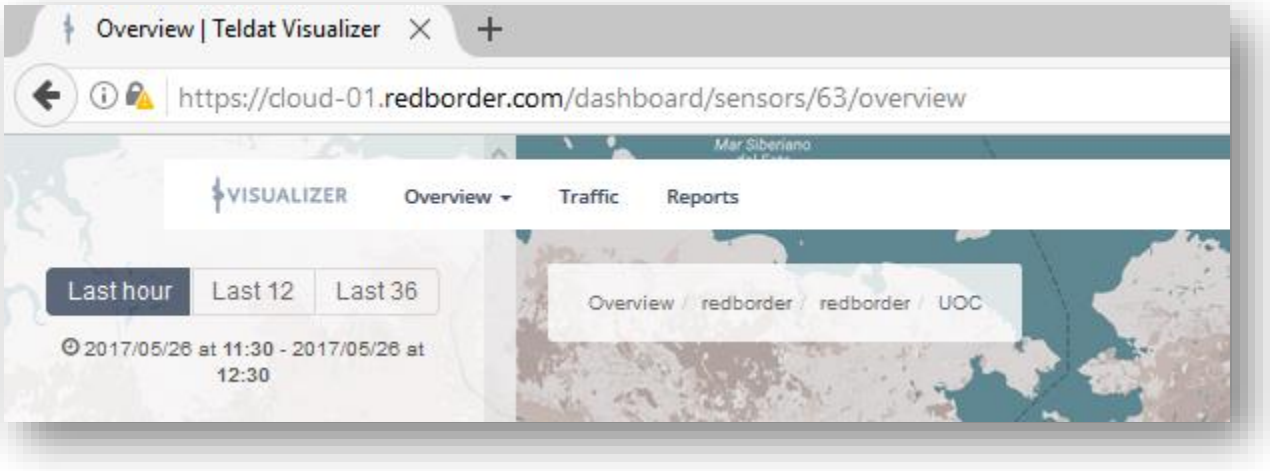


Figura 11. Vista de la sección Overview

- Modificando la URL https://cloud-01.Redborder.com/sensors/?/monitor_categories que se encuentra como enlace de la opción Monitors de cada uno de los menús de las sondas de tipo Flow(sección Sensors) fue posible conocer toda la estructura de dominios y subdominos de Redborder versión cloud.

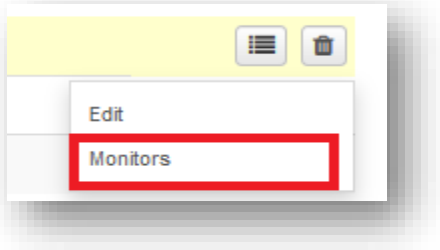


Figura 12. Opción Monitors del menú de una sonda –sección Sensors-

Sustituyendo ? por el valor 90 se pudo obtener el nombre del dominio/sensor que corresponde a ese ID, se identificó que es el dominio jmollagi

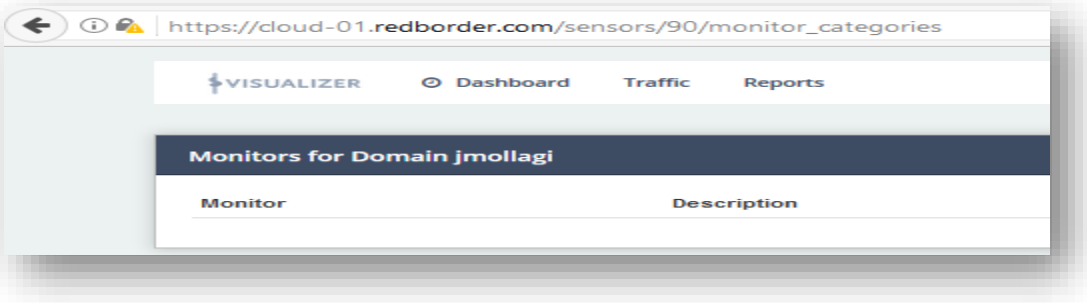


Figura 13. Sección Monitors

- Modificando los valores de los atributos data-sensorid y value (del campo "dashboard[sensors_collaborators][0][sensor_id]") de las sección editar o crear Dashboard se logró obtener el nombre de los dominios y subdominios de la solución

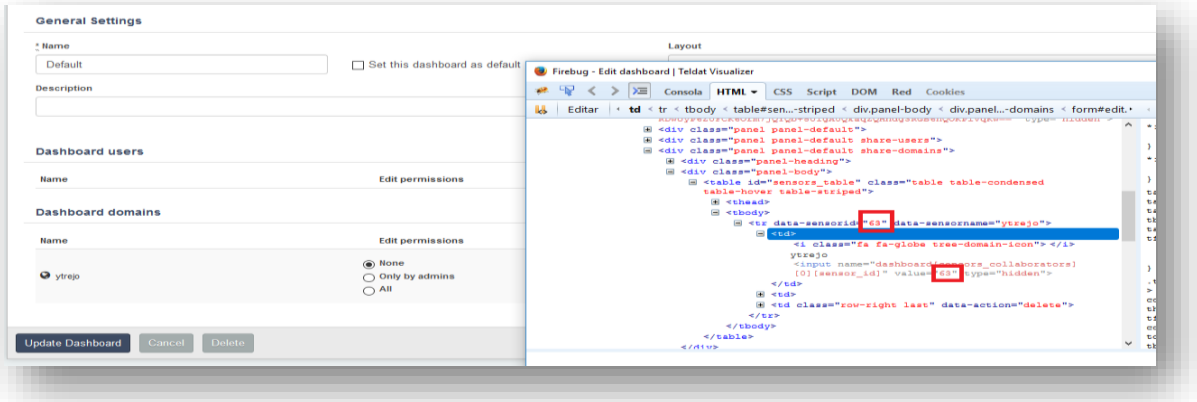


Figura 14. Edición del código en sección dashboard

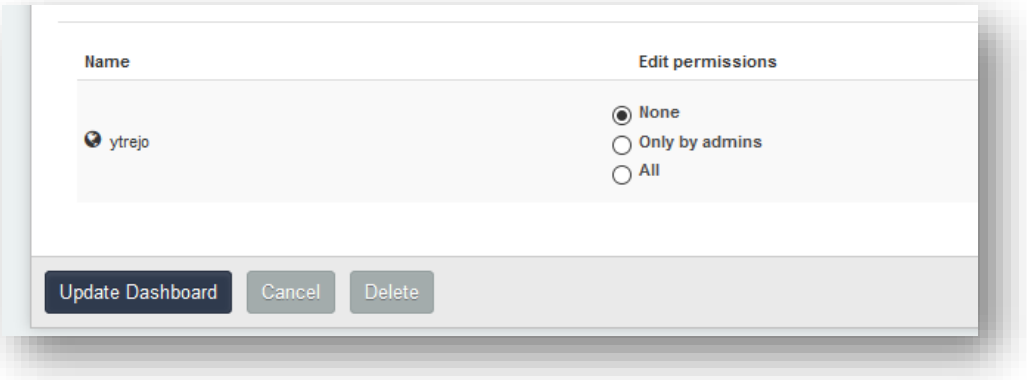


Figura 15. Edición del código en sección dashboard – versión amplificada

Sustituyendo los valores de ytrejo por otro valor, por ejemplo 63, y guardando los cambios, se pudo observar que al abrir de nuevo la sección editar Dashboard apareció el nombre del dominio que corresponde al ID 63: UOC.

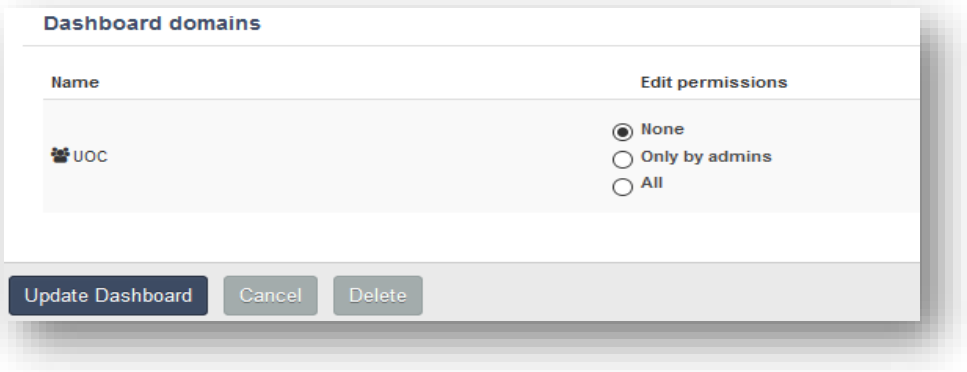


Figura 16. Dominio modificado

- De la misma forma, modificando los valores de los atributos data-sensorid y value (del campo “report[sensors_collaborators][0][sensor_id]”) de las secciones editar o crear un Reporte se obtuvo el nombre de los dominios y subdominios de la solución

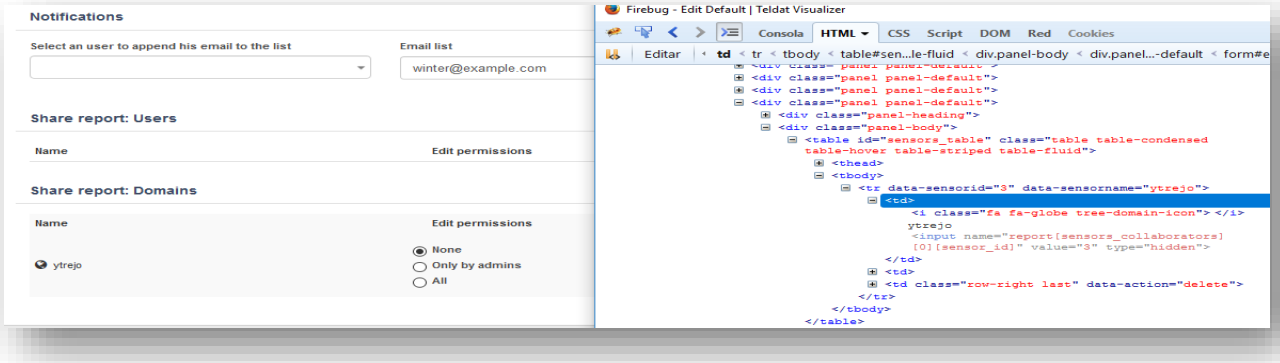


Figura 17. Edición de reporte

Por ejemplo, primero se sustituyeron los valores de ytrejo por el valor 3 y se guardaron los cambios, y posteriormente se abrió de nuevo la sección editar reporte, una vez abierto se puedo apreciar que el nombre del dominio al que corresponde el ID 3 es Redborder.

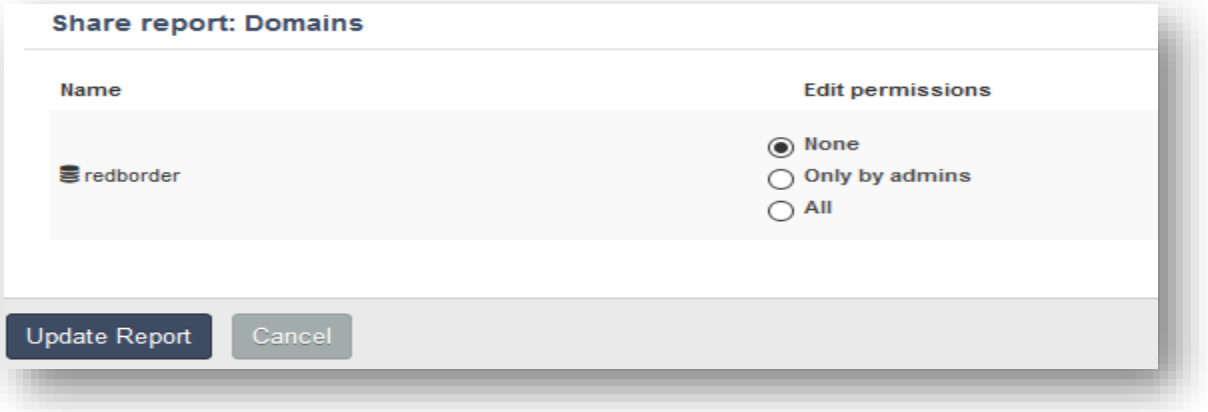


Figura 18. Edición de reporte –versión amplificada

- Modificando el valor del atributo value del campo “domains-select” al realizar una búsqueda avanzada (secciones Traffic e Infrastructure Monitor) permitió obtener el nombre de cada uno de los dominios y sondas de Redborder versión cloud.

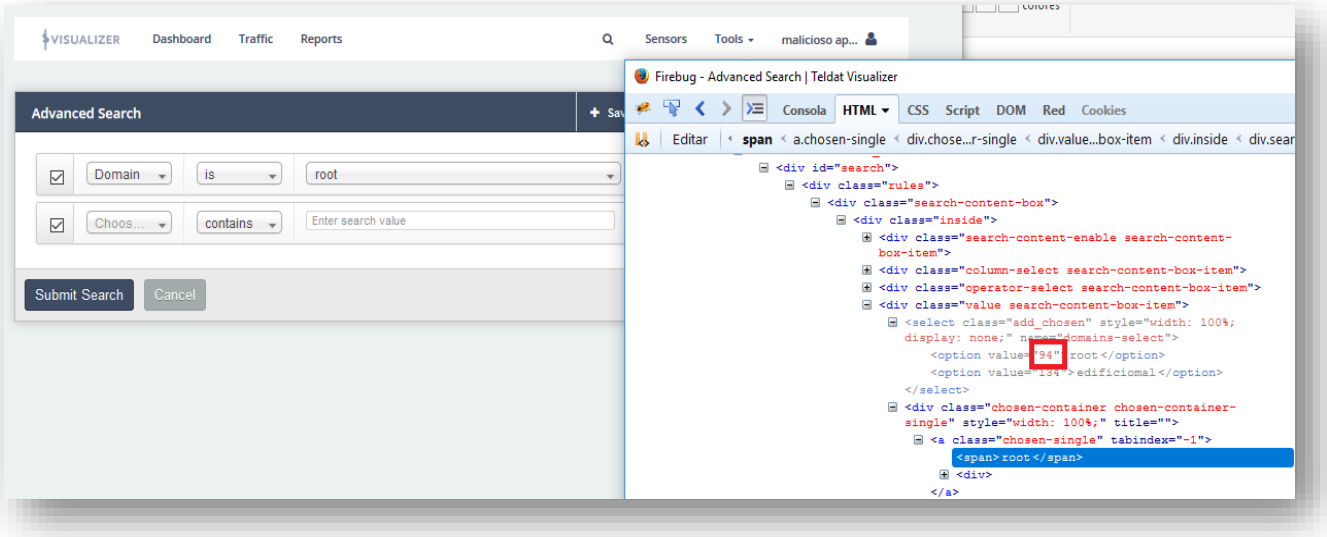


Figura 19. Búsqueda avanzada –sección Traffic e Infrastructure monitor-

Reemplazando el valor del atributo value del campo “domains-select” por el valor 63 se pudo identificar que el ID 63 corresponde al dominio UOC.

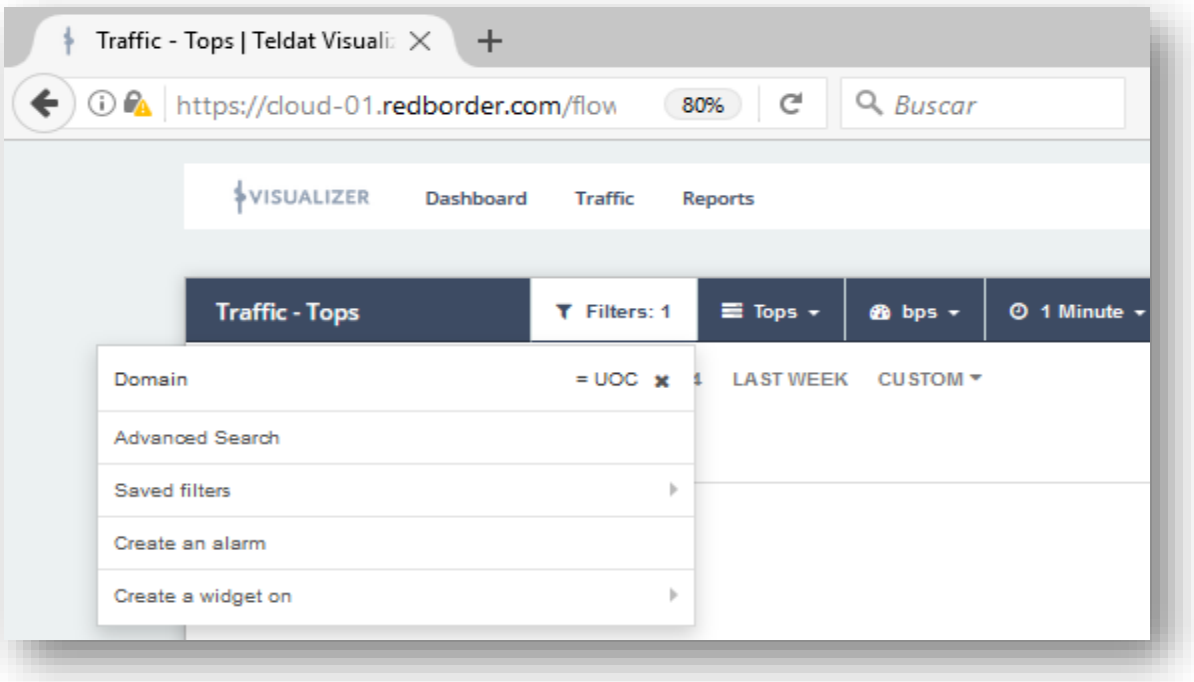


Figura 20. Dominio divulgado en sección búsqueda avanzada

5.1.2. Creación de dominios y sondas a cualquier dominio/usuario

Se detectó una vulnerabilidad de tipo “web parameter tampering” que permite crearle a cualquier dominio de Redborder una sonda, apoyándose de la información obtenida en la sección 5.1.1.

- Modificando la URL https://cloud-01.Redborder.com/sensors/?/import_tree que se encuentra como enlace de la opción Import Tree de cada uno de los menús de los dominios (sección Sensors) se logró importarle a cualquiera de los dominios cualquier tipo de subdominio y sonda.

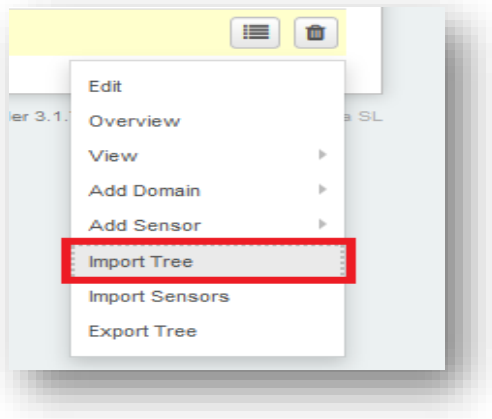


Figura 21. Opción Import Tree del menú de un dominio –sección Sensors-

Por ejemplo, reemplazando ? por el valor 90 fue posible crearle al dominio jmollagi (ID 90) un conjunto de dominios y sondas. En un principio se creó la estructura en el perfil malicioso:

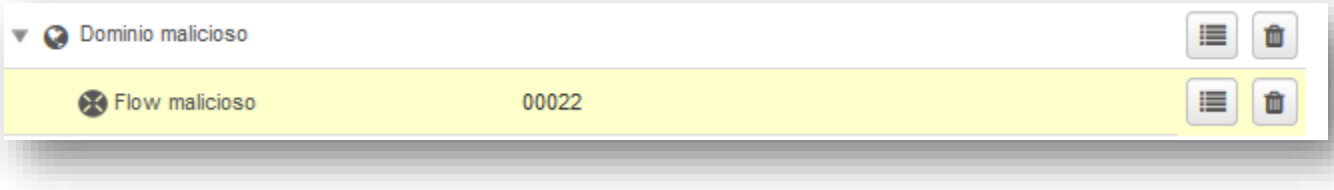


Figura 22. Estructura de dominios de ytrejo

Una vez creada, se exportó el dominio y con ello toda la estructura:

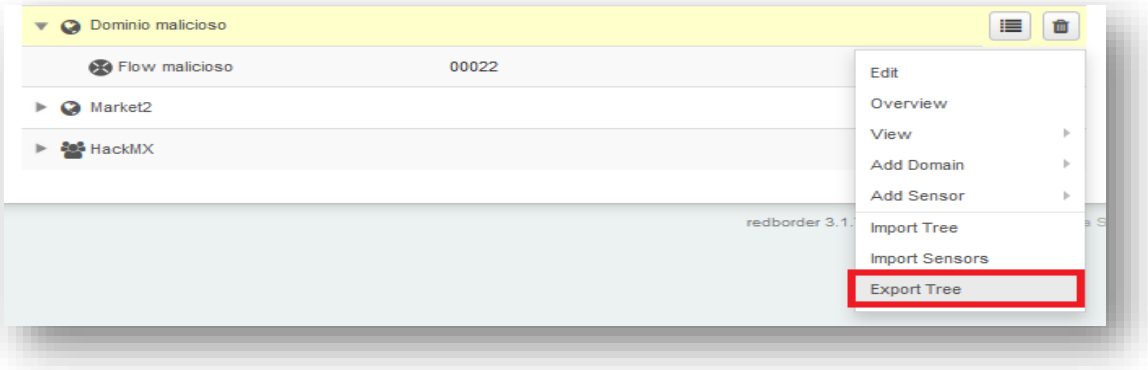


Figura 23. Opción Export Tree del menú de un dominio –sección Sensors-

Y posteriormente, se importó el fichero al dominio de jmollagi sustituyendo el símbolo ? de la siguiente URL https://cloud-01.redborder.com/sensors/?/import_tree por el valor 90.

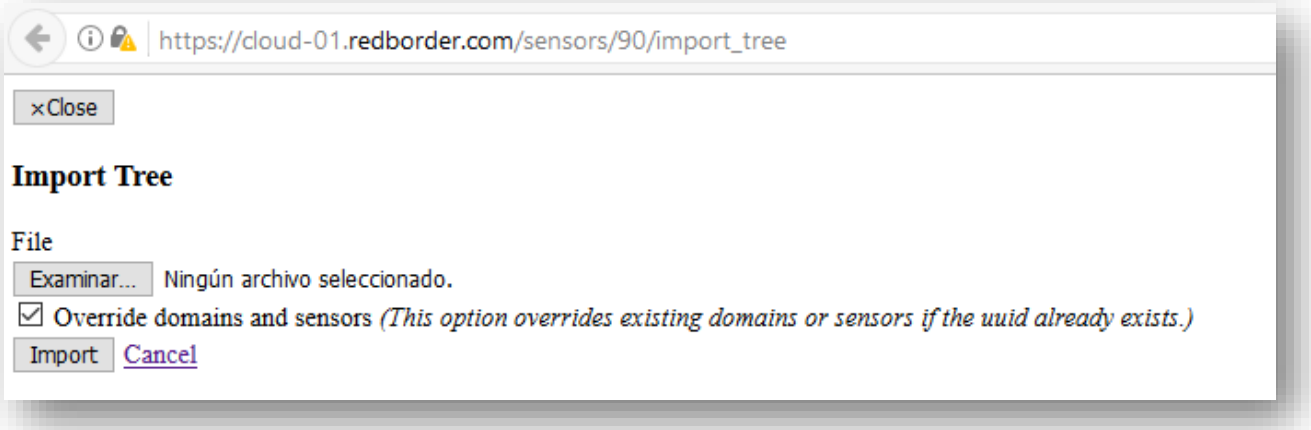


Figura 24. Sección Import tree

Una vez que la estructura se importó, esta desapareció del perfil malicioso. Para comprobar que el dominio jmollagi había creado la estructura de dominios y sondas satisfactoriamente se usaron una de las

vulnerabilidades de la sección 5.1.1 (https://cloud-01.Redborder.com/sensors/90/export_tree):

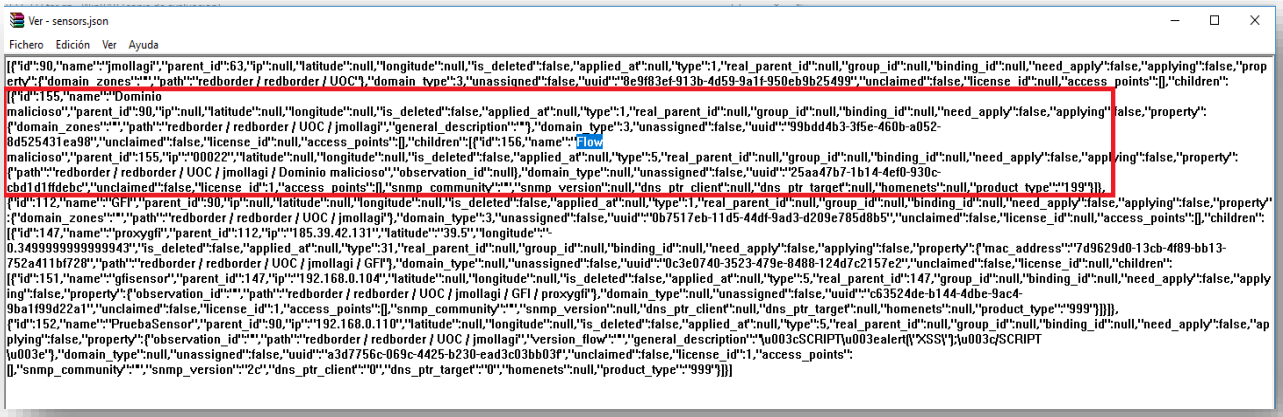


Figura 25. Estructura de dominios y sondas de jmollagi

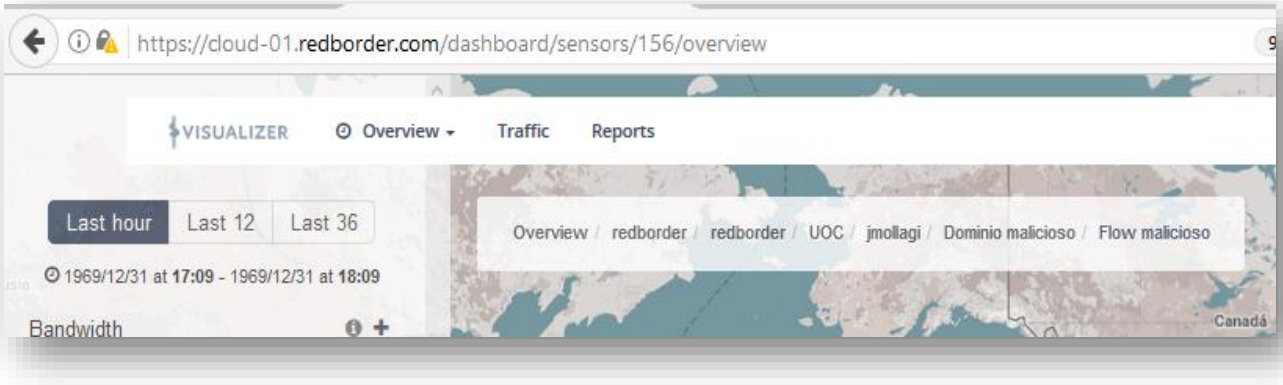


Figura 26. Sección overview de jmollagi

5.1.3. Obtención de la configuración de los dashboards de cualquier usuario

Se detectó una vulnerabilidad de tipo “web parameter tampering” que permite tener acceso a los dashboards de cualquier usuario.

- Modificando la URL https://cloud-01.Redborder.com /dashboard/?/export que se encuentra como enlace de la opción Export Dashboard al editar un Dashboard se pudo tener acceso a la configuración y widgets de todos los dashboards.

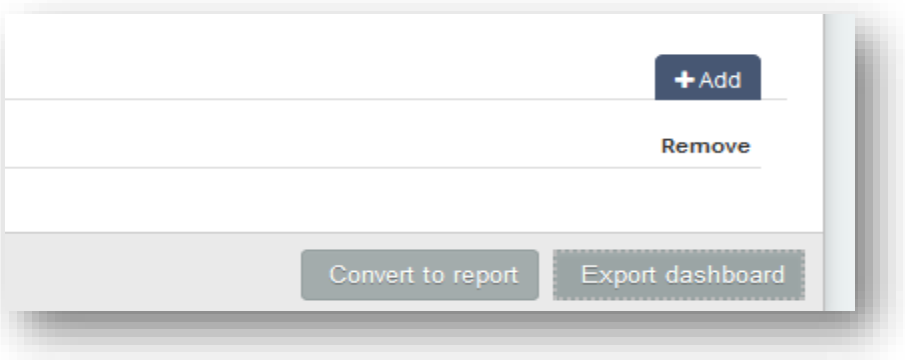


Figura 27. Opción Export- sección editar Dashboard-

Por ejemplo, sutituyendo ? por el valor 189 se pudo obtener el Dashboard Teldat Group.

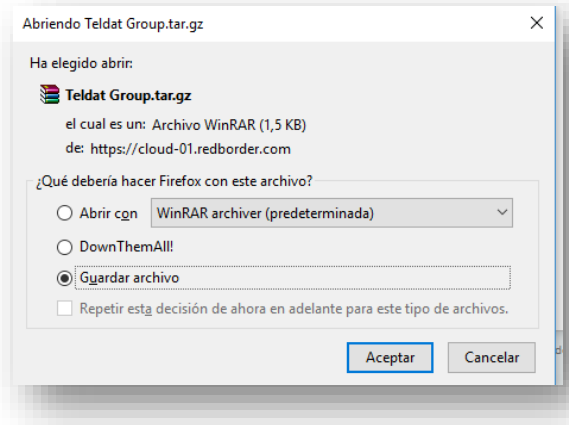


Figura 28. Fichero con cofiguración del dashboard

Figura 29. Contenido del fichero dashboard.json

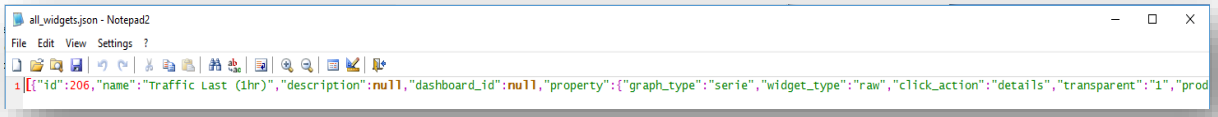


Figura 30. Contenido del fichero all_widgets.json

5.1.4. Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets

A partir de la información obtenida en el apartado anterior se pudieron conocer los widgets presentes en cada dashboard, y por medio de diferentes vulnerabilidades de tipo “web parameter tampering” fue posible crear y eliminar widgets.

- Eliminación de cualquier widget. Por ejemplo, para eliminar el widget de título del dashboard 120, propiedad del usuario ytrejo, primero se descargó el dashboard y se analizó cuál widget era de tipo text:

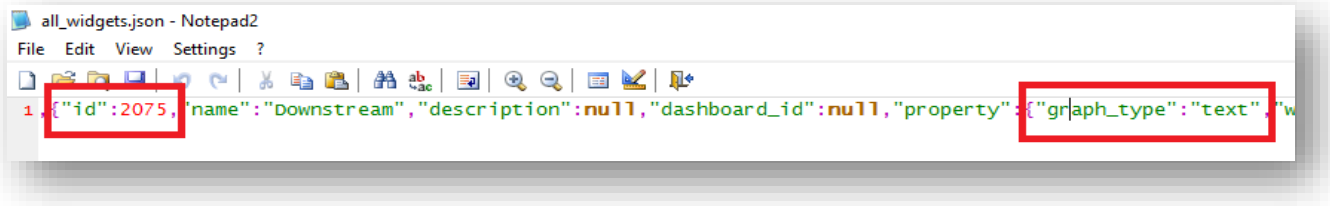


Figura 31. Contenido del fichero all_widget.json

Una vez que se ha analizó, en la URL https://cloud-01.Redborder.com /dashboard/?ID_dashboard/widgets/?ID_widget se sustituyeron los valores de ?ID_dashboard por el valor 120 e ?ID_widget por el valor 2075. Esta URL se encuentra como enlace de la opción Delete de cualquier widget:

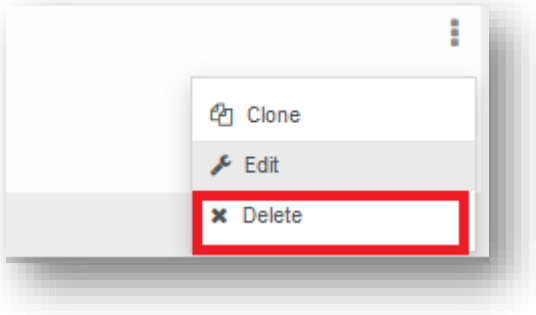


Figura 32. Opción Delete de widget

Una vez que se modificaron los valores, se procedió a eliminar el widget. Se corroboró dicha eliminación empleando la vulnerabilidad de la seción anterior (sección 5.1.3), puesto que con esa vulnerabilida se pudo extraer la configuración y widgets asociados al dasboard ID 120. En este caso, como se tuvo acceso al dashboard de ytrejo se puede corroboar desde la web que el título se eliminó.

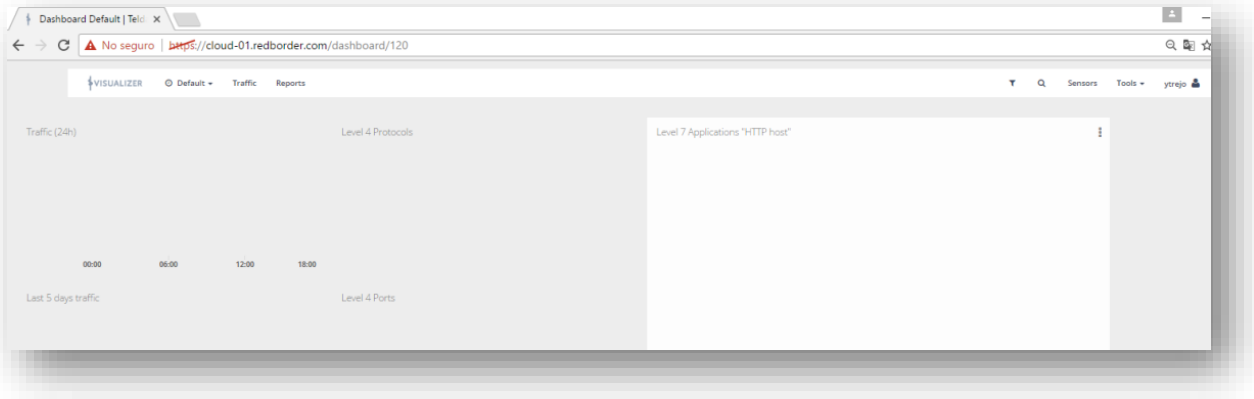


Figura 33. Dashboard de ytrejo

- Creación de un widget en cualquier Dashboard. Se modificó la URL https://cloud-01.Redborder.com/dashboard/?/widgets/list y se reemplazó el valor ? por el ID del dashboard, en este ejemplo, también se usó el dashboard 120, propiedad del usuario ytrejo. La URL anterior se encuentra en la opción Add widget del menú Dashboard.

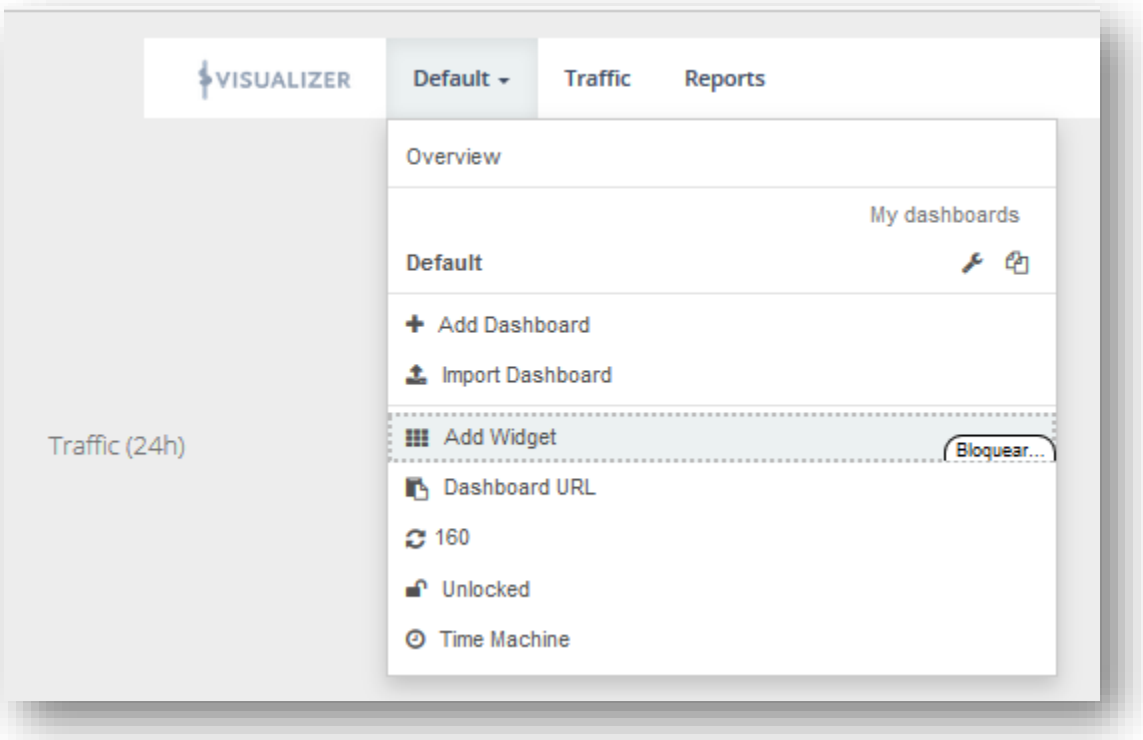


Figura 34. Opción Add widget del menú Dashboard

Y se procedió a crear el widget:

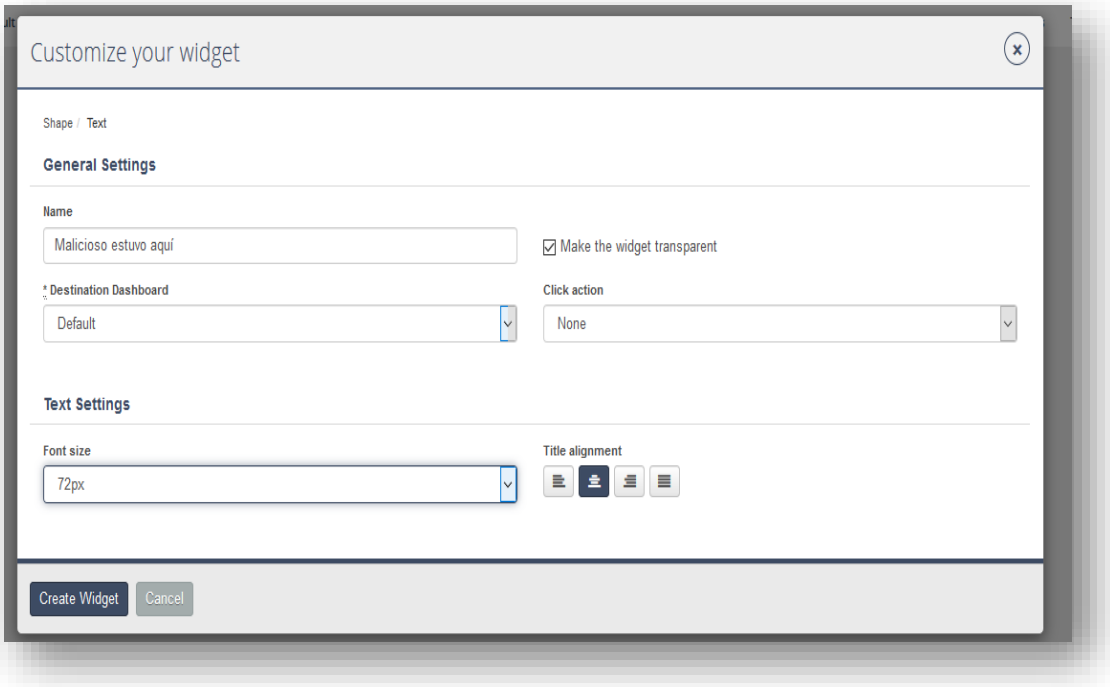


Figura 35. Creación de widget

Dado que se tenía acceso a la cuenta del usuario ytrejo, se pudo comprobar fácilmente la existencia del widget ingresando al dashboard ID 120:

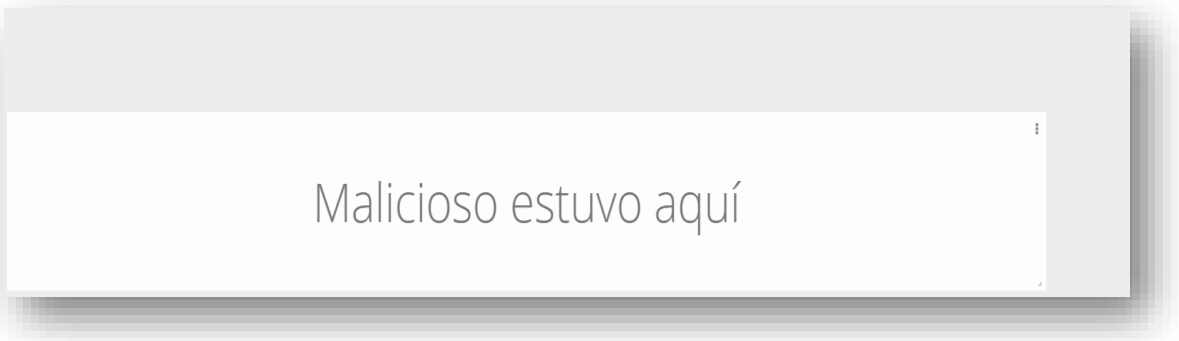


Figura 36. Widget del dashboard de ytrejo

- Creación de un widget en cualquier reporte. Se modificó la URL https://cloud-01.Redborder.com/reports/?ID_reporte/widgets /list?page=1 y se reemplazó el valor ?ID_reporte por el ID del reporte, en este ejemplo se usó el reporte 75 (propiedad del usuario ytrejo). La URL anterior se encuentra en la opción Add block al abrir un reporte

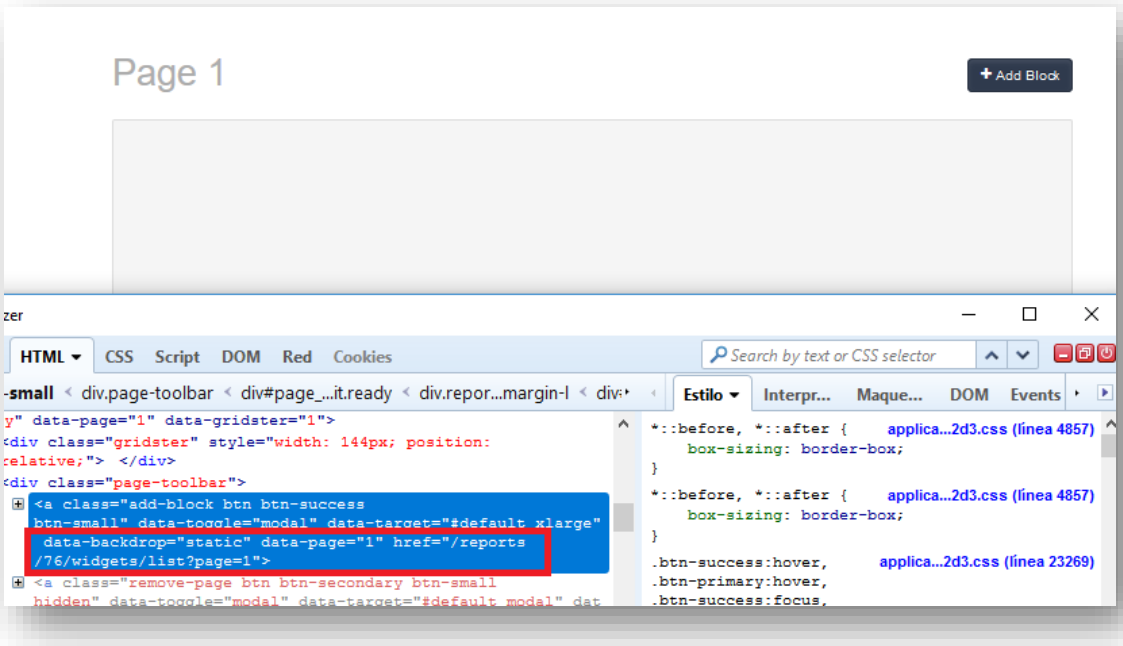


Figura 37. Edición del botón Add Block

Y se generó el widget:

Figura 38. Creación del widget malicioso

Al ingresar al reporte ID 75 se pudo apreciar que el widget fue creado exitosamente:

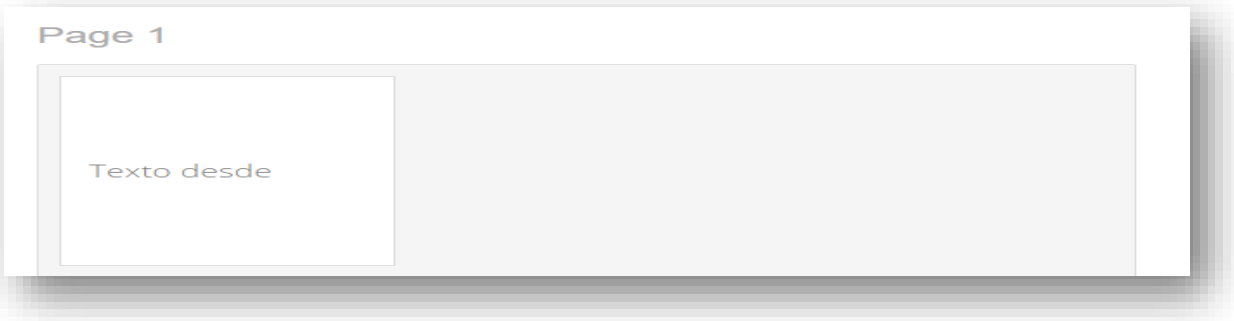


Figura 39. Widget malicioso creado

5.1.5. Obtención de los ID's de los usuarios activos en la solución

Se detectaron vulnerabilidades de tipo "Information exposure through an error message". Sustituyendo el símbolo ? por valores numéricos en la siguiente dirección URL https://cloud-01.Redborder.com/users/?/edit fue posible saber que ID's están activos.

La URL se encuentra en la sección Users del recuadro Editar

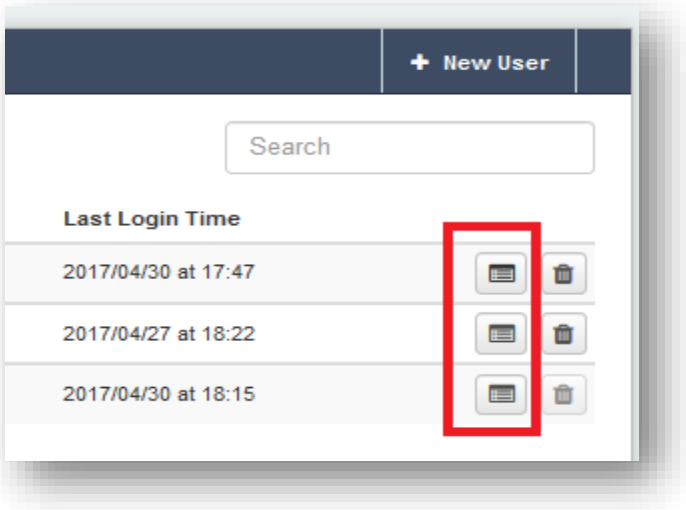


Figura 40. Sección users

Por ejemplo, cuando se intentó editar el usuario con el ID 9 apareció el siguiente mensaje:

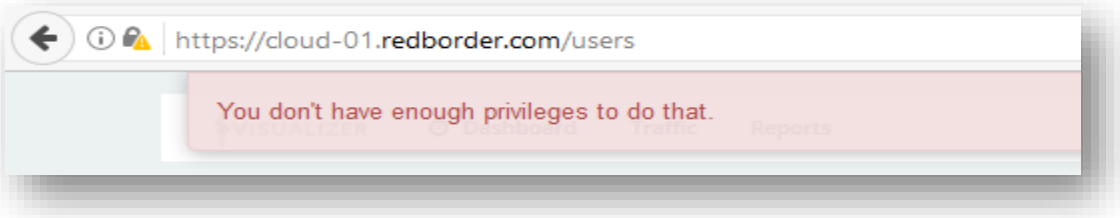


Figura 41. Mensaje de error cuando no existe el usuario

Y cuando no hubo ningún usuario asociado, apareció el siguiente mensaje:

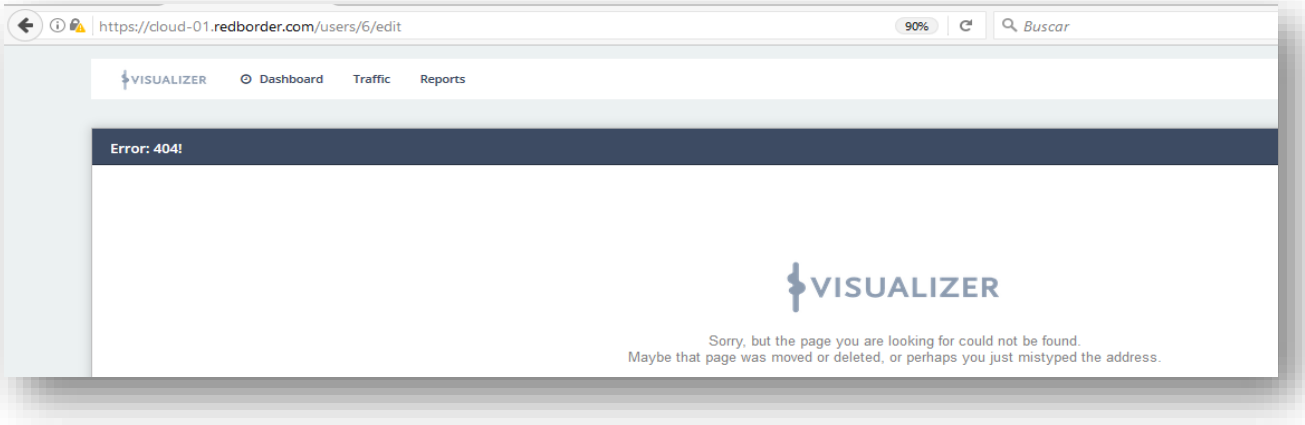


Figura 42. Mensaje de error cuando existe el usuario

5.1.6. Obtención del listado de todos los usuarios

Se detectaron vulnerabilidades de tipo “web parameter tampering” que permiten tener acceso al listado de usuarios de Redborder.

- Modificando los valores de los atributos data-userid y value (del campo “dashboard[collaborators][][user_id]”) de las secciones editar o crear un Dasboard fue posible obtener el nombre de los usuarios activos.

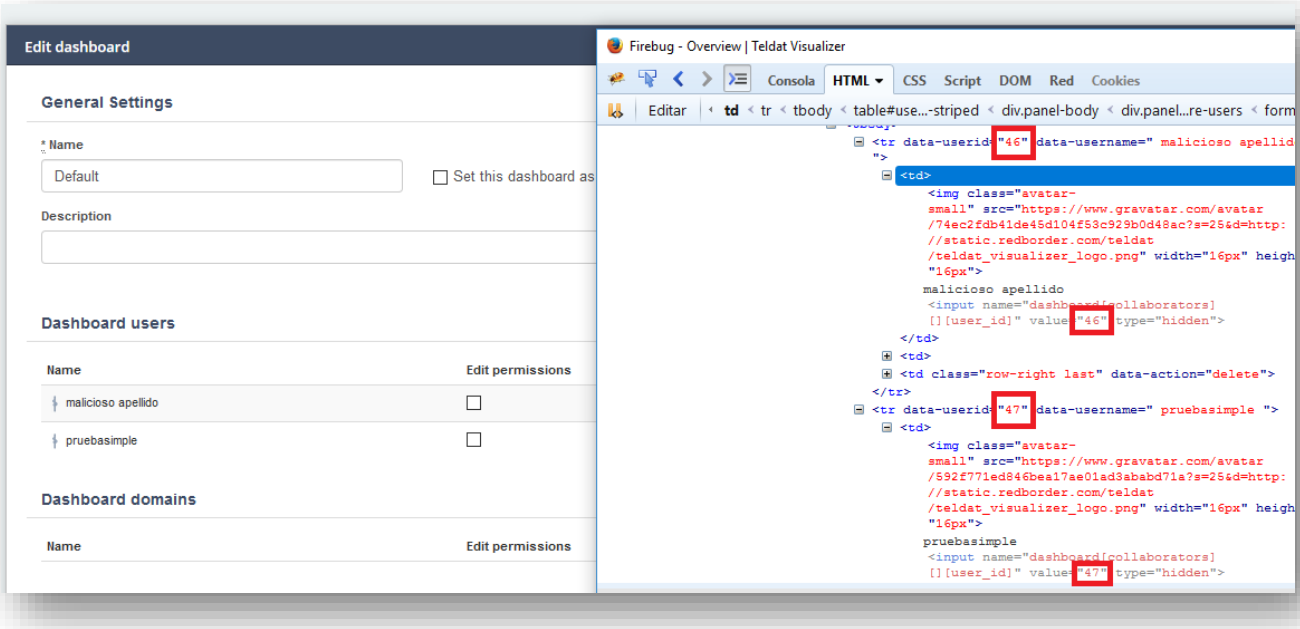


Figura 43. Sección editar dashboard

Por ejemplo, sustituyendo los ID's de los usuarios malicioso y pruebasimple por ID's válidos divulgados usando la vulnerabilidad anterior , en este ejemplo los ID's del 1 al 5, fue posible obtener los siguientes nombres de usuarios:

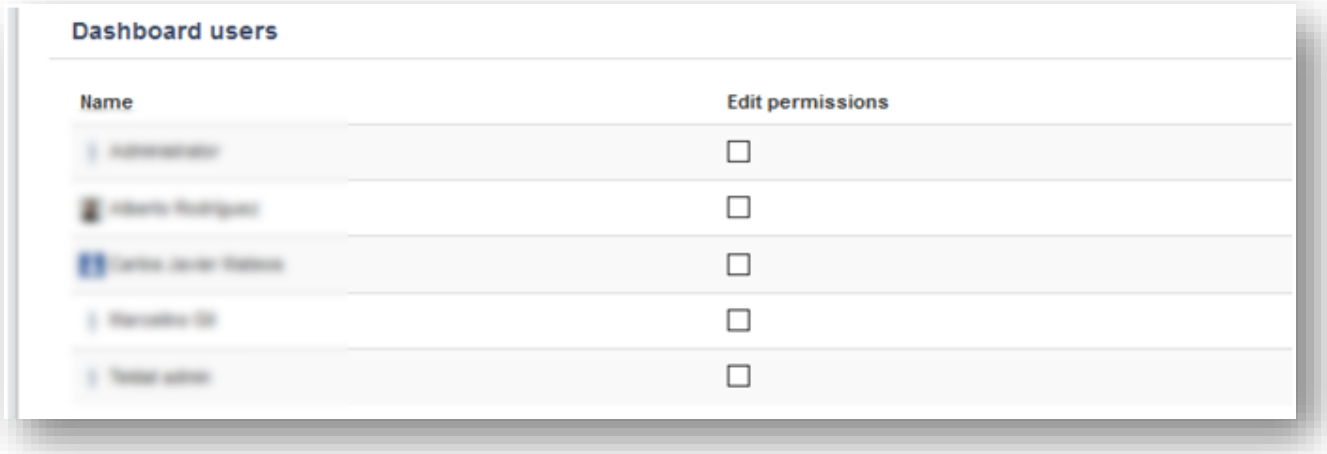


Figura 44. Divulgación de usuarios ID 1 al 5

- También modificando los valores de los atributos data-userid y value (del campo "report[collaborators][][user_id]") de las secciones editar o crear un Reporte fue factible obtener los nombres de los usuarios de la solución Redborder

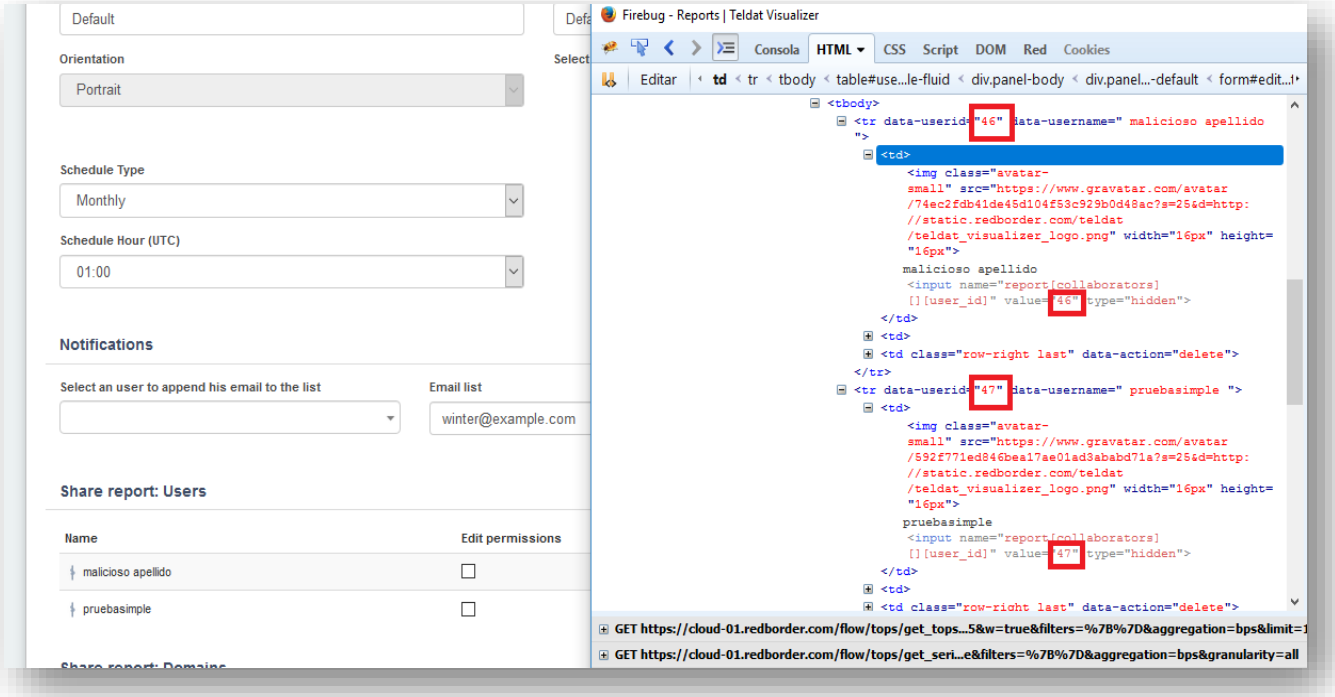


Figura 45. Modificación de reporte para obtener nombres de usuarios

Sustituyendo los ID's de los usuarios malicioso y pruebasimple por los ID's activos 9,10,12,13,14,15, y posteriormente guardando los cambios, se pudieron obtener los nombres de los usuarios asociados a esos ID's:

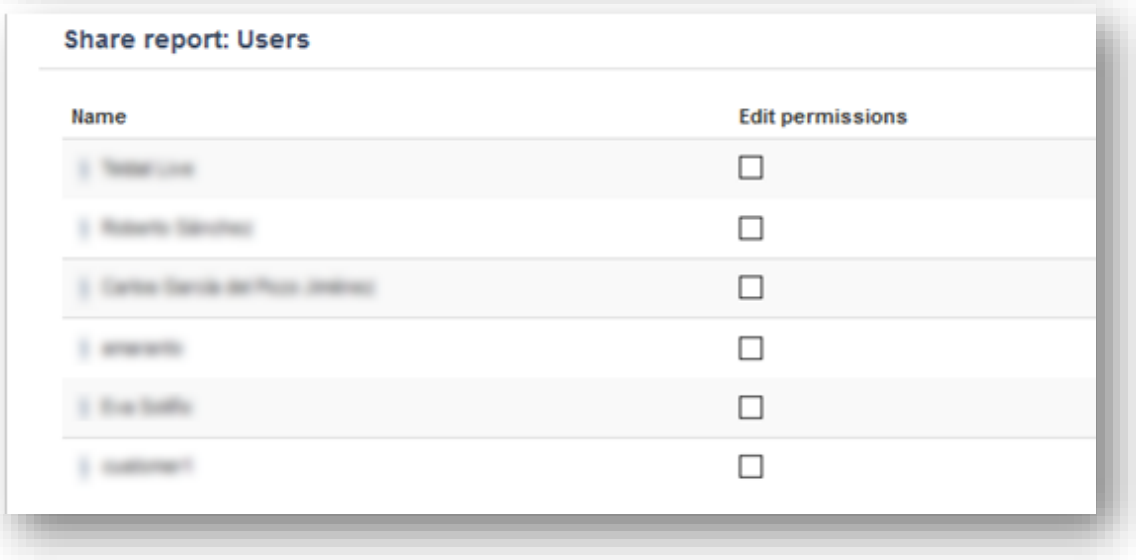


Figura 46. Divulgación de usuarios ID's 9, 10, 12, 13, 14, 15

5.1.7. Eliminación de las notificaciones de todos los usuarios

Se detectó una vulnerabilidad de tipo "web parameter tampering" que permite eliminar todas las notificaciones de cualquier usuario.

- Modificando la URL https://cloud-01.Redborder.com/notifications/? que se encuentra como enlace de la opción Delete de cada una de las notificaciones se pudieron eliminar notificaciones de cualquier usuario.

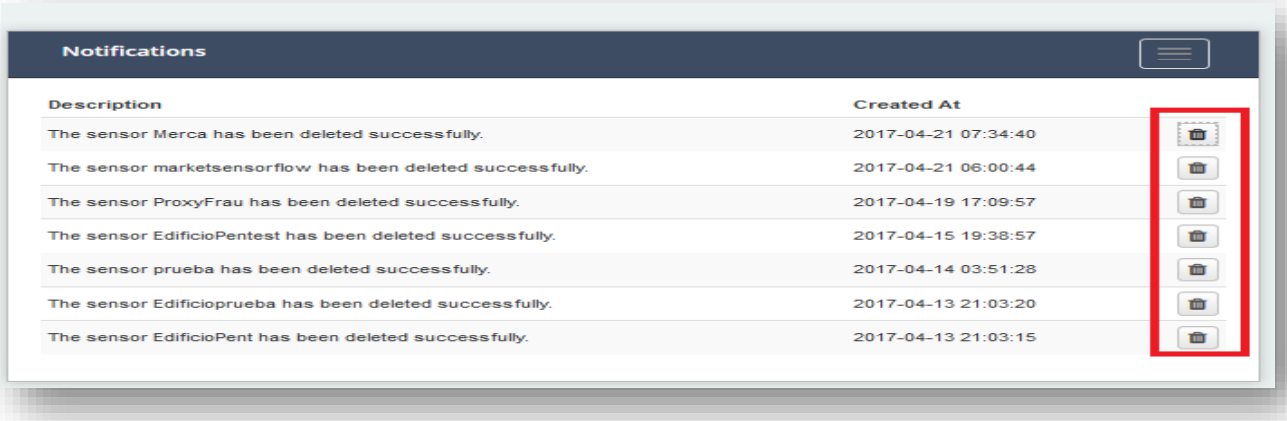


Figura 47. Sección Notifications

Por ejemplo, reemplazando ? por los valores 32, 29 y 25 y ejecutando el botón Delete se eliminaron las primeras tres notificaciones del usuario ytrejo.

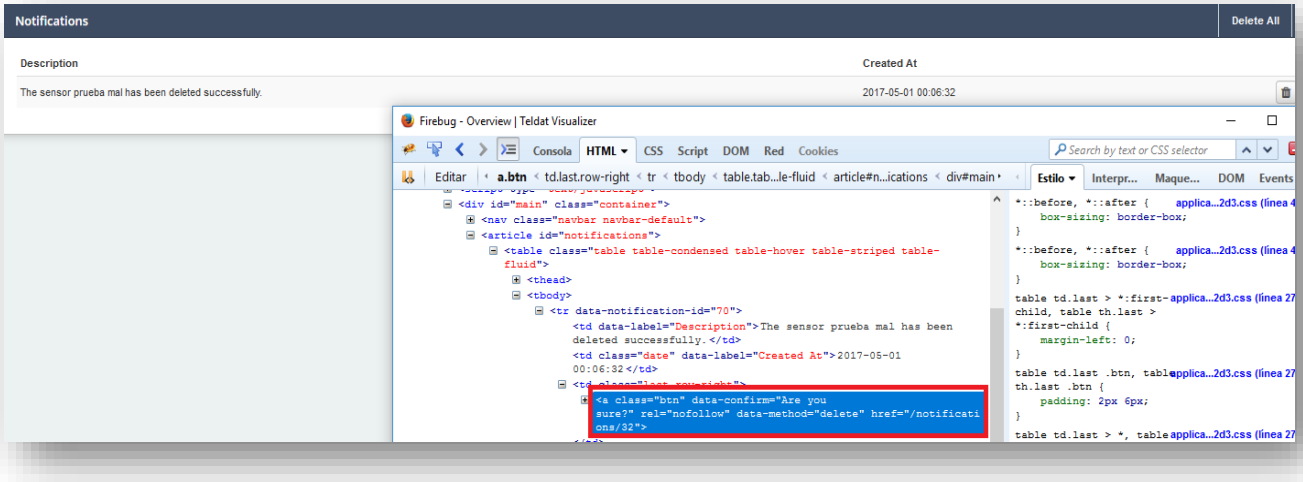


Figura 48. Modificación de código -sección Notifications-

Como se tuvo acceso a la cuenta del usuario ytrejo, fue posible comprobar que las notificaciones desaparecieron:

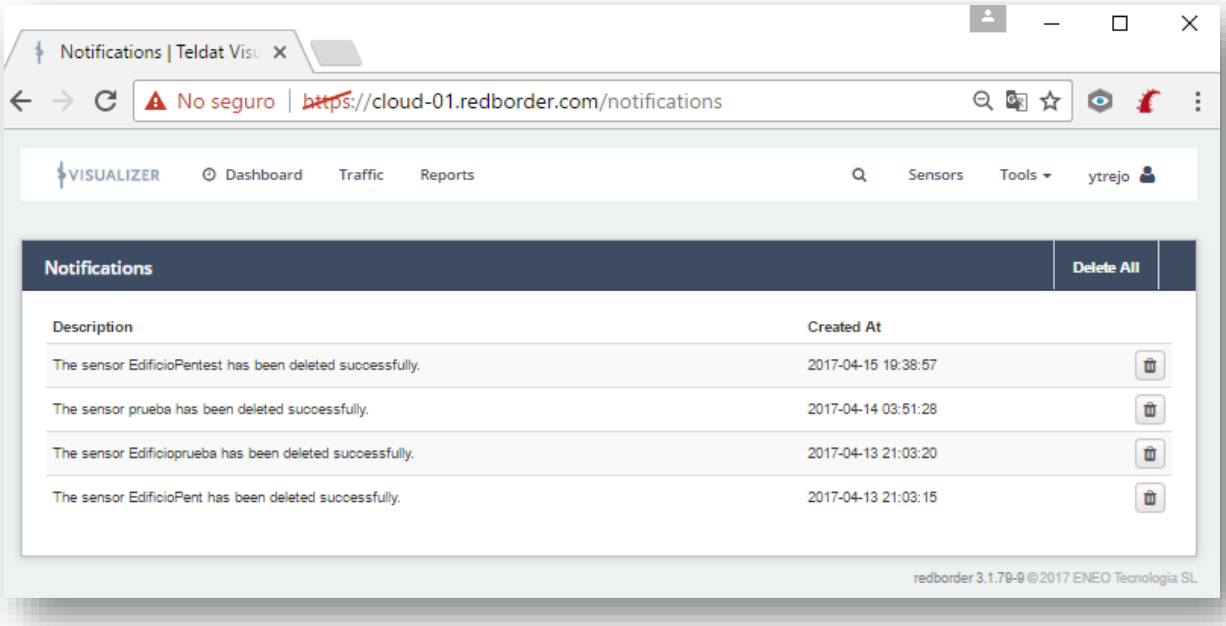


Figura 49. Sección notifications de usuario ytrejo

5.1.8. Carga de ficheros maliciosos a las cuentas de todos los usuarios

A partir de los formularios para cargar widgets de tipo imagen, los cuales se encuentran en las secciones Reports y Dashboard, es factible subir ficheros maliciosos a la cuenta de cualquier usuario, es decir, estos formularios presentan la vulnerabilidad: “Unrestricted File Upload”. Mediante esta vulnerabilidad se pudieron llevar a cabo los siguientes ataques:

- Ataque XSS persistente. Por ejemplo, desde el usuario malicioso se subió un widget de tipo image al usuario ytrejo usando la vulnerabilidad descrita en la sección 5.1.4. En la siguiente imagen se puede apreciar cómo se modificó la URL para que se pudieran crear widgets en el dashboard 120.

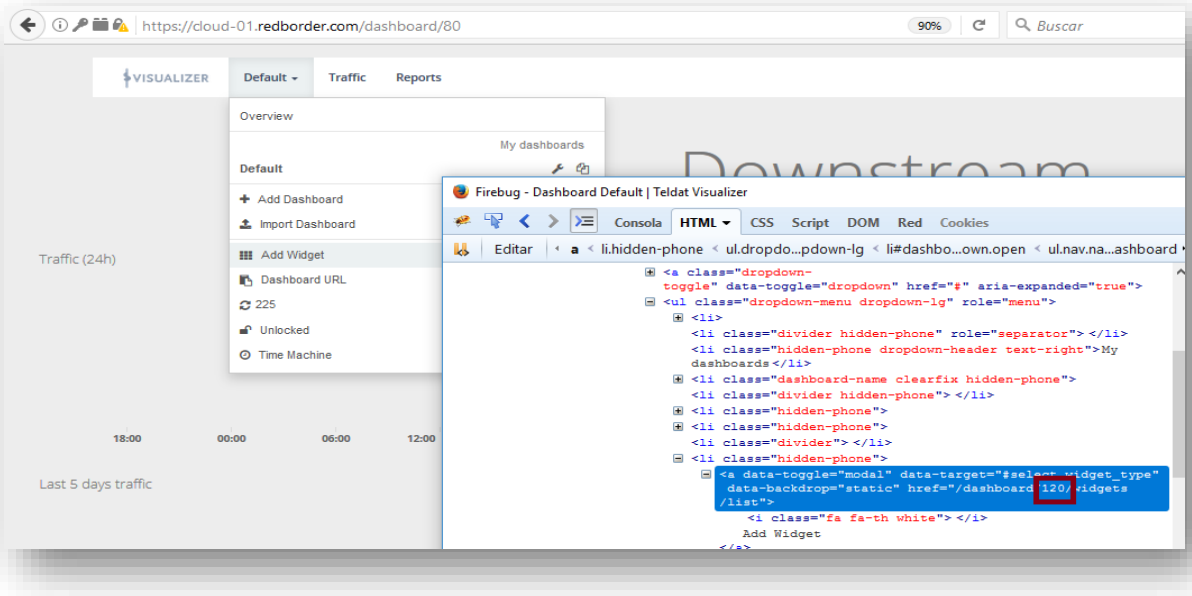


Figura 50. Modificación de widget de usuario ytrejo

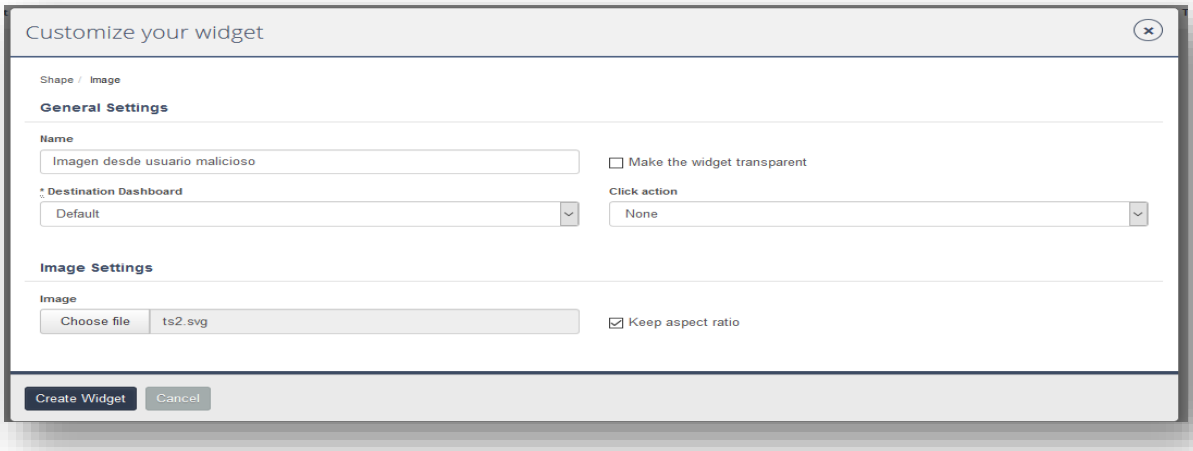


Figura 51. Creación de widget malicioso

Una vez que se creó el widget, este se pudo visualizar desde el dashboard de ytrejo.

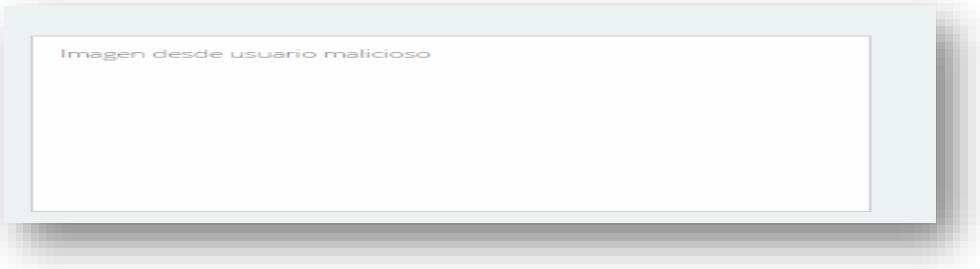


Figura 52. Widget malicioso creado

Al momento de abrir la URL de la imagen el XSS se ejecutó de forma automática:

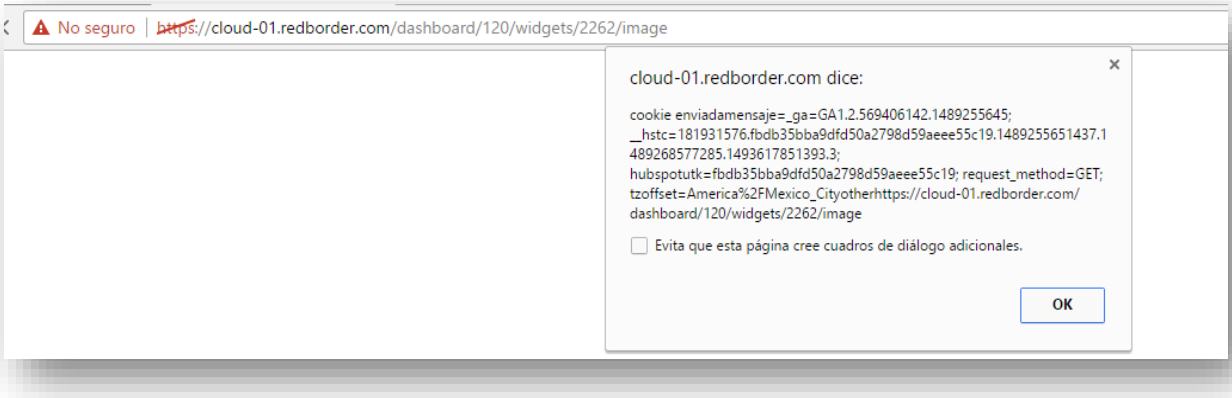


Figura 53. Ejecución del widget malicioso

- Inyección de malware. Desde el usuario malicioso fue viable subir un widget de tipo image a x usuario usando la vulnerabilidad descrita en la sección 5.1.4. Por ejemplo, se pudo cargar una imagen con un payload malicioso (malware) al reporte 75 del usuario ytrejo

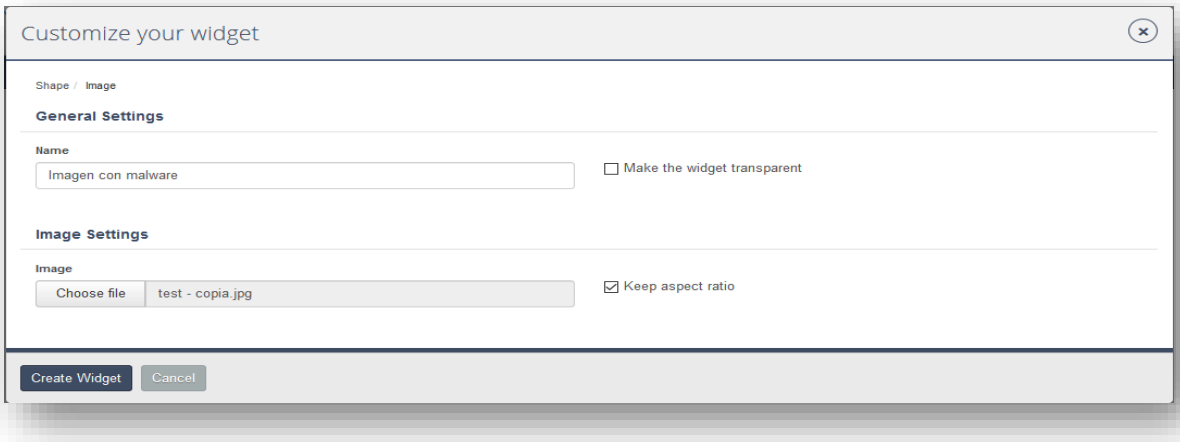


Figura 54. Imagen maliciosa

Al ingresar desde la cuenta de ytrejo a la sección de edición de Reporte se observó que la imagen se cargó con éxito:

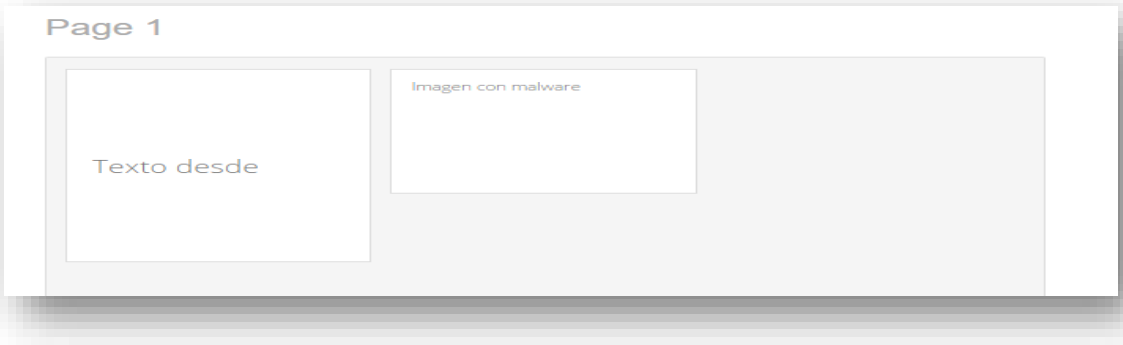


Figura 55. Reporte modificado

Se utilizó un editor hexadecimal para verificar que el PDF embebió el payload malicioso que venía en la imagen:

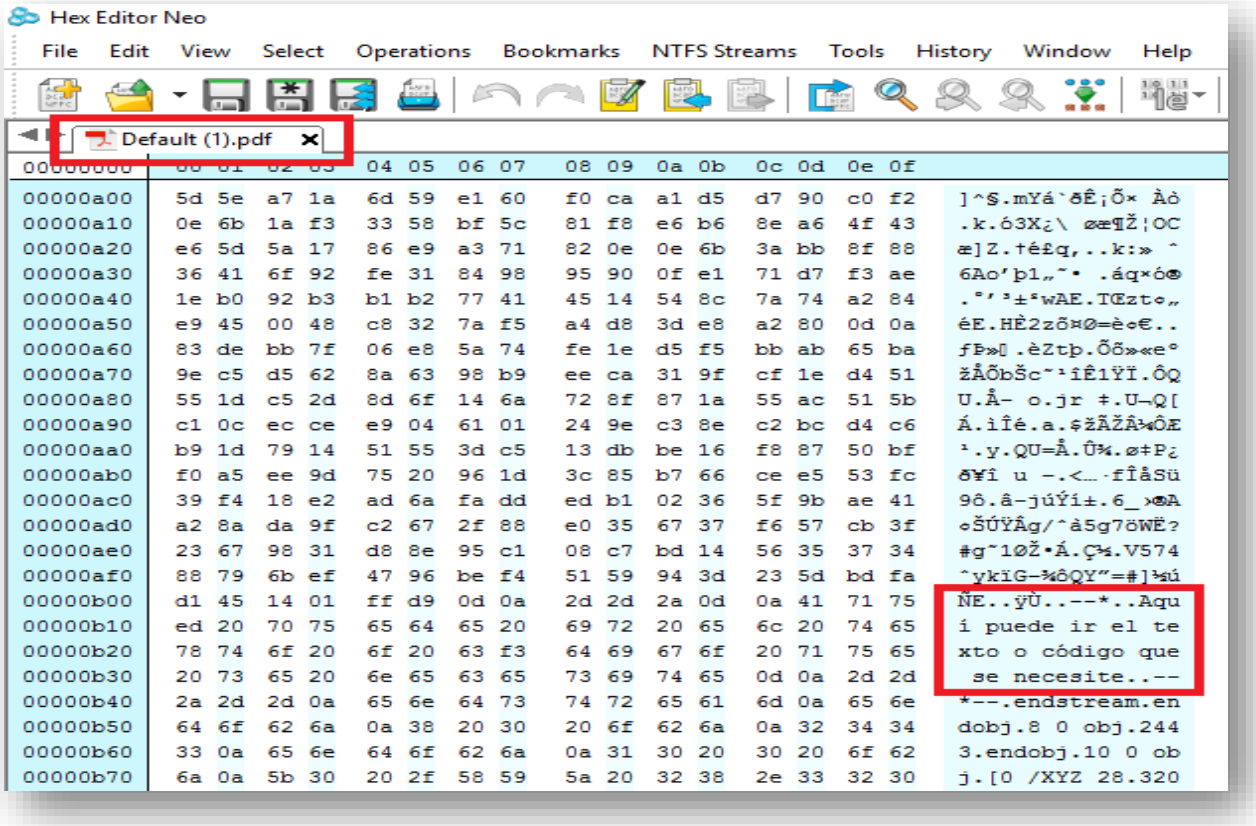


Figura 56. Editor hexadecimal

Estos reportes son una excelente vía para la propagación de malware puesto que son enviados a los correos electrónicos de los clientes de forma periódica y además no generan desconfianza ya que en un inicio fueron generados por los propios usuarios para que la plataforma se los enviara.

5.1.9. Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario

A partir de las vulnerabilidades descritas en la sección 5.1.4 fue posible crear un widget de tipo URL a cualquier usuario, lo que a su vez llevó a los siguientes ataques:

- Ataque XSS persistente. Con esta vulnerabilidad, las imágenes maliciosas descritas en la sección anterior 5.1.8 ya no necesitaron que el usuario abriera el enlace por medio de un ataque de ingeniería social, puesto que el XSS se pudo ejecutar al momento de abrir cualquier dashboard.
  Por ejemplo, desde la cuenta del usuario malicioso se creó un widget de tipo URL al dashboard ID 120 de ytrejo. Esta dirección URL contenía el enlace a la imagen maliciosa generada en la sección anterior.

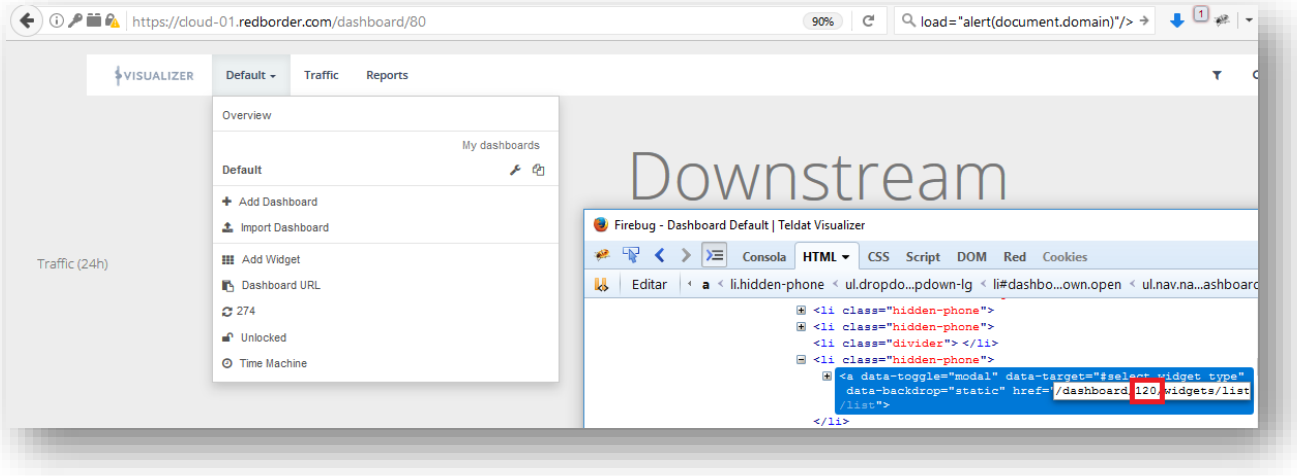


Figura 57. Dashboard del usuario malicioso

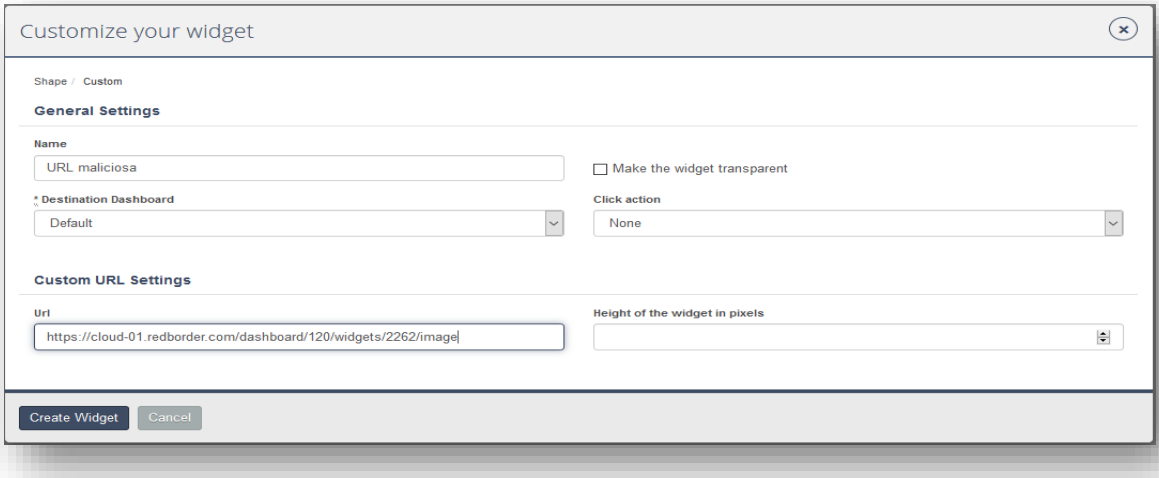


Figura 58. Dirección URL maliciosa

En el momento en que el usuario ytrejo abrió el dashboard, automáticamente se ejecutó el XSS.

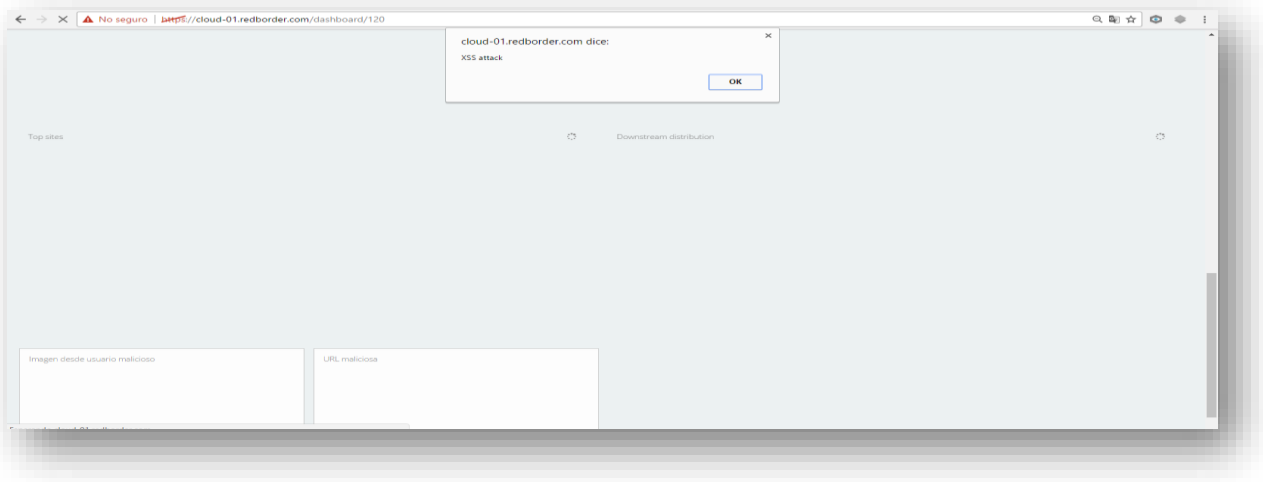


Figura 59. Ejecución del XSS en el dashboard de ytrejo

- Ataque DDOS. A partir del XSS se pudo haber generado un ataque recursivo que llevara al consumo de los recursos del servidor. Por ejemplo, el fichero malicioso pudo redireccionarse a los dashboards comprometidos.
- Redireccionamiento a URL maliciosa. El widget pudo haber redireccionado a una URL maliciosa con la apariencia de Redborder versión cloud, etc.
- Defacement. A partir del XSS se pudo haber intentado un ataque para modificar la apariencia del dashboard.
- Descarga de ficheros maliciosos: La URL pudo haber contenido un enlace a un fichero malicioso, para que cada que se visiten los dashboards se realice la descarga.

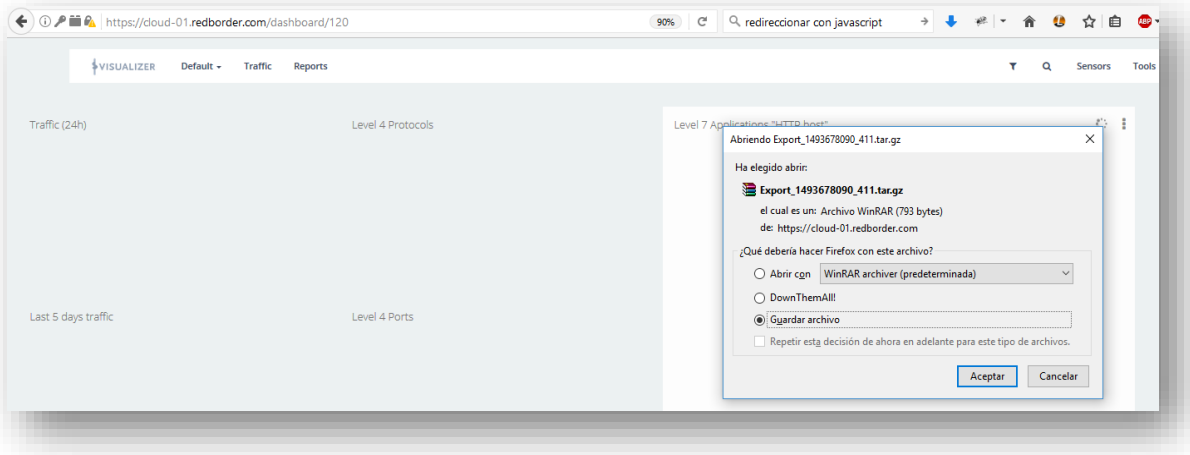


Figura 60. Ejecución de la URL maliciosa desde dashboards

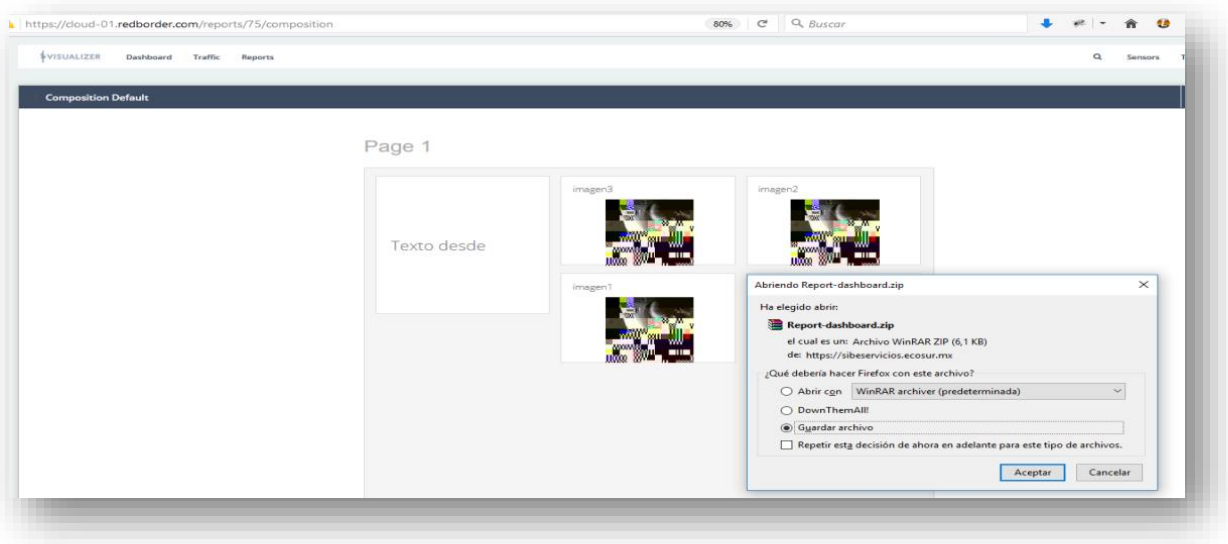


Figura 61. Ejecución de la URL maliciosa desde la sección Composition Default de Reports

5.1.10. Edición y borrado de alarmas

Se detectaron vulnerabilidades de tipo “web parameter tampering” que permiten modificar y borrar alarmas de cualquier usuario:

- Modificando la URL https://cloud-01.Redborder.com/alarms/?/edit que se encuentra como enlace de la opción Modificar alarma de la sección Alarms se pudo tener acceso a la configuración de alarmas de otros usuarios.

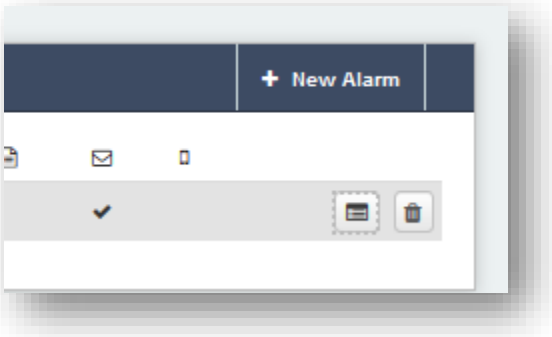


Figura 62. Opción Modificar alarma –sección Alarms-

Por ejemplo, reemplazando ? por el valor 38 se tuvo acceso a la alarma ngil test del usuario xxx, y también a su cuenta de email

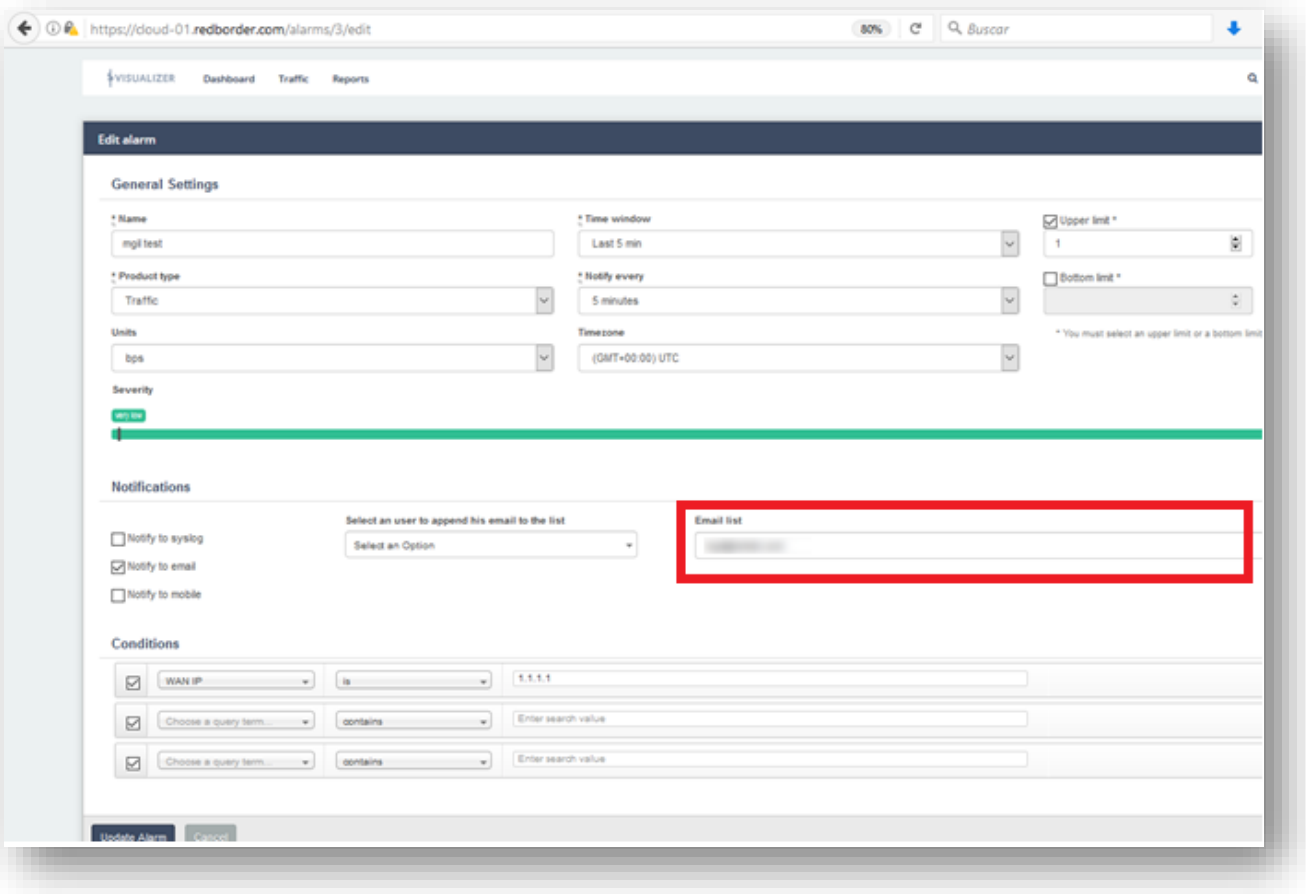


Figura 63. Acceso a alarma de cliente

- Modificando la URL https://cloud-01.redborder.com/alarms/?
  que se encuentra como enlace de la opción Delete de cada una de las alarmas fue posible eliminar alarmas de cualquier usuario.

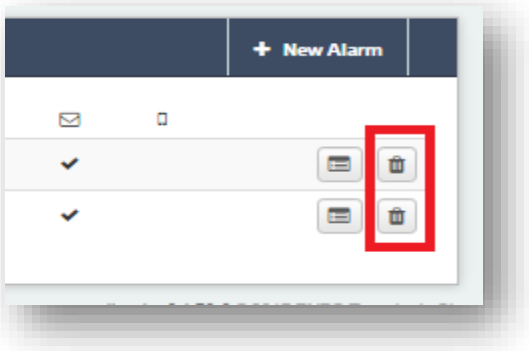


Figura 64. Opción Delete de sección Alarms

Por ejemplo, apoyándose de la información obtenida en la vulnerabilidad anterior, reemplazando ? por el valor de 10 y ejecutando el botón Delete se eliminó la alarma flujo del usuario ytrejo.

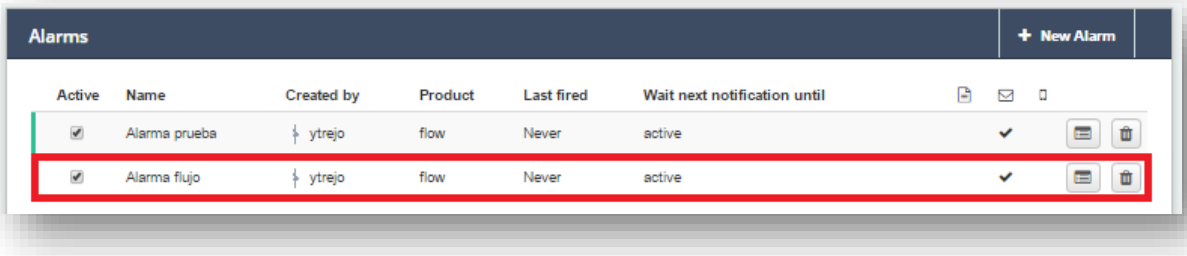


Figura 65. Alarmas de ytrejo

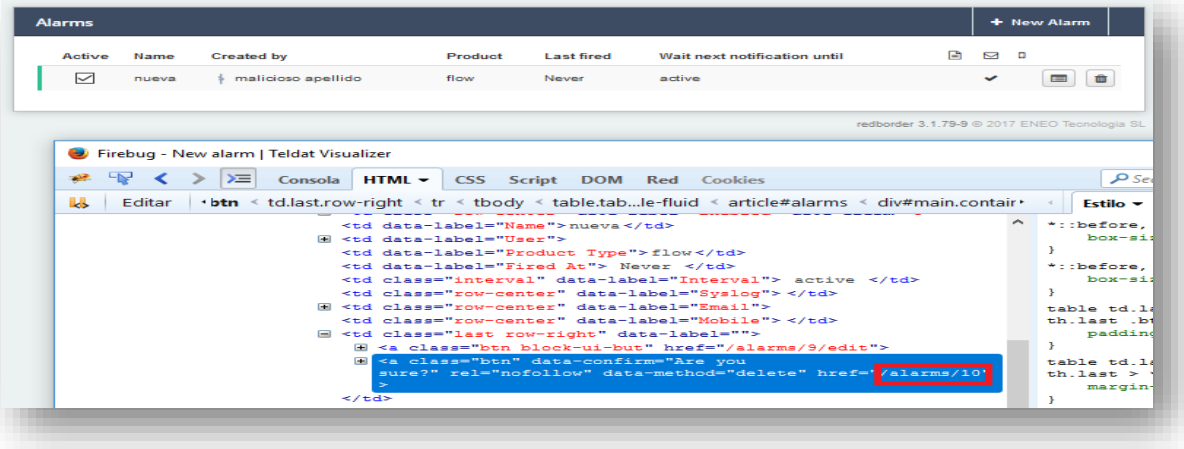


Figura 66. Borrado de alarma de ytrejo desde cuenta de usuario malicioso

5.1.11. Creación de dominios de distintos tipos (diferentes de los habilitados)

Se detectó una vulnerabilidad de tipo “web parameter tampering” que permite agregar dominios de diferente tipo:

- Modificando el valor del atributo value del campo “sensor[domain_type]” que se despliega al crear una sonda, se pudieron generar diferentes tipos de dominios

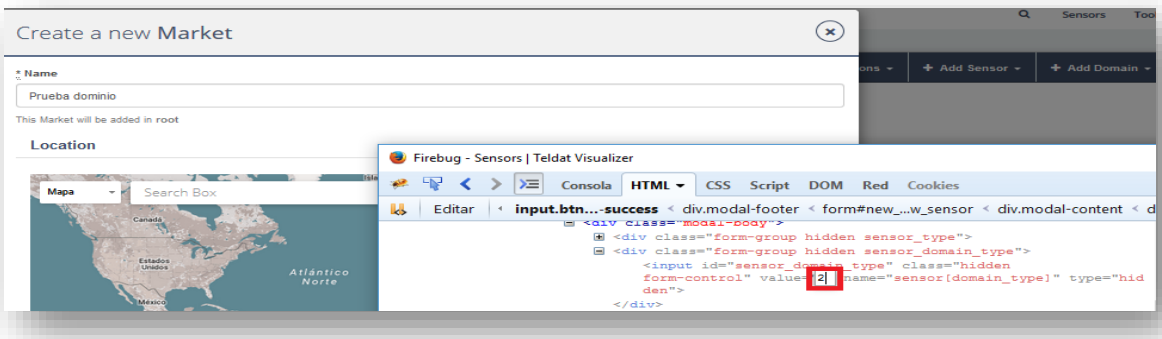


Figura 67. Creación de un dominio – distinto de los tipos habilitados-

En la siguiente imagen se puede apreciar la variedad de tipos de dominio creados:

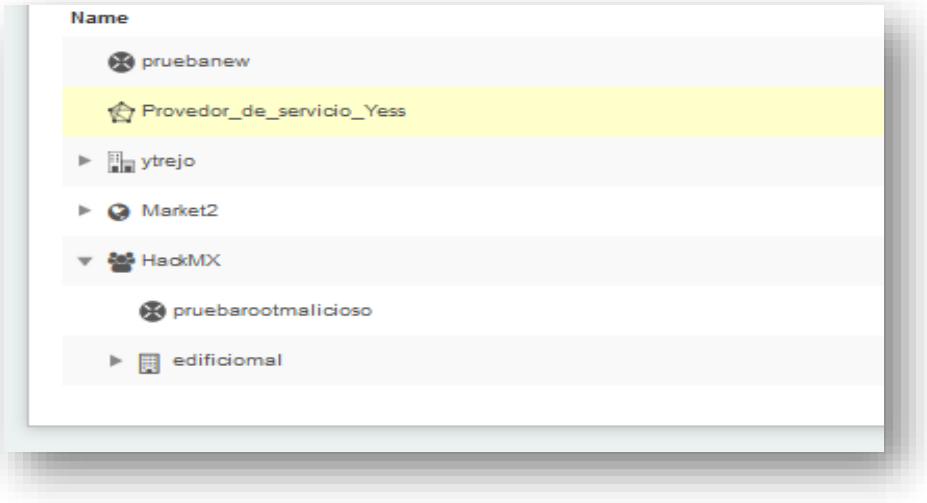


Figura 68. Dominios creados

5.1.12. Divulgación de IP's locales

Por medio de la herramienta de escaneo Nessus se detectó una vulnerabilidad del tipo "Web Server HTTP Header Internal IP Disclosure", donde se pudo extraer la siguiente dirección IP 10.1.5.40:

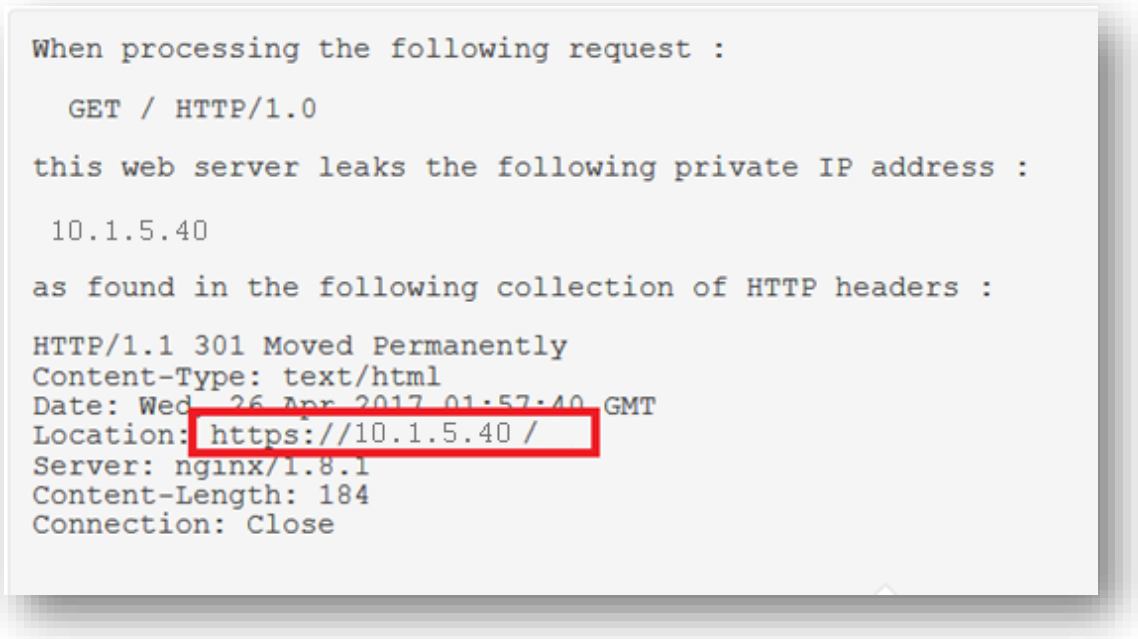


Figura 69. Divulgación de IP local

5.1.13. Ataques de downgrade, SSL-stripping man-in-the-middle attacks y secuestro de cookies

Las herramientas de escaneo Nessus y Burp Suite Professional detectaron una vulnerabilidad de tipo “HSTS Missing From HTTPS Server”. La falta de HSTS permite ataques de downgrade, SSL-stripping man-in-the-middle attacks y debilita las protecciones para evitar los secuestros de cookies.

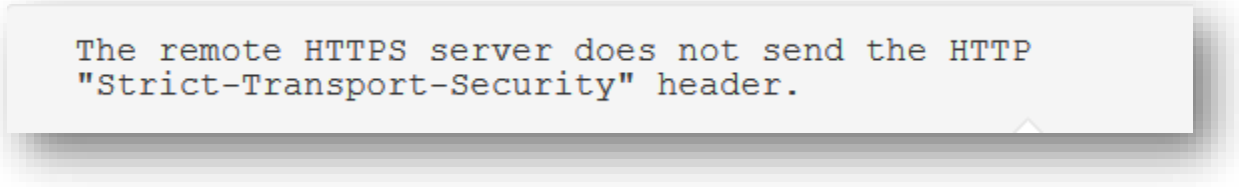


Figura 70. Mensaje de falta de cabecera HSTS

5.1.14. Divulgación de dominios no oficiales

A través de las herramientas de escaneo Nessus y Burp Suite Professional se detectó una vulnerabilidad de tipo “SSL Certificate commonName Mismatch”. Estas herramientas arrojaron otros dominios asociados al sitio:

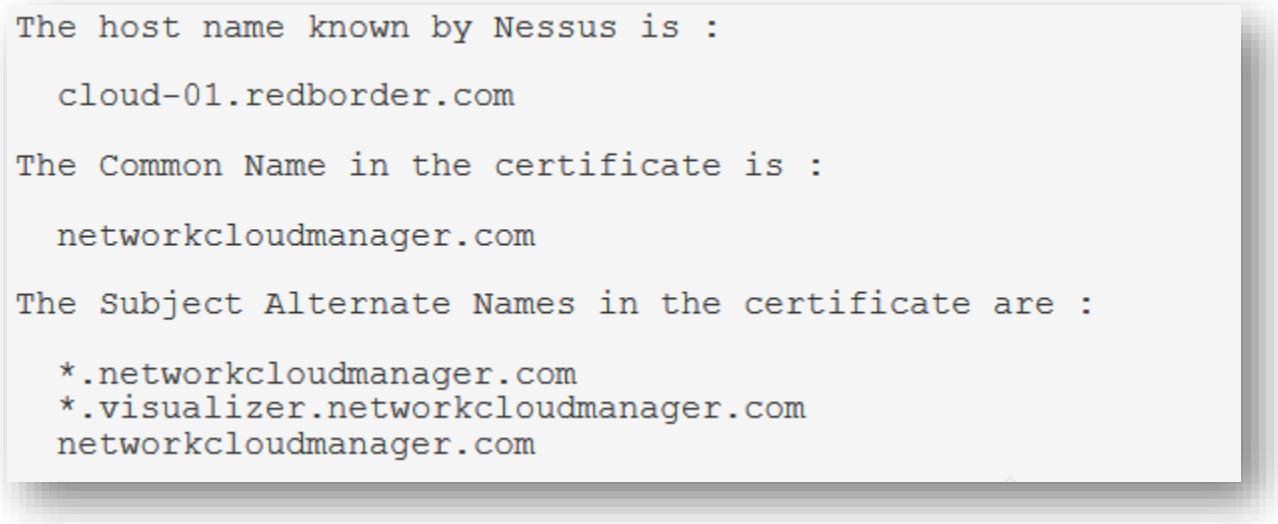


Figura 71. Dominios no oficiales

De los cuales se corroboró la existencia del dominio https://visualizer.networkcloudmanager.com/users/login

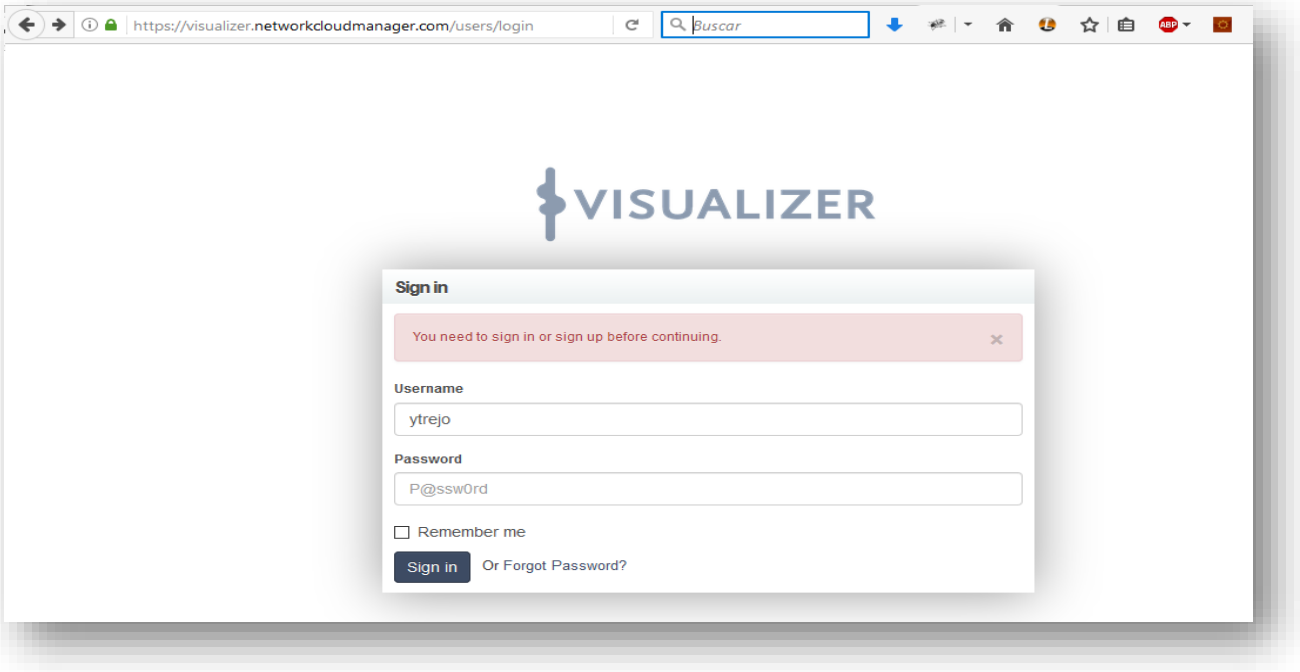


Figura 72. Dominio visualizer.networkcloudmanager.com

5.1.15. Almacenamiento de información confidencial en la memoria caché local

Por medio de Burp Suite Professional se detectó una vulnerabilidad de tipo "Cacheable HTTPS response". Si la información confidencial en las respuestas de la aplicación se almacena en la memoria caché local, ésta puede ser recuperada por otros usuarios que tengan acceso a la misma computadora en el futuro.

El servidor web debería devolver los siguientes encabezados HTTP en todas las respuestas que contengan contenido sensible:

- Cache-control: no-store
- Pragma: no-cache

5.1.16. Obtención de credenciales a través del formulario de inicio de sesión con autocomplete habilitado

Las credenciales almacenadas pueden ser capturadas por un atacante que gane el control sobre la computadora del usuario. Además un atacante, a través de un XSS, podría recuperar las credenciales almacenadas en el navegador del usuario.

5.2. En el dominio live.redborder.com

5.2.1. Divulgación de ID's de organizaciones activas

Se detectó una vulnerabilidad de tipo "Information exposure through an error message". Sustituyendo el símbolo ? de la siguiente dirección URL https://live.redborder.com/organizations/? por valores numéricos fue posible saber que ID's están activos. La URL se encuentra en la sección Organization

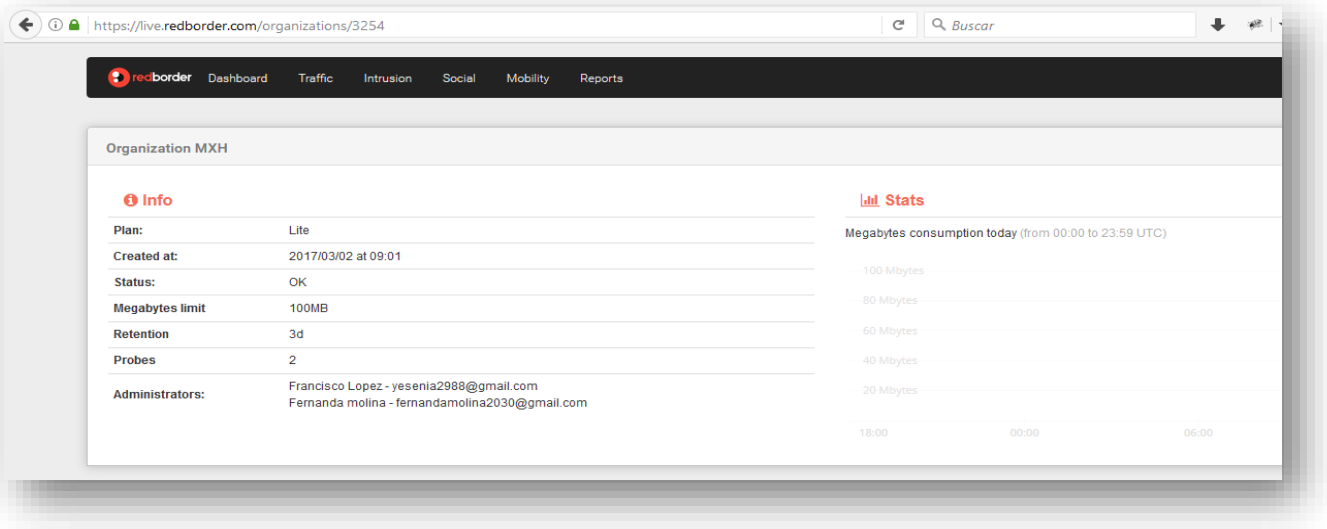


Figura 73. Sección organizations

Por ejemplo, al intentar editar la organización con ID 3253 apareció el siguiente mensaje de error: Error 500

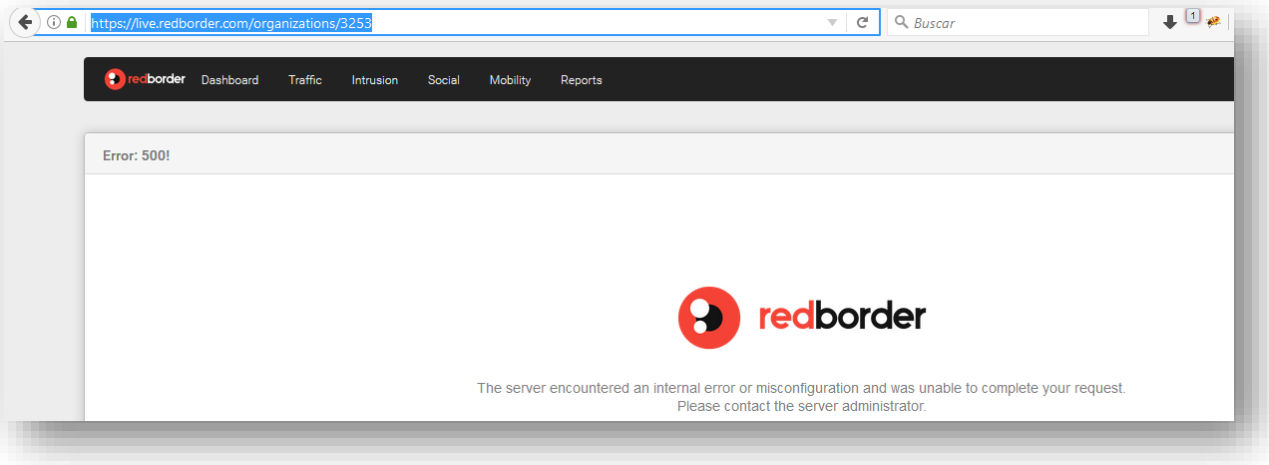


Figura 74. Error 500 desplegado cuando la organización existe

Y cuando no hubo ninguna organización asociada, apareció el mensaje de error 404:

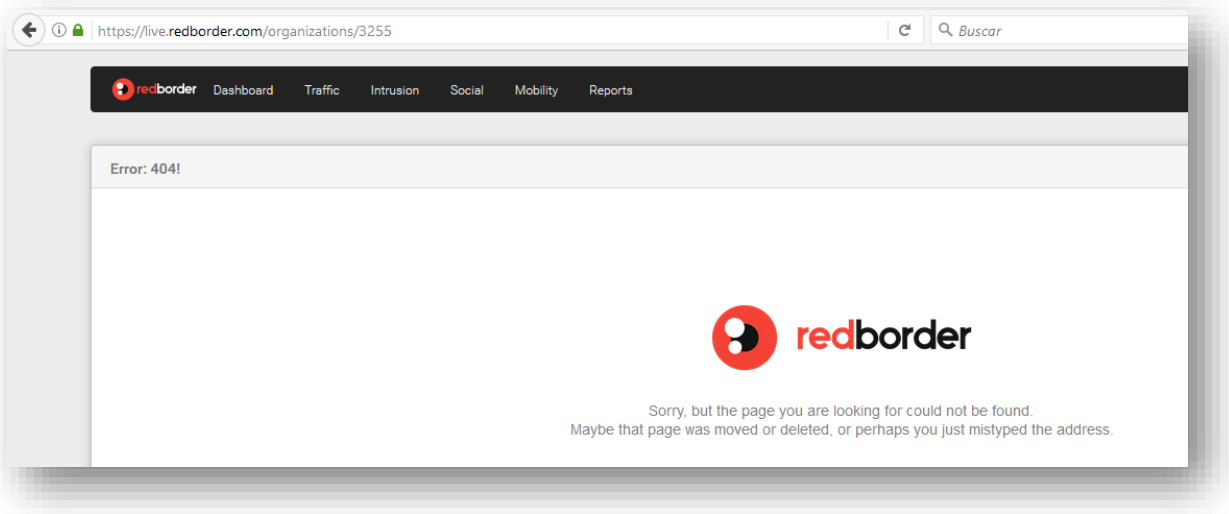


Figura 75. Error 404 desplegado cuando la organización no existe

5.2.2. Creación de cuentas con privilegio de administrador a cualquier organización

Se encontró una vulnerabilidad de tipo “web parameter tampering” que permite crear usuarios de tipo administrativo a cualquier organización:

- Modificando el valor del atributo value del campo “user[sensor_id]” de la sección invite user se pudo crear un usuario de tipo administrativo a cualquier organización cliente

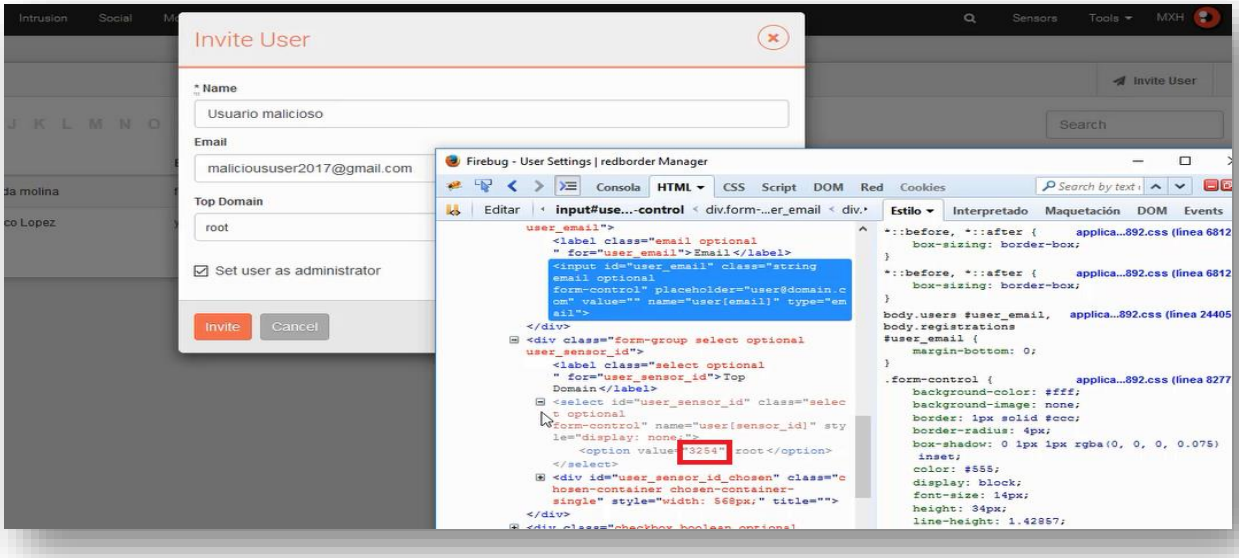


Figura 76. Modificación del ID de la organización

Como ejemplo, se creó una cuenta de usuario a la organización UOC cuyo ID es 3268

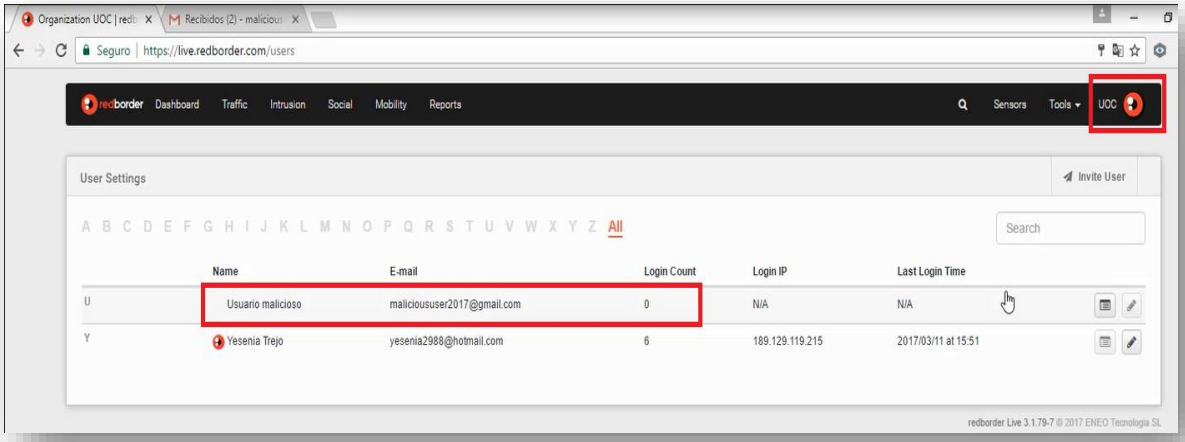


Figura 77. Sección users de la organización UOC

Figura 78. Usuario malicioso creado exitosamente

Por otra parte, al usuario malicioso le llegó un mensaje con el nombre de la organización donde se le generó la cuenta:

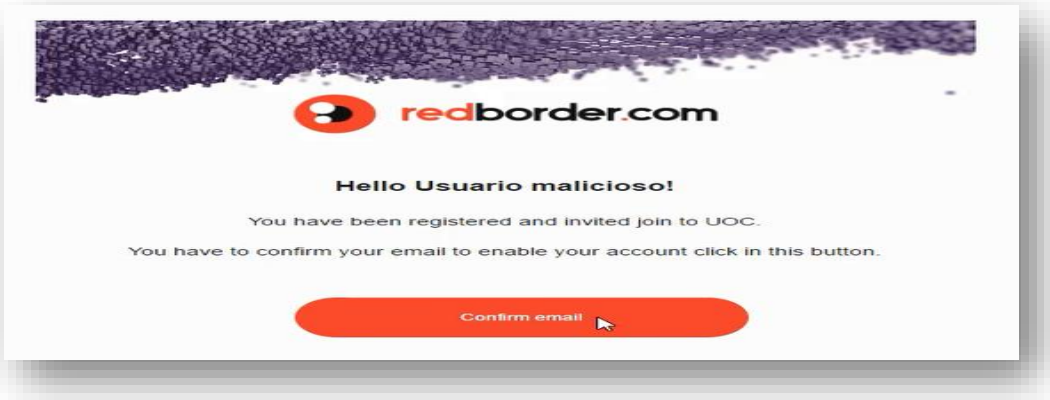


Figura 79. Correo electrónico con la confirmación de creación del usuario malicioso

Por medio del enlace que apareció en el correo, el usuario malicioso pudo dar de alta su perfil, y en cuanto terminó pudo acceder a la cuenta de la organización UOC.

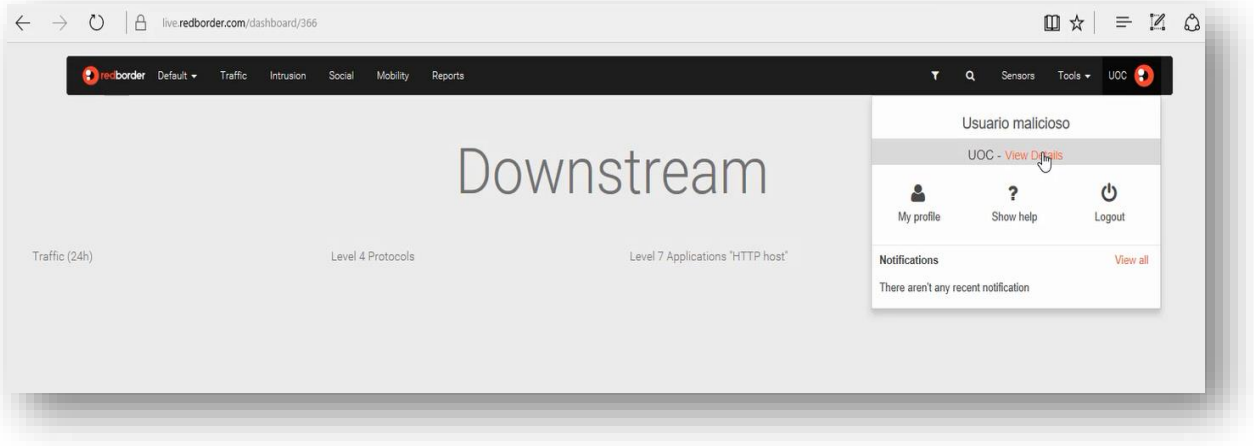


Figura 80. Acceso a la organización UOC por parte del usuario malicioso

5.3. Resumen de vulnerabilidades detectadas

Se detectaron en total 30 vulnerabilidades, la mayoría de estas de tipo web parameter tampering

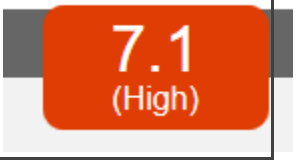
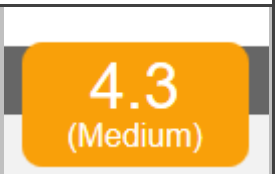
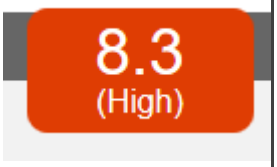
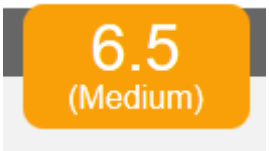
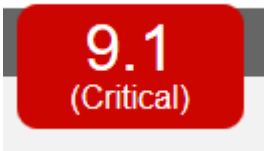
Categoría	Tipo de vulnerabilidades encontradas	Acción permitida por la vulnerabilidad
5.1.1. Obtención del listado y configuración de todos los dominios y sondas	Web parameter tampering	Acceso a la estructura y configuración de dominios, subdominios y sondas
	Web parameter tampering	Acceso a la estructura de dominios y subdominos
	Web parameter tampering	Acceso a la estructura de dominios y subdominos
	Web parameter tampering	Acceso a la estructura de dominios y subdominos
	Web parameter tampering	Acceso a los nombres de los dominios y subdominios de la solución
	Web parameter tampering	Acceso a los nombres de los dominios y subdominios de la solución
	Web parameter tampering	Acceso a los nombres de los dominios y sondas
5.1.2. Creación de dominios y sondas a cualquier domino/usuario	Web parameter tampering	Importación a cualquiera de los dominios cualquier tipo de subdominio y sonda
5.1.3. Obtención de la configuración de los dashboards de cualquier usuario	Web parameter tampering	Acceso a los widgets y configuración de todos los dashboards
5.1.4. Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets	Web parameter tampering	Eliminación de cualquier widget
	Web parameter tampering	Creación de un widget en cualquier Dashboard
	Web parameter tampering	Creación de un widget en cualquier reporte

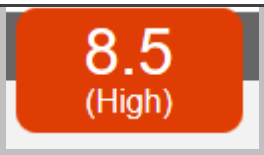
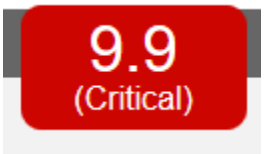
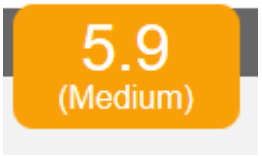
5.1.5. Obtención de los ID's de los usuarios activos en la solución	Information Exposure through an Error Message	Acceso a los ID's activos
5.1.6. Obtención del listado de todos los usuarios	Web parameter tampering	Acceso a los nombres de los usuarios activos
	Web parameter tampering	Acceso a los nombres de los usuarios activos
5.1.7. Eliminación de las notificaciones de todos los usuarios	Web parameter tampering	Eliminación de las notificaciones de cualquier usuario
5.1.8. Carga de ficheros maliciosos a las cuentas de todos los usuarios	Unrestricted File Upload	Creación de widgets maliciosos de tipo image en el dashboard
	XSS persistente	Creación de widgets maliciosos de tipo image con XSS en el dashboard
5.1.9. Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario	XSS persistente	Carga de URL con XSS en dashboards y reportes
	URL injection	Carga de URL maliciosa en los reportes y dashboards
5.1.10. Edición y borrado de alarmas	Web parameter tampering	Acceso y modificación de la configuración de alarmas de otros usuarios.
	Web parameter tampering	Eliminación de alarmas de cualquier usuario
5.1.11 Creación de dominios de distintos tipos (diferentes de los habilitados)	Web parameter tampering	Creación de diferentes tipos de dominios
5.1.12. Divulgación de IP's locales	Web Server HTTP Header Internal IP Disclosure	Acceso a IP local

5.1.13 Ataques de downgrade, SSL-stripping man-in-the-middle attacks y secuestro de cookies	HSTS Missing From HTTPS Server	Ataques de downgrade, SSL-stripping man-in-the-middle attacks y debilitación de las protecciones que evitan los secuestros de cookies
5.1.14. Divulgación de dominios no oficiales	Information Exposure	Acceso a dominios no oficiales
5.1.15. Almacenamiento de información confidencial en la memoria caché local	Cacheable HTTPS response	Acceso a información confidencial puesto que esta configuración permite que las respuestas de la aplicación se almacenen en la memoria caché local
5.1.16. Obtención de credenciales a través del formulario de inicio de sesión con autocomplete habilitado	Information Exposure	Las credenciales almacenadas pueden ser capturadas por un atacante que gane el control sobre la computadora del usuario
5.2.1. Divulgación de ID's de organizaciones activas	Information Exposure through an Error Message	Acceso a ID's de las organizaciones clientes activos
5.2.2. Creación de cuentas con privilegio de administrador a cualquier organización	Web parameter tampering	Creación de cuentas de tipo administrativo a cualquier organización
TOTAL	**30**	

Tabla 5. Vulnerabilidades encontradas organizadas por categoría

5.4. Impacto de las vulnerabilidades detectadas conforme el sistema CVSS 3.0

Sección	ID	Métricas	CVSS 3.0
5.1.1. Obtención del listado y configuración de todos los dominios y sondas	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	
5.1.2. Creación de dominios y sondas a cualquier domino/usuario	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N	
5.1.3. Obtención de la configuración de los dashboards de cualquier usuario	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	
5.1.4. Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L	
5.1.5. Obtención de los ID's de los usuarios activos en la solución	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	
5.1.6. Obtención del listado de todos los usuarios	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	
5.1.7. Eliminación de las notificaciones de todos los usuarios	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L	
5.1.8. Carga de ficheros maliciosos a las cuentas de todos los usuarios	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:L	

5.1.9. Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N	
Combinación de la 5.1.8 y 5.1.9	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H	
5.1.10. Edición y borrado de alarmas	Zero day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L	
5.1.11 Creación de dominios de distintos tipos (diferentes de los habilitados)	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N	
5.1.12. Divulgación de IP's locales	CVE-2000-0649	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	
5.1.13. Ataques de downgrade, SSL-stripping man-in-the-middle attacks y secuestro de cookies	___	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	
5.1.14. Divulgación de dominios no oficiales	____	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N	
5.1.15. Almacenamiento de información confidencial en la memoria caché local	CWE-524: Information Exposure Through Caching CWE-525: Information Exposure Through	CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N	

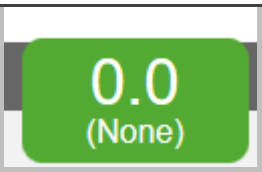
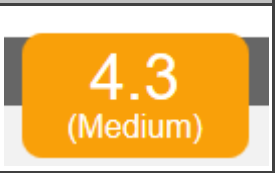
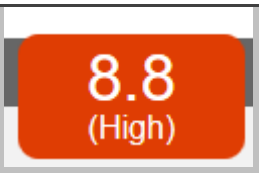
	Browser Caching		
5.1.16. Obtención de credenciales a través del formulario de inicio de sesión con autocomplete habilitado	CWE-200: Information Exposure	CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:N	
5.2.1. Divulgación de ID's de organizaciones activas	Zero Day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	
5.2.2. Creación de cuentas con privilegio de administrador a cualquier organización	Zero day	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	

Tabla 6. Impacto de las vulnerabilidades

6. Explotación

A partir de la información obtenida durante la fase de análisis de vulnerabilidades se efectuaron diferentes pruebas con la finalidad de establecer el acceso al sistema o a recursos de la plataforma Redborder versión cloud. El enfoque principal de esta fase fue identificar puntos de entrada principal en la organización e identificar activos de valor alto evitando las restricciones de seguridad a través del uso de herramientas de explotación.

6.1. Herramientas

Las siguientes herramientas fueron necesarias para crear el entorno de explotación:

- navegador Mozilla firefox,
- plugin Firebug para navegador firefox,
- metasploit,
- editor de textos
- editor hexadecimal HHD Hex Editor Neo,
- PDFStream Dumper

6.2. Ataques

A continuación se listan algunos ataques y la metodología utilizada para replicarlos, sin embargo, cabe mencionar que estos son solo una representación de la infinidad de ataques que se pueden llevar a cabo, los cuales dependerán de los objetivos, creatividad e imaginación de los atacantes.

6.2.1. Distribución de malware desde dashboards

Para realizar este ataque se usaron las vulnerabilidades 5.1.3. Obtención de la configuración de los dashboards de cualquier usuario, 5.1.4. Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets, 5.1.8. Carga de ficheros maliciosos a las cuentas de todos los usuarios y 5.1.9. Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario.

El ataque se realizó desde la cuenta del usuario malicioso y el dashboard objetivo fue el ID 53. Los pasos fueron:

1. Desde la cuenta del usuario malicioso se editó cualquier dashboard.
2. Se modificó la URL del botón Export Dashboard, y se sustituyó el ID original por el valor 53:

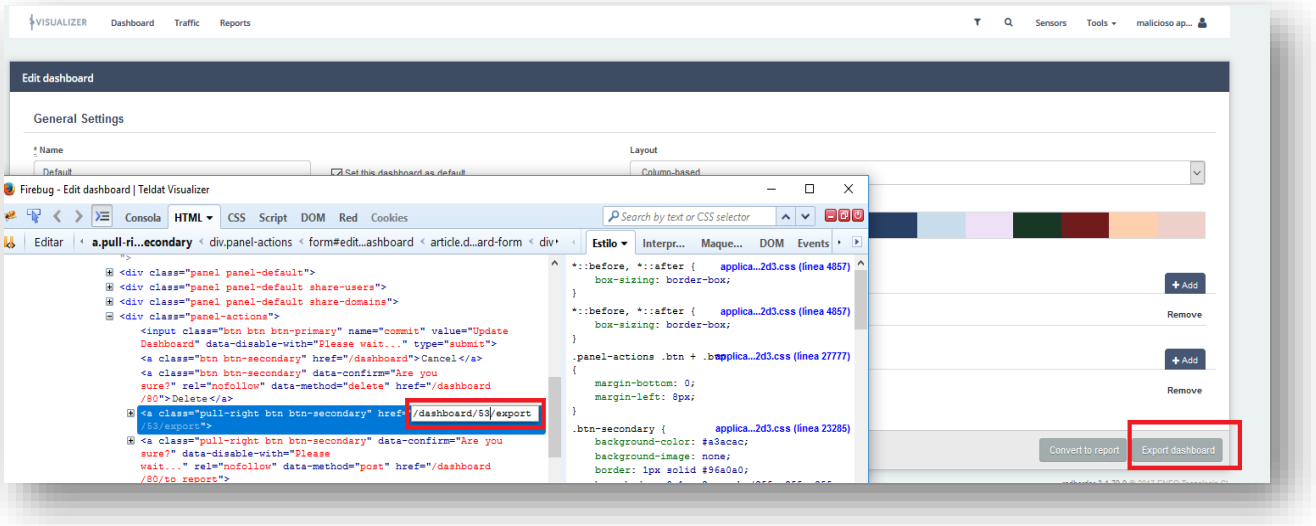


Figura 81. Botón Export- sección editar Dashboard-

3. Una vez descargado el fichero .tar.gz con la configuración del dashboard, se pudo apreciar el nombre del dashboard: “Network traffic”

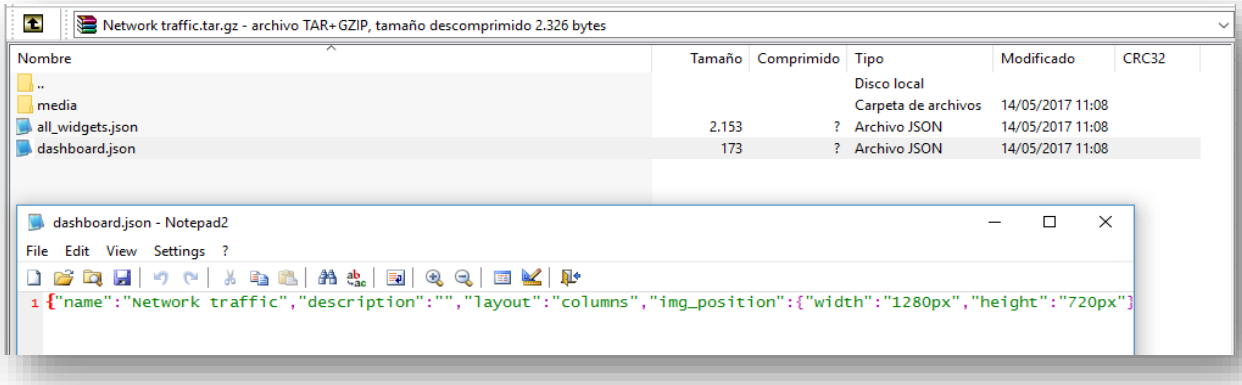


Figura 82. Fichero de configuración del dashboard

El cual a su vez estaba compuesto por 3 widgets:

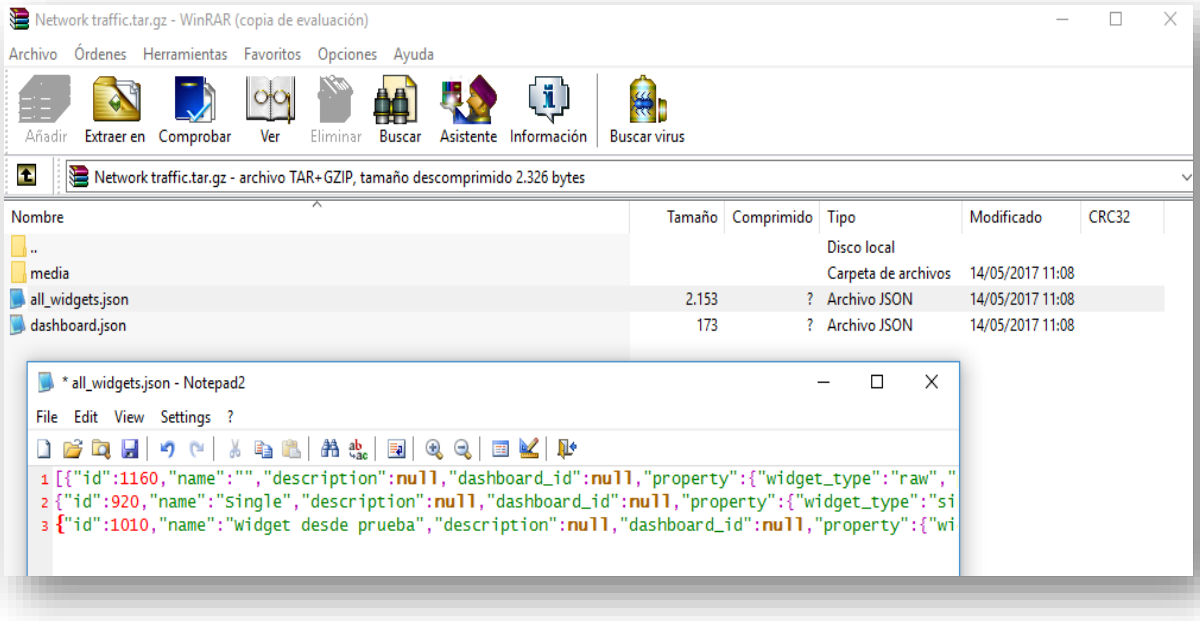


Figura 83. Widgets del dashboard

4. Una vez que se obtuvieron los datos del dashboard se procedió a crear una imagen con código javascript malicioso dirigido al usuario. Para hacerlo más realista, se utilizó el nombre del dashboard en el mensaje que se muestra al usuario.

Figura 84.Imagen svg con XSS malicioso

5. Se creó un PDF malicioso usando los diferentes exploits disponibles en metasploit.
6. Para impedir que el PDF fuera leído por los visores de los navegadores se comprimió en un fichero .zip (se pudo haber utilizado otro sistema de compresión como .tar.gz) cuyo nombre fue igual al nombre del dashboard, todo ello con la intención de evitar la desconfianza por parte del usuario. Después este fichero se subió a un servidor previamente comprometido con https habilitado.
7. Se generó un widget de tipo Shape → image que contenía la imagen maliciosa, para esto se usó la vulnerabilidad 5.1.4 Modificación de los

dashboards y reportes de los usuarios a través de la eliminación y creación de widgets

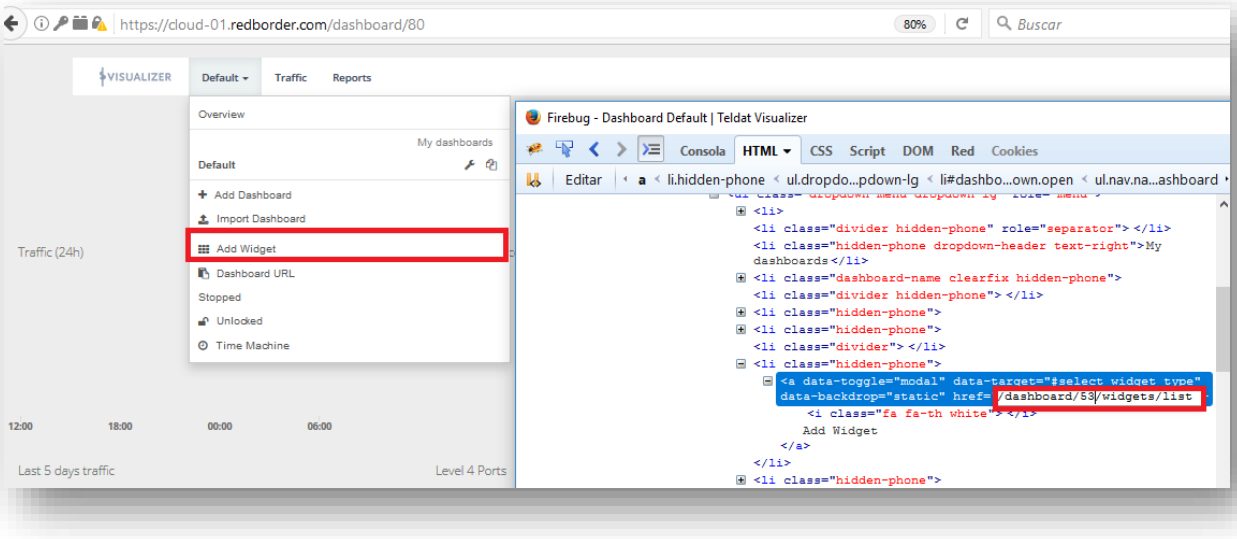


Figura 85. Modificación de la opción Add widget

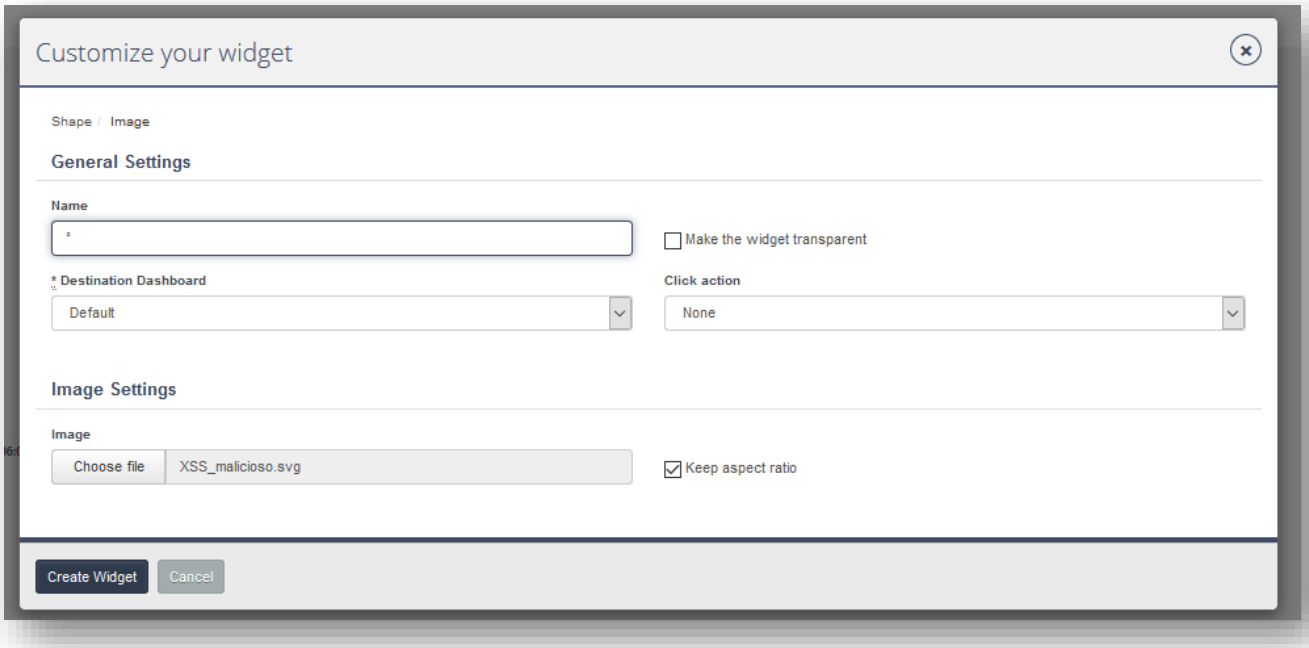


Figura 86. Creación de widget con imagen maliciosa

8. De nuevo se utilizó la vulnerabilidad 5.1.3 Obtención de la configuración de los dashboards de cualquier usuario, y se descargó la configuración del dashboard ID 53

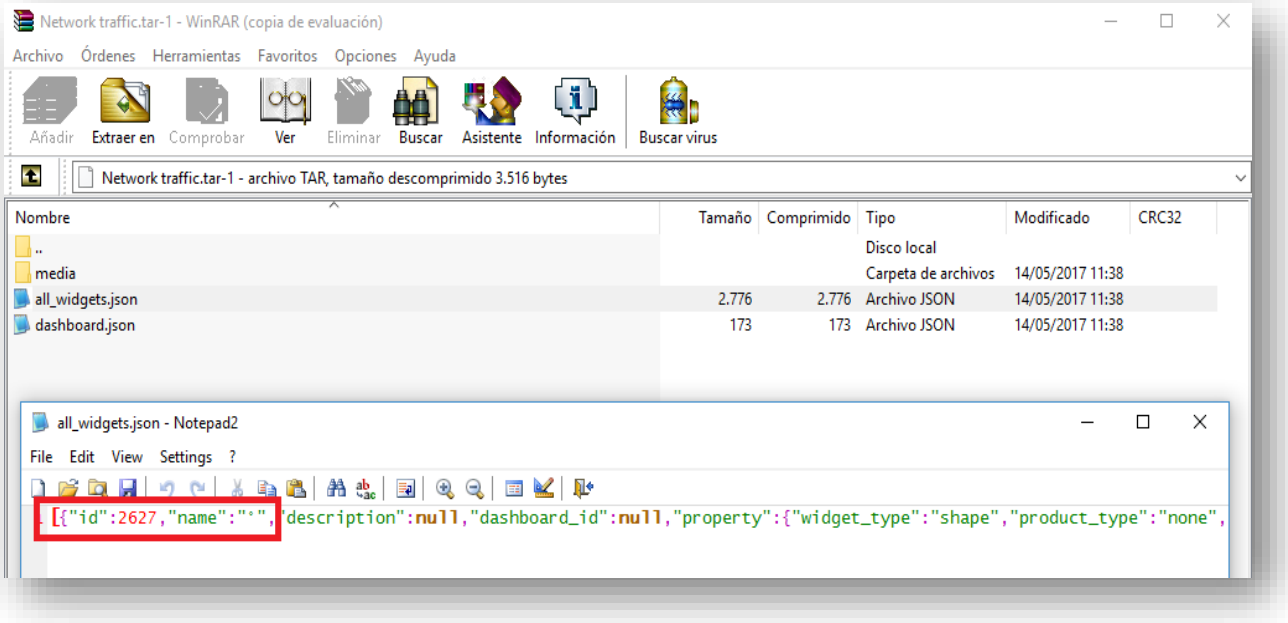


Figura 87. Comprobación de la creación exitosa del widget malicioso

Como se aprecia en la figura anterior, a la imagen maliciosa se le asignó el ID 2627, lo que significa que la URL de la imagen era: https://cloud-01.Redborder.com /dashboard/53/widgets/2627/image

9. Una vez que se obtuvo la URL, se le creó al dashboard ID 53 un widget de tipo URL que contenía un enlace hacia la imagen maliciosa

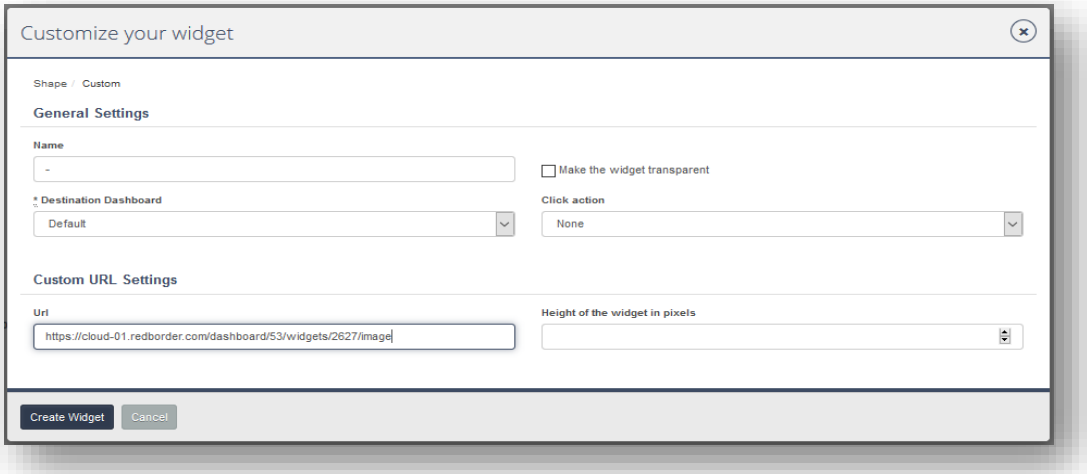


Figura 88. Creación de widget con URL maliciosa

10. Cuando el propietario, en este caso ytrejo, abrió el dashboard se le mostró el siguiente mensaje:

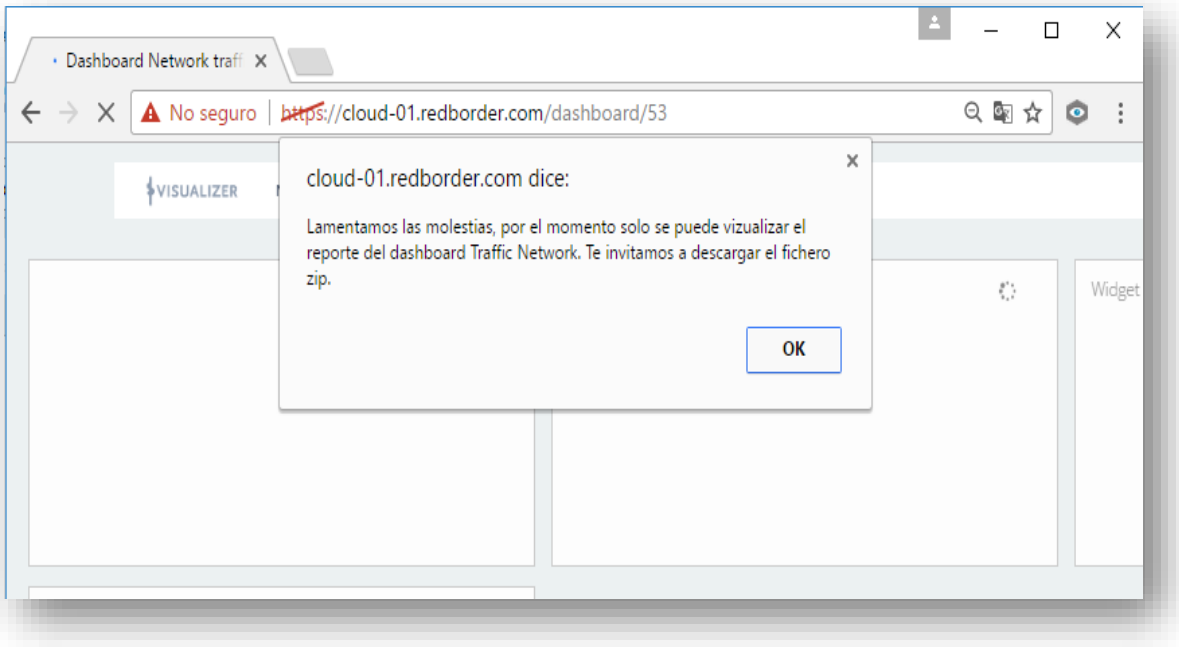


Figura 89. Ejecución del XSS embebido en la imagen

Y en automático se descargó el fichero .zip

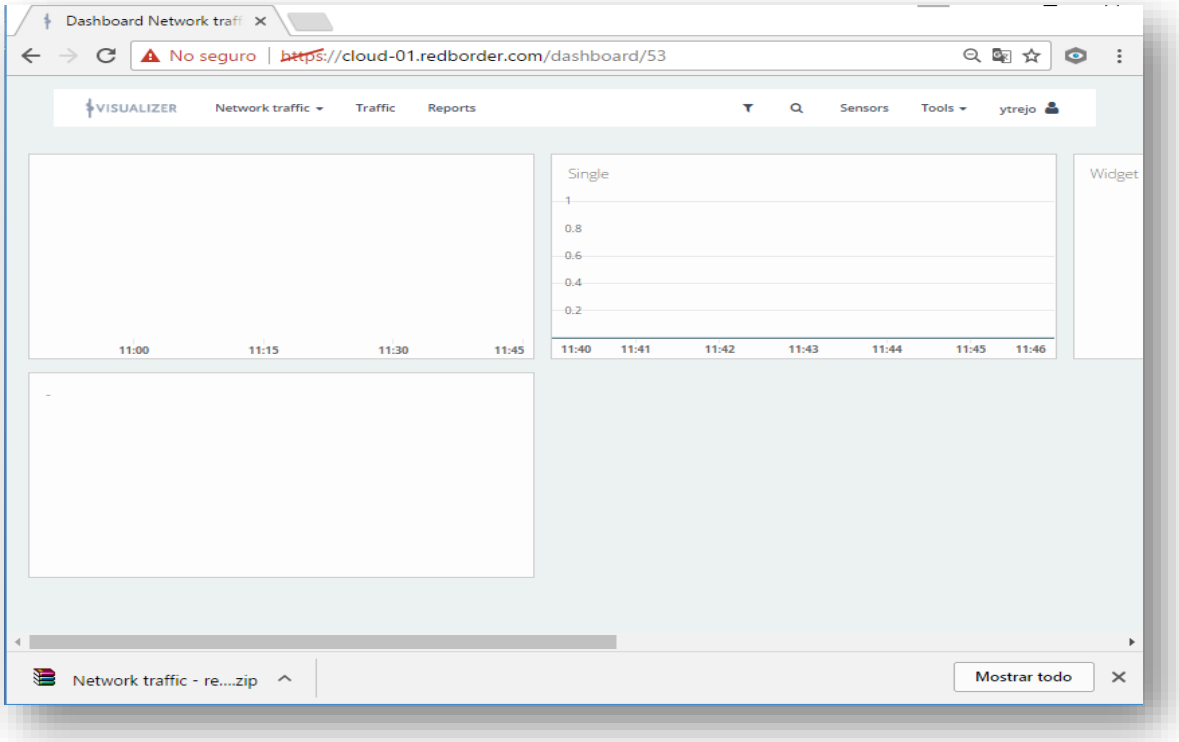


Figura 90. Descarga automática del fichero zip malicioso

11. Cuando el usuario abrió el fichero .zip, el código malicioso se ejecutó inmediatamente

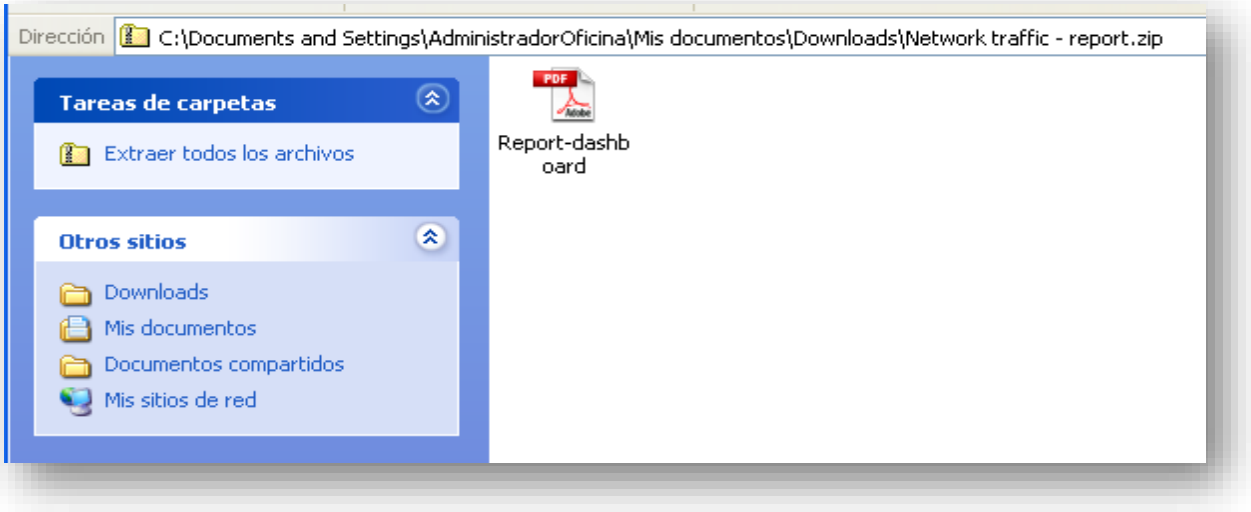


Figura 91. Archivo PDF malicioso

En este caso el payload contenía el siguiente código:

cmd /c echo ^<html^>^<body^>^<center^>^<img src="http://www.webseoanalytics.com/blog/wp-content/uploads/2015/10/3-580x386.jpg"^>^</center^>^</body^>^</html^> > message.html & cmd /c start message.html

El cual le mostraba al usuario el siguiente mensaje en pantalla:

Figura 92. Mensaje del navegador

Se puede distribuir cualquier tipo de malware: espionaje industrial, ransomware, APT, ya que para el usuario este PDF es un archivo de confianza.

6.2.2. Distribución de malware desde Reports

Para efectuar este ataque se usaron las vulnerabilidades 5.1.4 Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets y 5.1.9 Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario.

El ataque se realizó desde la cuenta del usuario malicioso y el reporte objetivo fue el ID 94. Los pasos fueron:

1. Desde la cuenta del usuario malicioso se editó cualquier reporte.
2. Se modificó la URL del botón Add block, y se sustituyó el ID original por el valor 94:

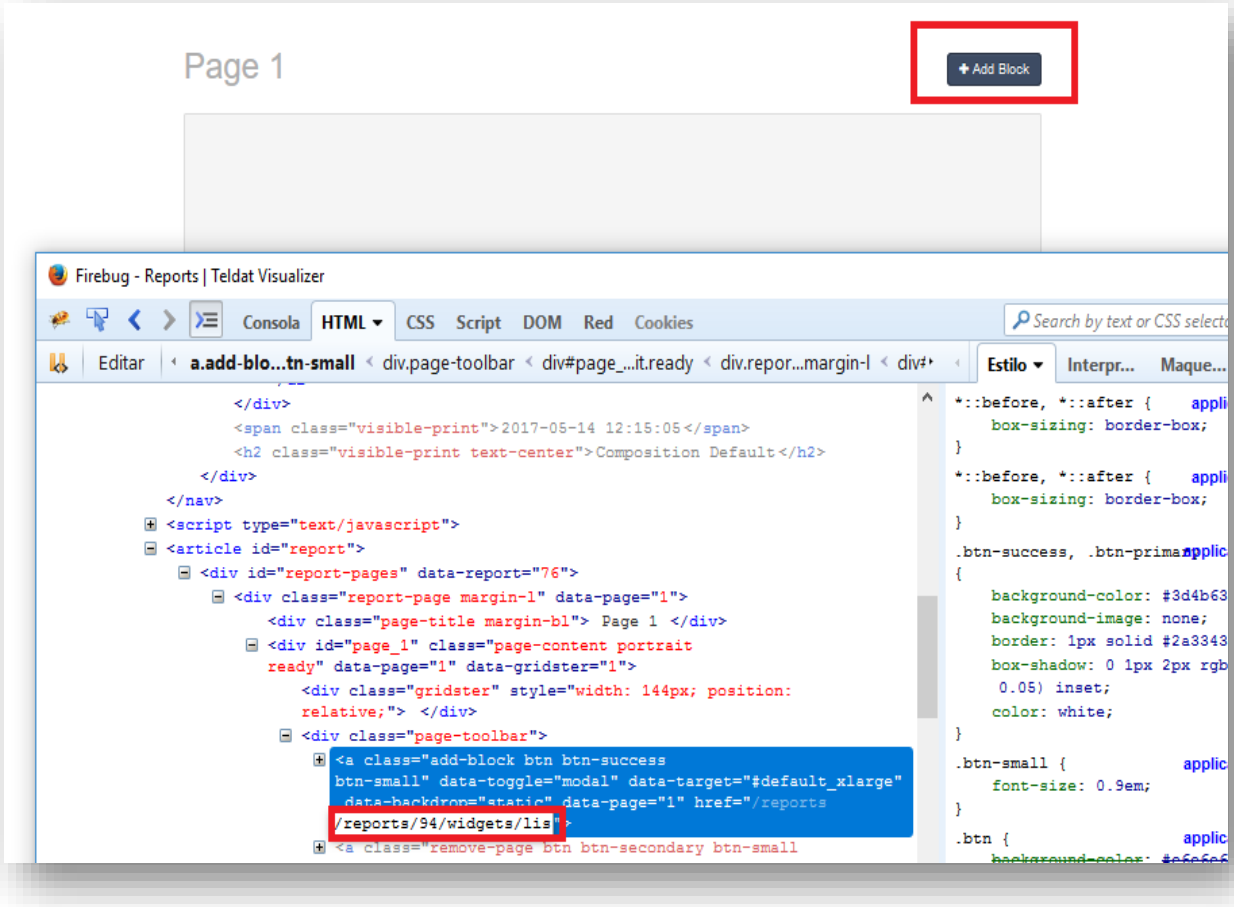


Figura 93. Modificación del código del Botón Add block

3. Se creó un PDF malicioso usando los diferentes exploits disponibles en Metasploit.
4. Para evitar que el PDF fuera leído por los visores de los navegadores se comprimió en un fichero .zip, posteriormente para que el usuario pensara

que era un reporte del dashboard se renombró como Report-dasboard. Después, este fichero se alojó en un servidor comprometido con el protocolo https habilitado.

5. Se le creó al reporte ID 94 un widget de tipo URL que contenía como enlace el fichero zip malicioso. Si se observa, en la solución los reportes no tienen habilitada la opción para crear URL's, pero analizando la URL que permite crear este tipo de widget en la sección dashboards

https://cloud-01.Redborder.com/dashboard/?ID/widgets/new/shape/custom/none

se pudo notar que el enlace debe contener el formato new/shape/custom/none. Con esta información, se modificó una de las URL's, en este caso la del objeto square:

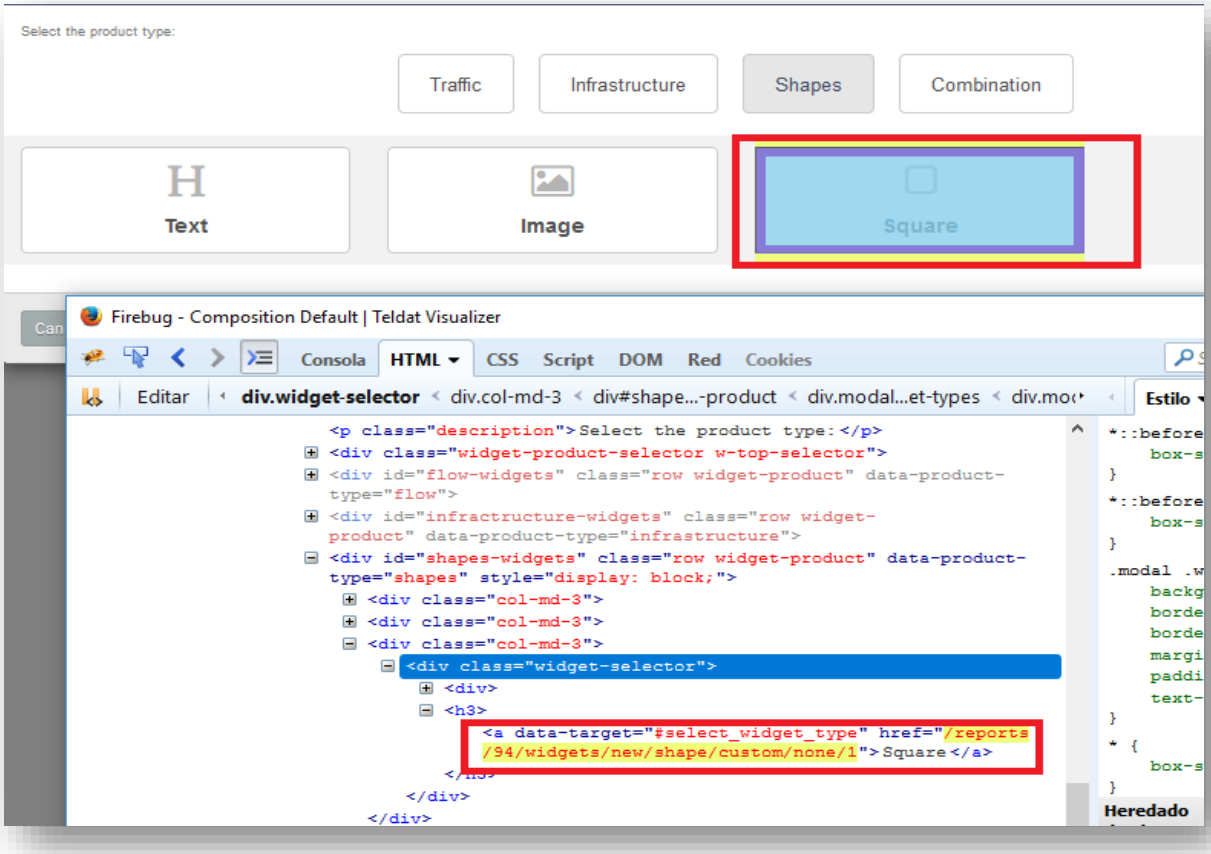


Figura 94. Modificación del código del objeto shape

Y se generó el widget de tipo URL:

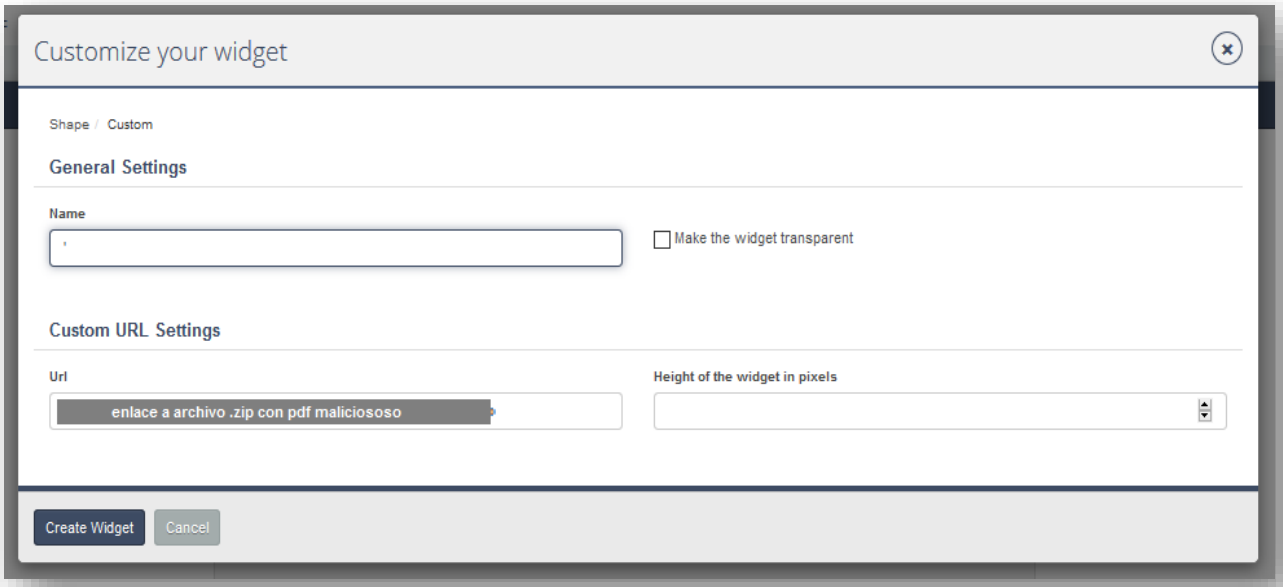


Figura 95. Creación del widget de tipo URL

6. De esta forma cuando el propietario del reporte abrió la sección composition, el fichero .zip fue descargado de forma automática.

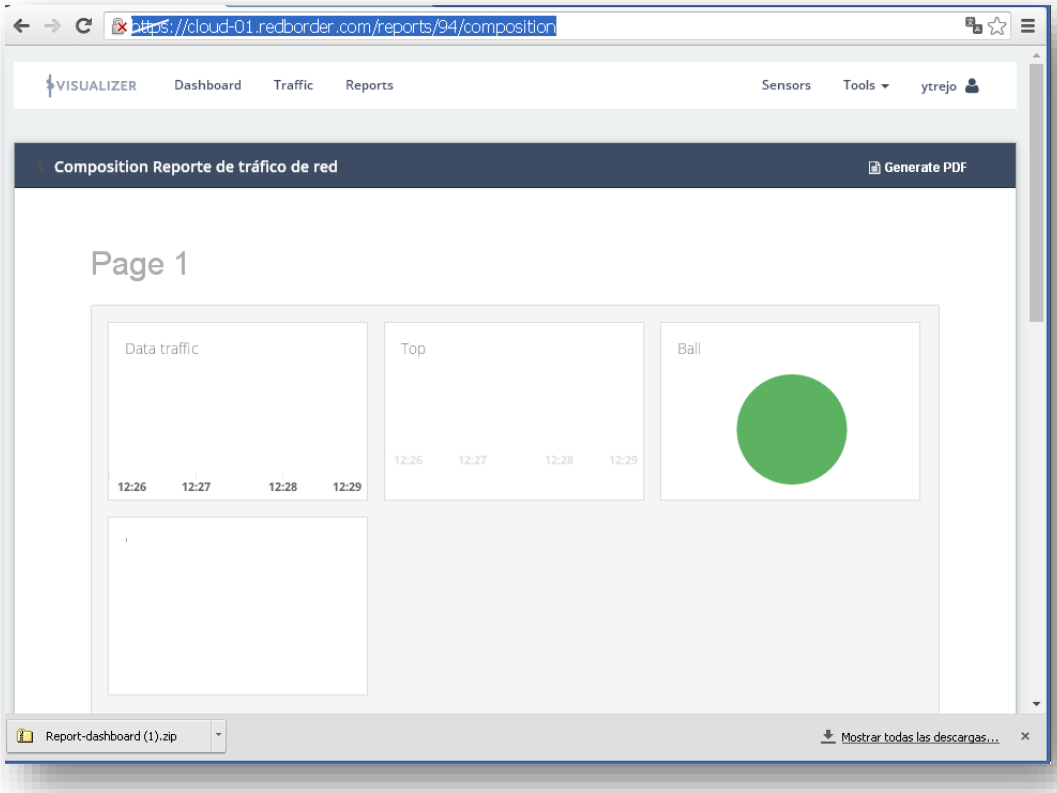


Figura 96. Descarga automática del fichero zip malicioso

7. Cuando el usuario abrió el fichero .zip, el archivo malicioso se ejecutó inmediatamente

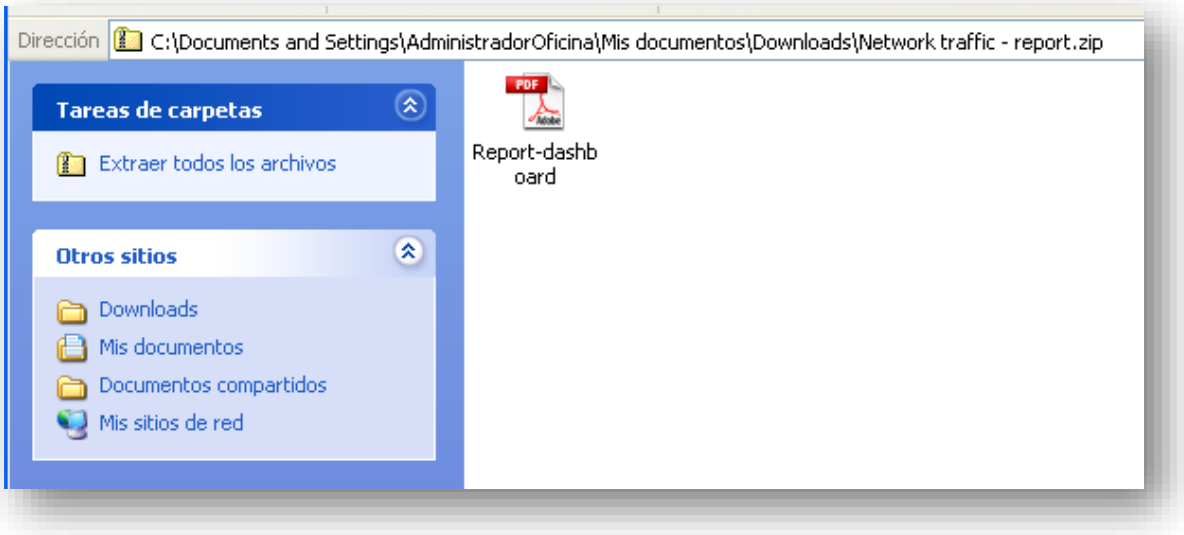


Figura 97. Archivo PDF malicioso

En este caso el payload contenía el siguiente código:

cmd /c echo ^<html^>^<body^>^<center^>^<img src="http://www.webseoanalytics.com/blog/wp-content/uploads/2015/10/3-580x386.jpg"^>^</center^>^</body^>^</html^> > message.html & cmd /c start message.html

El cual le mostraba al usuario el siguiente mensaje en pantalla:

Figura 98. Mensaje del navegador

Pero al igual que en el ataque anterior, se pudo haber distribuido cualquier tipo de malware: de espionaje industrial, ransomware, APT, pues este archivo aparentemente esta proviniendo de una fuente “confiable”.

6.2.3. Distribución de malware a través de los correos de los clientes por medio de la modificación de los reportes periódicos

Para lograr este ataque se usaron las vulnerabilidades 5.1.4 Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets, 5.1.8. Carga de ficheros maliciosos a las cuentas de todos los usuarios y 5.1.9 Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario.

El ataque se ejecutó desde la cuenta del usuario malicioso y el reporte objetivo fue el ID 94. Los pasos fueron:

1. Se editó cualquier reporte desde la cuenta del usuario malicioso.
2. Se modificó la URL del botón Add block, y se sustituyó el ID original por el valor 94

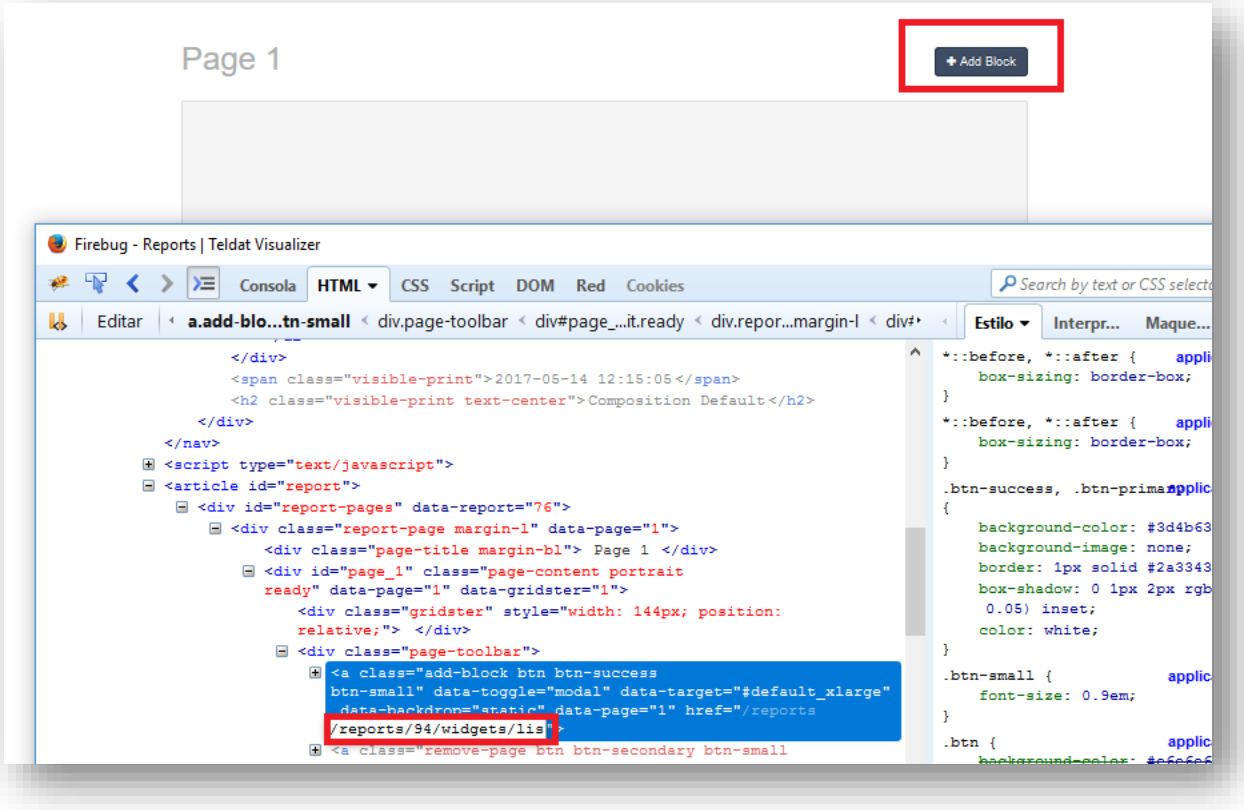


Figura 99. Modificación del botón Add block

3. Se crearon 3 imágenes con código malicioso.

Imagen	Código	Descripción
test-1	--*endstream.endobj 7 0 obj <</T#79p#65/#43ata#6c#6f#67/#4futl #69n#65s 2 0 R/P#61#67#65#73 3 0 R/O#70#65n#41#63t#69#6fn 10 0 R>>*--	Se define el stream 7. Indica que el script o acción que se ejecutará automáticamente está ubicado en el stream 10
test-2	--*endstream.endobj 10 0 obj<</T#79pe/Action/#53/J#61#76 #61Scri#70#74/#4a#53 12 0 R>>*- -	Se define el stream 10. Indica que se ejecutará un javascript en el stream 12
test-3	--*endstream.endobj 12 0 obj <</Le#6e#67#74h 5599/#46ilter[/Fl#61t#65#44ec#6f# 64e/A#53#43#49l#48e#78#44#65 code]>> payload --	Se define el stream 12. Contiene el payload malicioso a ejecutarse cuando se abra el PDF

Tabla 7. Imagenes y códido de los streams

4. Una vez que se generaron las imágenes, estas se cargaron de la siguiente forma:

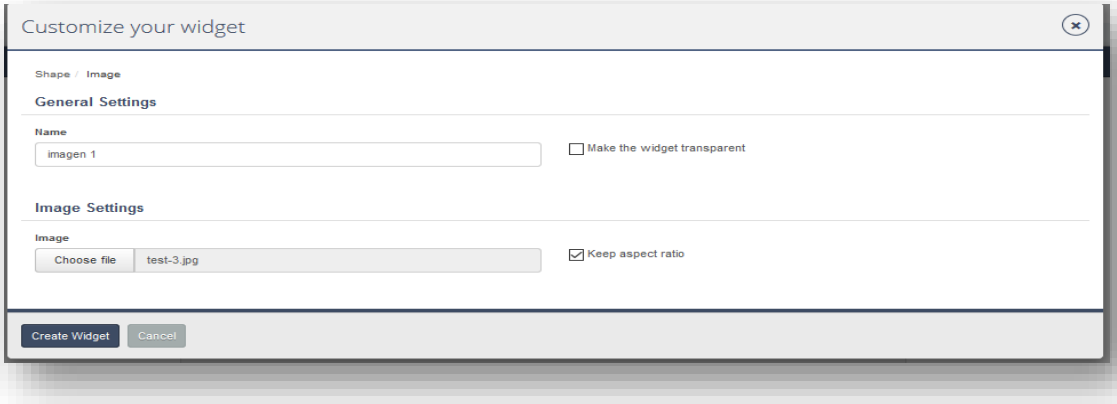


Figura 100. Creación del widget con la imagen test-3.jpg

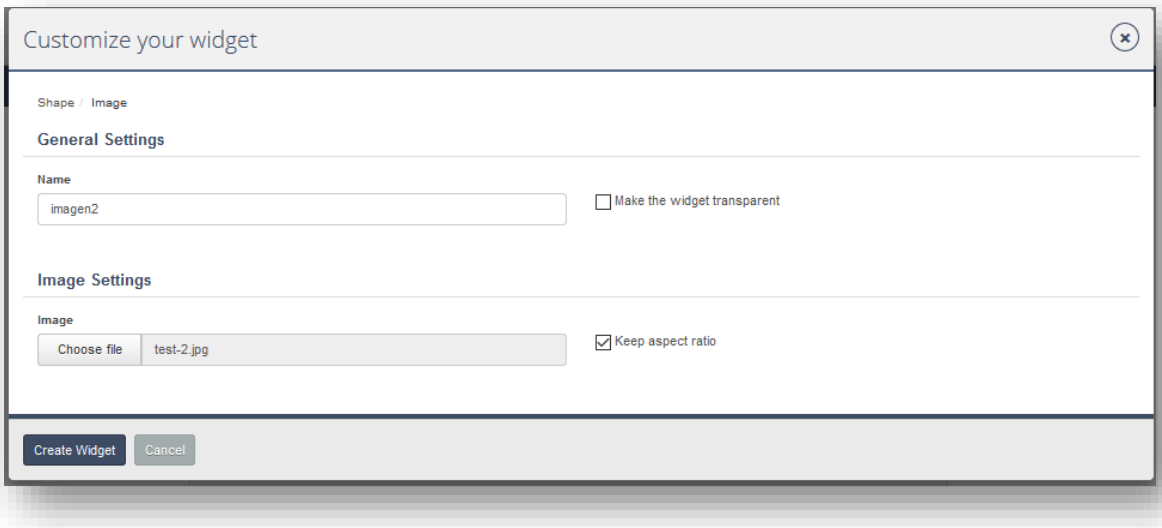


Figura 101. Creación del widget con la imagen test-2.jpg

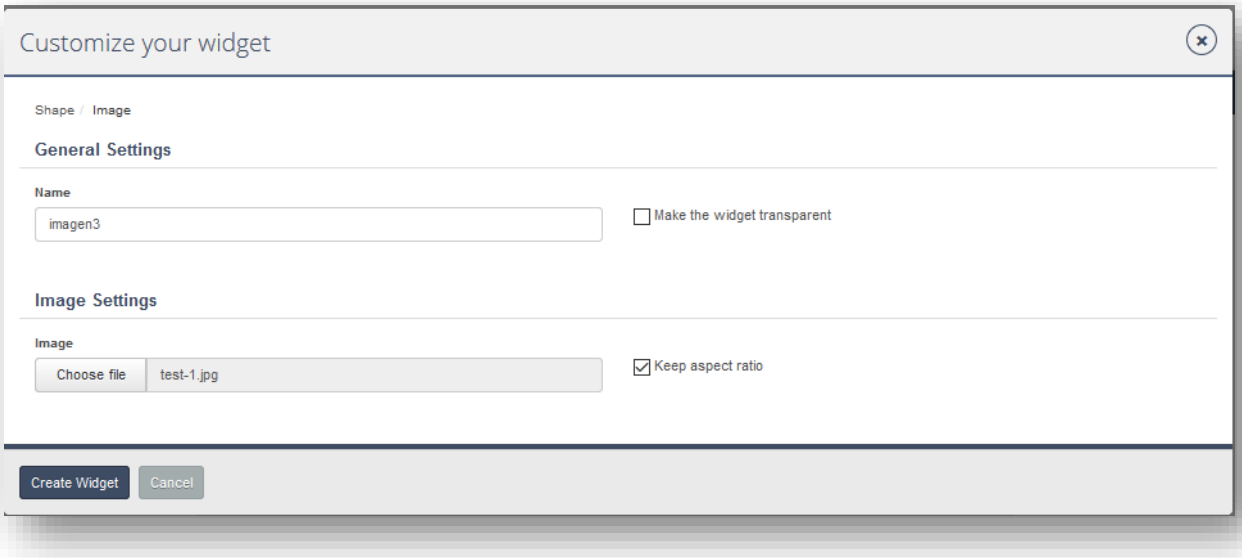


Figura 102. Creación del widget con la imagen test-1.jpg

Primero la imagen test-3, luego test-2, y al último test-1.

5. Por otra parte, el propietario abrió su correo, descargó el reporte y en el momento en que abrió el PDF el archivo malicioso se ejecutó.
6. Para verificar cómo el código malicioso se incrustó en el PDF se utilizó PDFstreamdumper

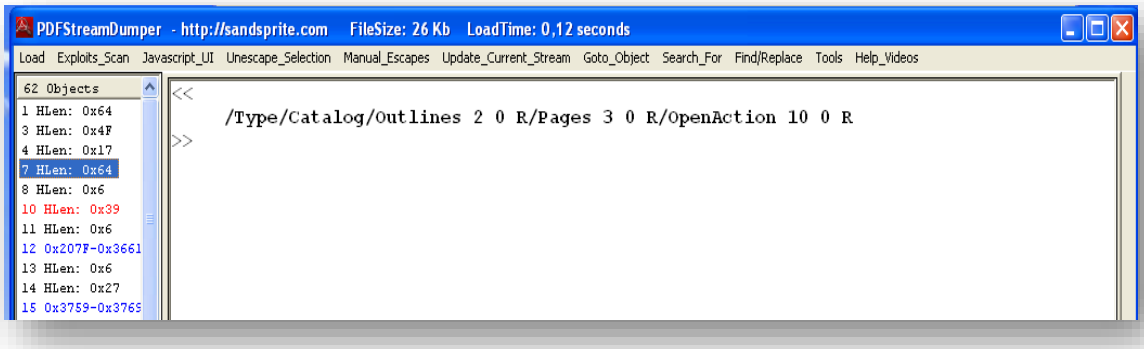


Figura 103. Stream contenido en la imagen test-1.jpg

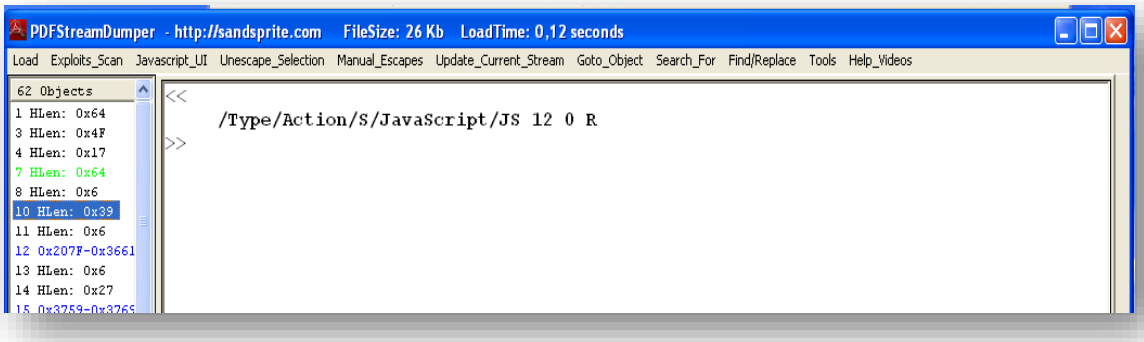


Figura 104. Stream contenido en la imagen test-2.jpg

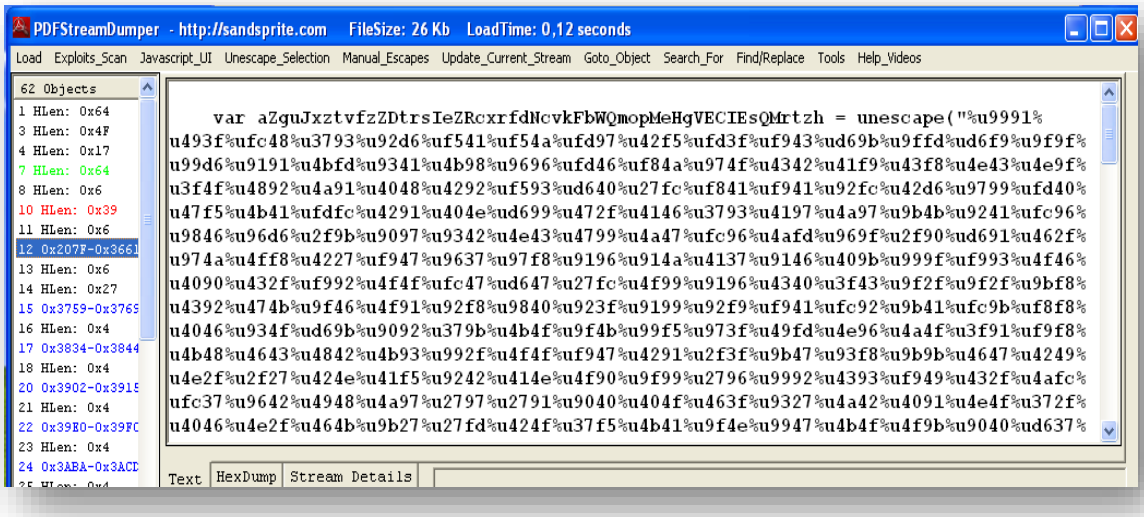


Figura 105. Stream contenido en la imagen test-3.jpg

7. Al abrir el PDF se observó que el documento ocultaba y mostraba la información dependiendo de los movimientos de la barra.

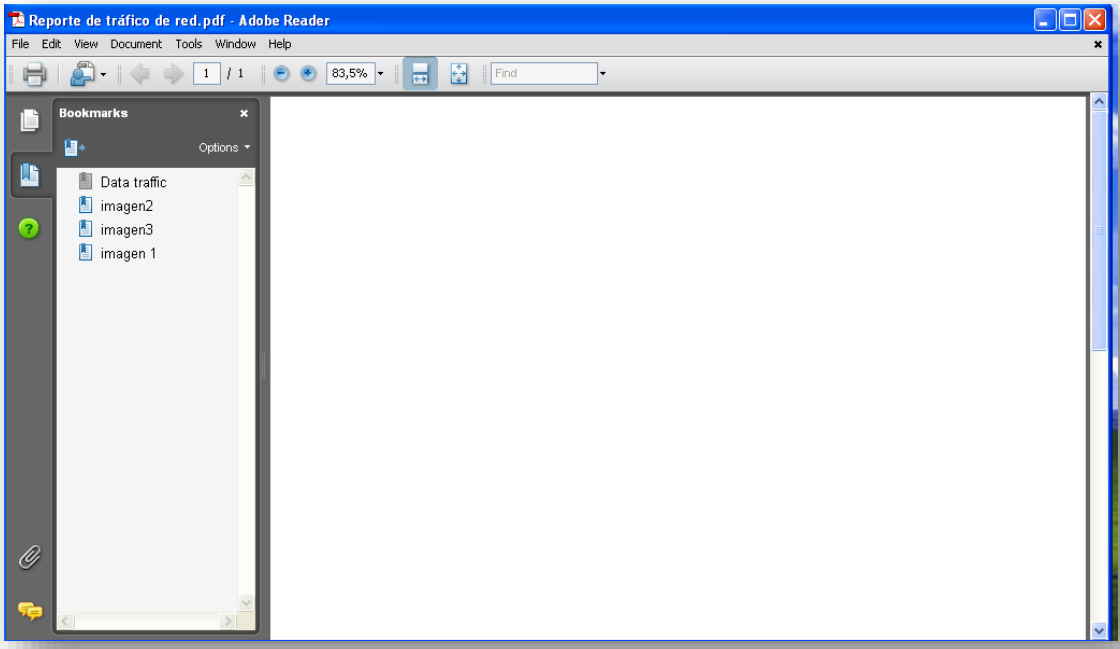


Figura 106. Página 1 del PDF con texto oculto

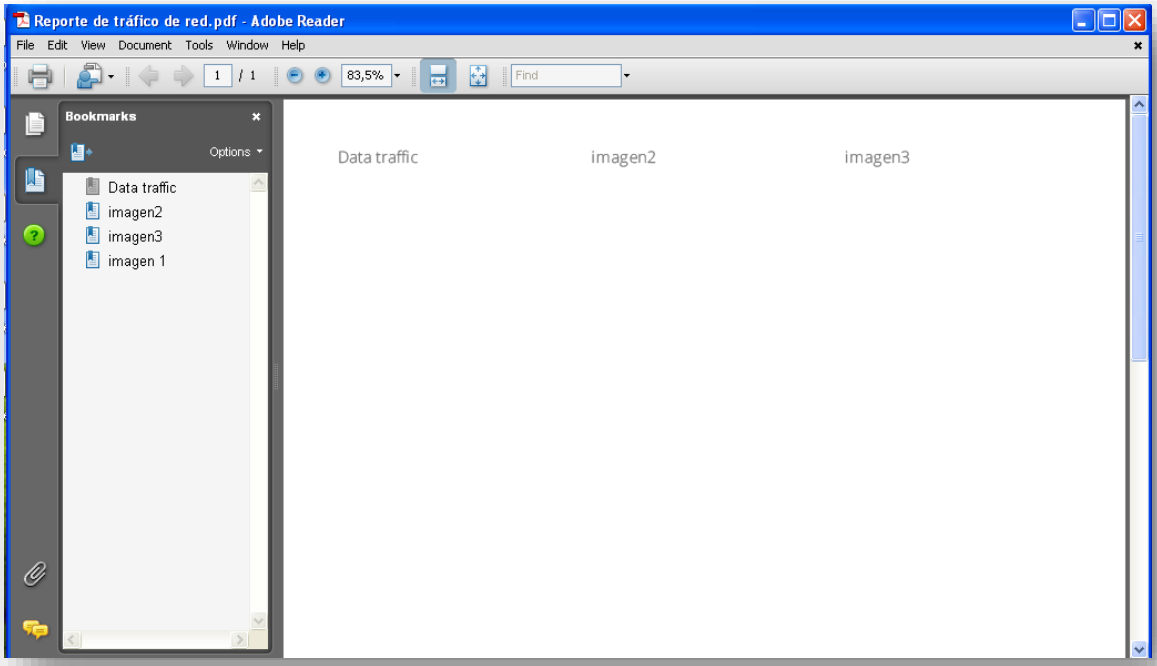


Figura 107. Página 1 del PDF mostrando parte del texto

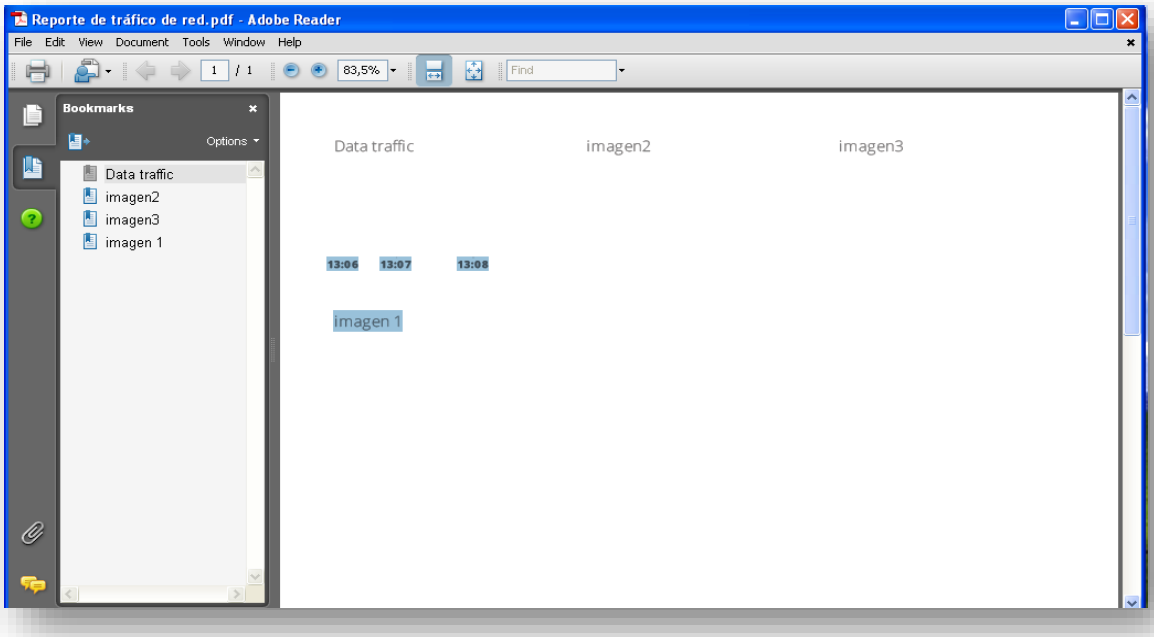


Figura 108. Página 1 del PDF mostrando mayor cantidad de texto

8. Por lo tanto, las imágenes maliciosas incrustadas en el PDF se pudieron utilizar para distintos fines: esconder información -secretos industriales, espionaje-, o para propagar malware sin que causara ninguna sospecha.

6.2.4. Ataques de ingeniería social a partir de la divulgación de nombres de usuario y correos electrónicos

De la combinación de las vulnerabilidades 5.1.5. Obtención de los ID's de los usuarios activos en la plataforma, 5.1.6. Obtención del listado de todos los usuarios y 5.1.10 Edición y borrado de alarmas, se podría deducir el nombre de los usuarios y cuentas de email asociadas para enviar correos de tipo phishing. Dichos correos simularían ser emitidos por parte del equipo de soporte y contendrían mensajes y URL maliciosos con el objetivo de engañar al usuario para que abra un sitio malicioso similar a Redborder y con ello recolectar las credenciales para otros fines maliciosos.

6.2.5. Apropiación de cualquier cuenta de Redborder

Usando las vulnerabilidades 5.2.1 Divulgación de ID's de organizaciones activas y 5.2.2 Creación de cuentas con privilegio de administrador a cualquier organización fue posible apropiarse de cualquier organización cliente de Redborder. Al tener permisos como usuario administrativo se pudieron haber eliminado el resto de cuentas y tener acceso a toda la información que se almacena: nombres de usuarios, cuentas de correo electrónico, información de las sondas, configuración de sondas; y lograr diferentes ataques como secuestro de dominios/sondas, propagación de malware, ataques de ingeniería social, y muchos más.

7. Post-explotación

Al ser una ambiente en producción, esta fase consistió en determinar cómo un atacante podría mantener el control de los dispositivos comprometidos para su uso posterior o para lograr comprometer aún más la red. Los métodos descritos en esta fase están diseñados para ayudar a identificar y documentar datos confidenciales, identificar configuraciones, canales de comunicación y relaciones con otros dispositivos que se pueden utilizar para obtener más acceso a la red y configurar uno o más métodos para acceder a los equipos en un momento posterior. Sin duda, todo dependerá de las máquinas comprometidas en la fase de explotación, ya que la sensibilidad de los datos almacenados en ellas favoreceré en mayor o menor medida a que se logre comprometer aún más a la organización.

7.1. Explotando las vulnerabilidades de divulgación y modificación de información

Considerando que se lograron comprometer equipos a partir de los ataques expuestos en la fase de explotación, sería posible comprometer aún más la red de las organizaciones afectadas empleando los hallazgos de la fase de análisis de vulnerabilidades:

a) Una vez obtenido acceso al equipo de los clientes se podría verificar la factibilidad de explotar la vulnerabilidad 5.1.16. Obtención de credenciales a través del formulario de inicio de sesión con autocomplete habilitado. Si el usuario almacenó las credenciales de Redborder en algún navegador

estas se podrían robar facilmente permitiendo tener control sobre cuentas de diferentes organizaciones clientes.

b) También desde el equipo comprometido se podría intentar explotar la vulnerabilidad 5.1.15. Almacenamiento de información confidencial en la memoria caché local con el objetivo de obtener información sensible.
c) Por medio de la vulnerabilidad 5.1.1. Obtención del listado y configuración de todos los dominios y sondas se podría conocer la estructura de la organización y la configuración de red para comprometer la confidencialidad, integridad y disponibilidad de los equipos de usuario, servidores y la propia red.
d) Con las vulnerabilidades 5.1.2. Creación de dominios y sondas a cualquier domino/usuario y 5.1.4. Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets sería factible crear una “cortina de humo” modificando los dashboards y creando sondas y dominios falsos con el propósto de ocultar un ataque a la red interna de los clientes. Y además, para desaparecer cualquier posible rastro de la nueva creación de sondas y dominios se podrían eliminar las notificaciones usando la vulnerabilidad 5.1.7. Eliminación de las notificaciones de todos los usuarios.
e) Si alguno de los equipos comprometidos fuera propiedad de algún empleado de Redborder, se podrían aprovechar las vulnerabilidades 5.1.12 Divulgación de IP’s locales y 5.1.14 Divulgación de dominios no oficiales para conocer la red y lograr obtener información sensible que pudiera llevar a comprometer aún más a la organización.

8. Informe

El informe se dividió en dos (2) secciones principales: informe ejecutivo e informe técnico, con el fin de comunicar a diferentes audiencias los objetivos, métodos, resultados de las pruebas realizadas y recomendaciones de mitigación.

8.1. Informe ejecutivo

El informe ejecutivo está compuesto por las siguientes secciones:

- alcance de la prueba de penetración,
- objetivos del proyecto,
- cronograma,
- resumen de hallazgos,
- nivel de riesgo,
- resumen de recomendaciones

Cada una de estas secciones se explica a continuación:

8.1.1. Alcance

Se realizaron pruebas de intrusión de caja gris sobre la solución Redborder versión cloud alojada en los siguientes subdominios: https://live.redborder.com y https://cloud-01.redborder.com. Estas pruebas de intrusión fueron a nivel de **aplicación web y red**.

8.1.2. Objetivos

El objetivo principal de esta prueba de intrusión fue evaluar los niveles de seguridad de la plataforma Redborder con la finalidad de detectar y mitigar vulnerabilidades y/o amenazas que pudieran poner en riesgo el funcionamiento normal de la misma, integridad/confidencialidad de los datos almacenados y la imagen-reputación de la empresa.

8.1.3. Cronograma

El siguiente cronograma muestra las fechas de inicio y fin de las pruebas de penetración

Actividades	Marzo				Abril				Mayo				Junio		
	Semana de 6 al 12 de marzo	Semana del 13 al 19 de marzo	Semana del 20 al 26 de marzo	Semana del 27 de marzo al 2 de abril	Semana del 3 al 9 de abril	Semana del 10 al 16 de abril	Semana del 17 al 23 de abril	Semana del 24 al 30 de abril	Semana del 1 al 7 de mayo	Semana del 8 al 14 de mayo	Semana del 15 al 21 de mayo	Semana del 22 al 28 de mayo	Semana del 29 de mayo al 4 de junio	Semana del 5 al 11 de junio	Semana del 12 de junio
Fase 1: Interacción contractual															
Fase 2: Reconocimiento															
Fase 3: Modelado de amenazas															
Fase 4: Análisis de vulnerabilidades															
Fase 5: Explotación															
Fase 6: Post-explotación															
Fase 7: Informe															

Tabla 8. Cronograma

8.1.4. Resumen de hallazgos

El siguiente gráfico muestra un resumen del tipo de vulnerabilidades encontradas en la solución Redborder versión cloud. En total se hallaron 30 vulnerabilidades, de las cuales un número significativo son de tipo **web parameter tampering** por lo que esta vulnerabilidad debería ser tratada como una prioridad al momento del desarrollo de la plataforma.

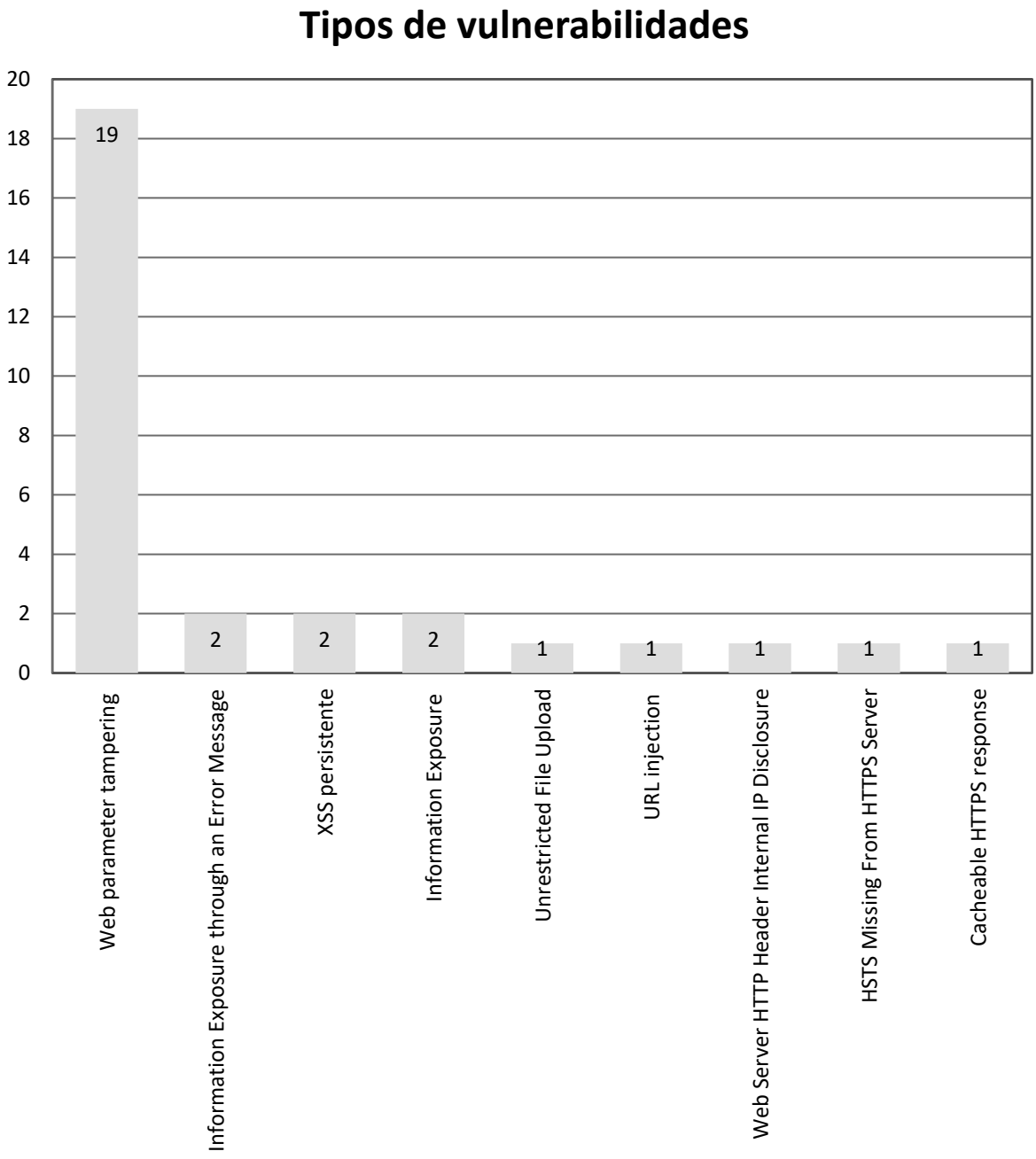


Figura 109. Tipos de vulnerabilidades encontradas

Como se puede apreciar en el gráfico de pastel, las vulnerabilidades de tipo Web parameter tampering representan el 64% de las vulnerabilidades encontradas.

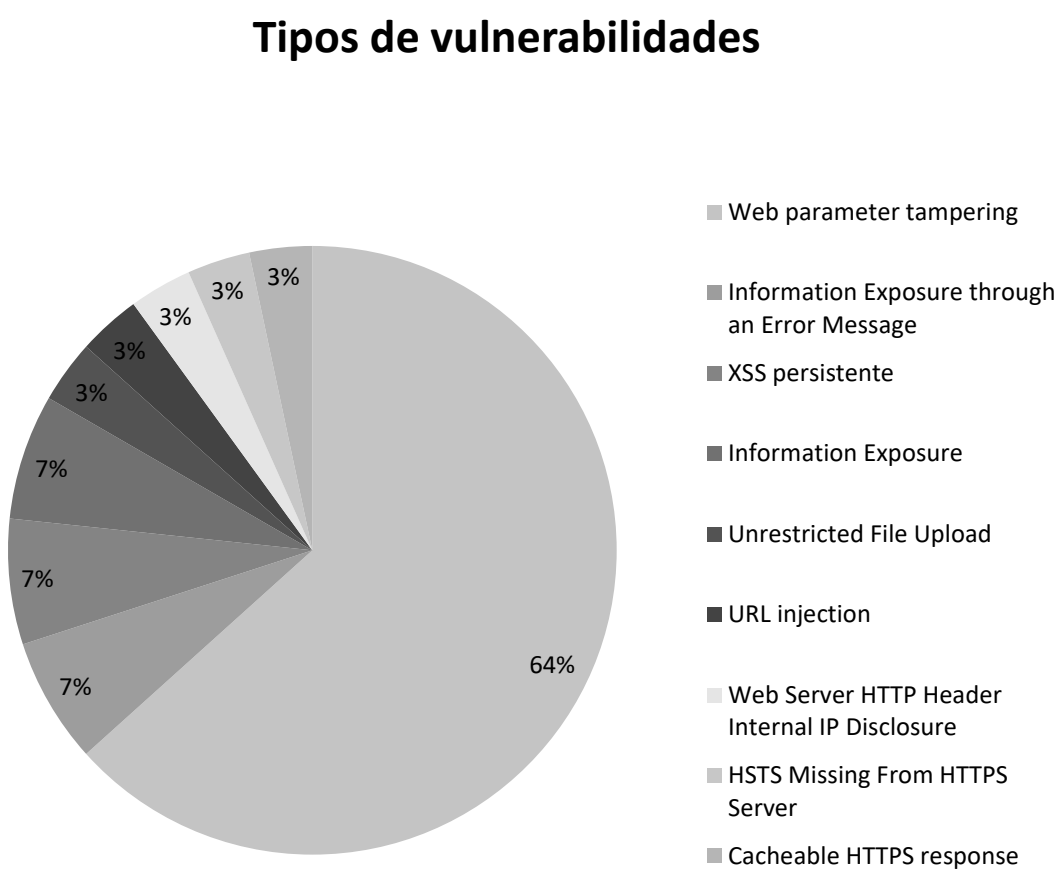


Figura 110. Gráfico de pastel –tipos de vulnerabilidades-

Y finalmente, en la siguiente tabla se clasifican las vulnerabilidades por el tipo de actividad que permiten ejecutar:

Categoría (actividad maliciosa)	Vulnerabilidades encontradas
5.1.1. Obtención del listado y configuración de todos los dominios y sondas	7
5.1.4. Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets	3
5.1.6. Obtención del listado de todos los usuarios	2
5.1.8. Carga de ficheros maliciosos a las cuentas de todos los usuarios	2
5.1.9. Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario	2
5.1.10. Edición y borrado de alarmas	2
5.1.2. Creación de dominios y sondas a cualquier domino/usuario	1
5.1.3. Obtención de la configuración de los dashboards de cualquier usuario	1
5.1.5. Obtención de los ID's de los usuarios activos en la solución	1
5.1.7. Eliminación de las notificaciones de todos los usuarios	1
5.1.11 Creación de dominios de distintos tipos (diferentes de los habilitados)	1
5.1.12. Divulgación de IP's locales	1
5.1.13. Ataques de downgrade, SSL-stripping man-in-the-middle attacks y secuestro de cookies	1
5.1.14. Divulgación de dominios no oficiales	1
5.1.15. Almacenamiento de información confidencial en la memoria caché local	1
5.1.16. Obtención de credenciales a través del formulario de inicio de sesión con autocomplete habilitado	1
5.2.1. Divulgación de ID's de organizaciones activas	1
5.2.2. Creación de cuentas con privilegio de administrador a cualquier organización	1

Tabla 9. Vulnerabilidades clasificadas por acción maliciosa

8.1.5. Nivel de riesgo

Durante la evaluación del riesgo se consideraron los siguientes aspectos: la puntuación CVSS 3.0 asignada a las vulnerabilidades, los resultados de las fases de explotación y finalmente, los escenarios expuestos en la fase de post-explotación. La clasificación del riesgo se realizó utilizando los siguientes niveles: crítico, alto, medio y bajo.

Se comprobó la existencia de 2 vulnerabilidades críticas, así como un número significativo de vulnerabilidades de alto y medio impacto, resultado del uso de rutinas inadecuadas o mal implementadas y la inexistente validación de entradas.

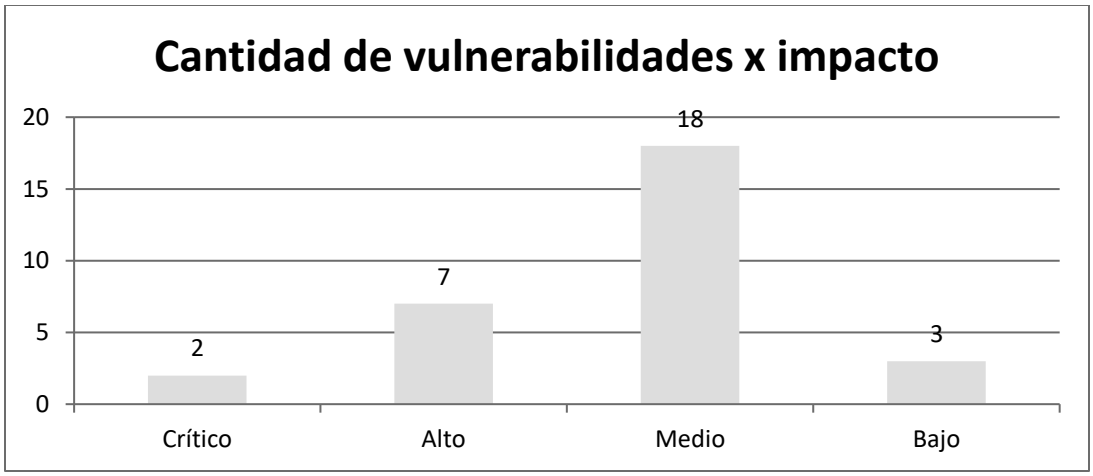


Figura 111. Vulnerabilidades x impacto

Las vulnerabilidades más severas identificadas fueron las involucradas con la carga de ficheros maliciosos en las cuentas de todos los usuarios a través del widget de tipo image y la combinación de estas con las vulnerabilidades que permiten la carga de URL's maliciosas en los dahsboards y reportes de cualquier usuario, puesto que estas podrían conducir al robo de cuentas de los clientes, pérdida de información sensible o al compromiso total de las organizaciones de los usuarios.

El listado de vulnerabilidades y nivel de riesgo asignado se aprecian en la siguiente tabla:

Categoría (actividad maliciosa)	Vulnerabilidades encontradas	Riesgo
5.1.8. Carga de ficheros maliciosos a las cuentas de todos los usuarios	2	Crítico
Combinación de 5.1.8 y 5.1.9		Crítico

5.1.4. Modificación de los dashboards y reportes de los usuarios a través de la eliminación y creación de widgets	3	Alto
5.1.9. Carga de URL's maliciosas en los dashboards y reportes de cualquier usuario	2	Alto
5.1.2. Creación de dominios y sondas a cualquier domino/usuario	1	Alto
5.2.2. Creación de cuentas con privilegio de administrador a cualquier organización	1	Alto
5.1.1. Obtención del listado y configuración de todos los dominios y sondas	7	Medio
5.1.6. Obtención del listado de todos los usuarios	2	Medio
5.1.10. Edición y borrado de alarmas	2	Medio
5.1.3. Obtención de la configuración de los dashboards de cualquier usuario	1	Medio
5.1.5. Obtención de los ID's de los usuarios activos en la solución	1	Medio
5.1.7. Eliminación de las notificaciones de todos los usuarios	1	Medio
5.1.12. Divulgación de IP's locales	1	Medio
5.1.13. Ataques de downgrade, SSL-stripping man-in-the-middle attacks y secuestro de cookies	1	Medio
5.1.15. Almacenamiento de información confidencial en la memoria caché local	1	Medio
5.2.1. Divulgación de ID's de organizaciones activas	1	Medio
5.1.11 Creación de dominios de distintos tipos (diferentes de los habilitados)	1	Bajo
5.1.14. Divulgación de dominios no oficiales	1	Bajo
5.1.16. Obtención de credenciales a través del formulario de inicio de sesión con autocomplete habilitado	1	Bajo

Tabla 10. Listado de vulnerabilidades y riesgo asociado

Considerando las vulnerabilidades críticas, altas y de riesgo medio halladas durante la prueba de penetración, así como el éxito de los ataques expuestos en la fase de explotación, se determinó que el nivel global de riesgo para la solución Redborder versión cloud es ALTO.

8.1.6. Recomendaciones

Con base en las vulnerabilidades y nivel de riesgo global, se emiten las siguientes recomendaciones:

Recomendaciones a corto plazo

- Mitigar todas las vulnerabilidades presentadas en este documento, priorizando las de mayor nivel de criticidad y dejando hasta el último aquellas que representan un bajo nivel de riesgo.
- Revisar el código fuente de la aplicación, configuraciones, tecnologías usadas y contenido activo puesto que podrían descubrirse diversas vulnerabilidades que no fueron susceptibles de ser encontradas durante la auditoría de caja gris. Para la revisión y evaluación del estado de seguridad de las soluciones y tecnologías se pueden usar las siguientes metodologías: **OWASP Testing Guide y OWASP Code Review Guide.**

Recomendaciones generales

- Implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) que mantenga a la organización en un entorno de riesgo gestionado, es decir, en el umbral de riesgo aceptado por Eneo Tecnología, a través de un seguimiento continuo y una inversión proporcional y justificada.
- Crear un comité de seguridad formado por diferentes responsables dentro de la organización el cual tomará las decisiones en cuanto a seguridad de la información. Algunas de las funciones serán: desarrollar las políticas, normas y responsabilidades en materia de seguridad de la información, validar el plan de seguridad de la información y presentarlo a aprobación a la Dirección, validar el modelado de riesgos y las acciones de mitigación propuestas por el responsable de seguridad, revisar las incidencias más destacadas, entre otras actividades.
- Crear e implementar una estrategia de desarrollo de software seguro que incorporé un estándar de codificación segura como la descrita en el estándar **OWASP Developer Guide.**
- Crear e implementar un programa de aseguramiento de la calidad del software que permita una eficaz identificación y eliminación de vulnerabilidades durante la etapa de desarrollo, la cual incluiría actividades tales como pruebas de penetración, pruebas de fuzzing, y auditorías de código fuente, etc.

- Asegurar que todo software desarrollado por la organización este sujeto a un proceso de control de calidad que incluya métricas de seguridad como parte del modelo de evaluación. De igual forma, que para el análisis de adopción de un software de terceros (aplicación, framework, plugin, ..) se incluya dentro de las métricas un apartado concerniente a la seguridad.
- Establecer un canal que permita estar atentos a los cambios y actualizaciones de las tecnologías usadas en la aplicación, con la finalidad de que el equipo involucrado (desarrolladores, mánagers, ingenieros,…) conozca las últimas noticias concernientes a problemas de seguridad y este consciente de los riesgos que implican. Y de este modo, el responsable de seguridad de la información pueda controlar la gestión de riesgos de nuevos proyectos y velar por el desarrollo seguro de las soluciones con un mayor apoyo por parte del resto del personal.

8.2. Informe técnico

El informe técnico describe en detalle el alcance, la información, la trayectoria de ataques, impacto y debe estar compuesto por las siguientes secciones:

- introducción,
- resultados de la fase de recopilación de información -expuesto en el apartado 3. Reconocimiento-,
- evaluación de las vulnerabilidades – correspondiente al apartado 5.4. Impacto de las vulnerabilidades detectadas conforme al sistema CVSS 3.0-,
- resultados de la fase de explotación -expuesto en el apartado 6. Explotación-,
- ejemplos para realizar la fase de post-explotación – expuestos en el apartado 7. Post-explotación - y
- riesgo de exposición –equivalente al apartado 8.1.5 Nivel de riesgo-.

Dado que cada una de las secciones de arriba ya se han explicado en apartados anteriores, se optó por evitar el duplicado de contenido y solamente mencionar la estructura que debe contener.

9. Conclusiones

El presenta trabajo permitió conocer en mayor profundidad las fases para llevar a cabo una prueba de penetración con base en la metodología PTES, se detectaron con éxito diversas vulnerabilidades que van desde el nivel de riesgo crítico hasta el bajo, además, en la fase de explotación y post-explotación se logró con éxito ejemplificar diferentes tipos de ataques.

Cabe menciona que a pesar de que fueron halladas muchas vulnerabilidades de nivel alto y medio, es necesario que se realice una auditoría de caja blanca con el propósito de analizar componentes que no fueron estudiados ya sea porque estaban fuera del alcance de la prueba o por falta de tiempo, pues su estudio implicaba un mayor nivel de conocimiento en técnicas como reversing y requerían un análisis más detallado, como muestra de esta situación están los componentes proxy e IPS de Redborder. Esta recomendación es una oportunidad para ampliar el alcance de las futuras pruebas de penetración y en consecuencia fortalecer la seguridad de la solución Redborder versión cloud, ya que como sabemos la gestión de la seguridad es un proceso de mejora continua y por ello, estas pruebas de penetración deben realizarse de forma periódica como parte de los controles establecidos dentro del marco del Sistema de Gestión de la Seguridad de la Información.

10. Bibliografía consultada

1. Daniel, P. F. & Dot, a T. Análisis y Modelado de Amenazas Tabla de contenido. (2006).

2. OWASP. Code Review Guide, V1.1. 1–234 (2008). at <https://www.owasp.org/images/f/fd/Code_review_guide_singleColumn_V05_%281%29.pdf>

3. Hewitt, J., Odvarko, J., Robcee & Firebug Working Group. Firebug. at <https://addons.mozilla.org/es/firefox/addon/firebug/>

4. HHD Free Hex Editor Neo. at <https://www.hhdsoftware.com/free-hex-editor>

5. Normalisation, P. L. InfoSec Reading Room. *Network*

6. Metasploit. at <https://www.metasploit.com/>

7. Microsoft Threat Modeling Tool 2016. at <https://www.microsoft.com/en-us/download/details.aspx?id=49168>

8. Steven van der Baan & Chesney, B. OWASP Developer Guide. *OWASP* at <https://github.com/OWASP/DevGuide>

9. Zimmer, D. PDF Stream Dumper. at <http://sandsprite.com/blogs/index.php?uid=7&pid=57>

10. Penetration Testing Execution Standard- PTES. at <http://www.pentest-standard.org/index.php/Main_Page>

11. Meucci, M. & Muller, A. Testing Guide 4.0. (2014). at https://www.owasp.org/images/1/19/OTGv4.pdf

11. Anexos entregados a la empresa

A continuación se listan los anexos entregados a la empresa Eneo Tecnología, por cuestiones de confidencialidad no se adjuntan en el TFM:

- Correspondiente a la fase de reconocimiento

    - Anexo A: Resultado de escaneos por nmap, who is, nslookup, traceroute, tracert, Google Hacking, revisión del portal Redborder.com
    - Anexo B. Resultado de escaneo de Maltego
    - Anexo C. Resultado de escaneo de SpiderFoot
    - Anexo D. Documentos con información sensible sobre tecnología y arquitectura de Redborder

- Correspondiente a la fase de modelado de datos

    - Anexo E: Diagrama de Flujo de Datos de la solución Redborder versión cloud.

- Correspondiente a la fase de análisis de vulnerabilidades

    - Anexo F. Estructura de dominios y sondas en Redborder versión cloud
    - Anexo G. Reporte enviado al equipo de soporte sobre las vulnerabilidades descritas en el apartado 5.2
    - Anexo H. Ficheros malicioso creados para realizar las validaciones de las vulnerabilidades de los apartado 5.1.8 y 5.1.9