INFORME DE PRUEBAS DE ETHICAL HACKING PRODUCCIÓN ELEFANTES BLANCOS ADMINISTRADOR SOLUCIONES MÓVILES 4 PROYECTO FÁBRICA DE SOFTWARE GRUPO 2

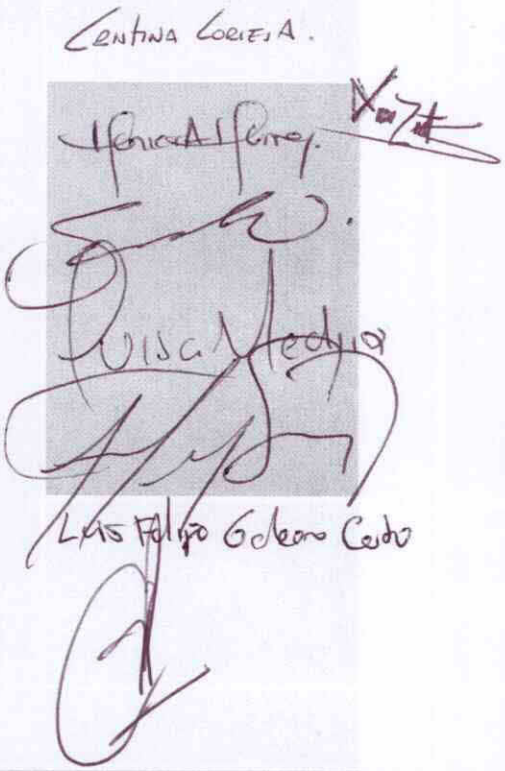
Soluciones y Servicios Tecnológicos
Dirección de Gobierno en línea

Bogotá, D.C, abril de 2014

FORMATO PRELIMINAR AL DOCUMENTO

Título:	**INFORME DE PRUEBAS DE ETHICAL HACKING**				
Fecha elaboración aaaa-mm-dd:	2014-04-03				
Sumario:	Este documento describe las pruebas de Ethical Hacking realizadas a la solución Elefantes Blancos Administrador del proyecto Soluciones Móviles 4.				
Palabras Claves:	Informe, pruebas, Ethical Hacking, producción.				
Formato:	DOC		Lenguaje:		Español
Dependencia:	Ministerio de Tecnologías de la Información y las Comunicaciones: Dirección de Gobierno en línea – Soluciones y Servicios Tecnológicos				
Código:	GLFS2-SM4-INF	Versión:	2.0	Estado:	Aprobado
Categoría:					
Autor (es):	Cristina Cortes Albadan Líder Técnico UT Software Works				
Revisó:	Mónica Monroy Consultor Procedimientos y herramientas de Interventoría Consorcio S&M Jorge Santiago Moreno Dirección de Gobierno en línea Luisa Fernanda Medina Dirección de Gobierno en línea Fernando Segura Asesor Secretaría de Transparencia				
Aprobó:	Luis Felipe Galeano Arquitecto IT Consorcio S&M Rafael Londoño Dirección de Gobierno en línea				
Información Adicional:	No Aplica				
Ubicación:	El archivo magnético asociado al documento está localizado en el repositorio de la solución 24 – SOLUCIONES MOVILES 4 en la siguiente ruta: 03. Fase de Ejecucion / 06.Produccion / 01. Entrega / 02. Pruebas de Seguridad				

Firmas:



CONTROL DE CAMBIOS

VERSIÓN	FECHA	No. SOLICITUD	RESPONSABLE	DESCRIPCIÓN
1.0	2014-04-03	No aplica	UT Software Works	Creación del documento
2.0	2014-04-14	No aplica	UT Software Works	Aprobación del documento

TABLA DE CONTENIDO

LISTA DE FIGURAS

.

1. INTRODUCCIÓN

Este documento presenta el informe de los resultados obtenidos en la ejecución de las pruebas de Ethical Hacking realizadas a los Servicios Web y la aplicación Elefantes Blancos Administrador, instalada en el ambiente de producción en la entidad Synapsis.

Las pruebas de vulnerabilidad permitieron identificar las vulnerabilidades en los componentes objetivos de estas pruebas para la solución Elefantes Blancos Administrador. Las pruebas de Ethical Hacking buscan explotar esas vulnerabilidades.

2. INFORME DE PRUEBAS DE ETHICAL HACKING

Las pruebas de Ethical Hacking, buscan medir el impacto real de las vulnerabilidades identificadas en las pruebas, por medio de la explotación de las mismas.

La explotación de vulnerabilidades encontradas, se realiza de manera controlada, buscando comprometer los principios de la seguridad de la información, contenida en la aplicación, sin generar ataques de negación de servicio a la plataforma.

Las pruebas fueron realizadas en su gran mayoría sin acceso privilegiado a la aplicación, como lo realizaría cualquier atacante, los accesos con los usuarios proporcionados para las pruebas, se realizaron para comprobar vulnerabilidades específicas de autenticación o de elevación de privilegios.

2.1 EXPLOTACIÓN DE VULNERABILIDADES

2.1.2 Inyección de Código

- **Tipo de Vulnerabilidad**: Inyección de Código
- **Descripción**: Es posible realizar intentos de inyección de código en campos específicos del servicio, lo cual puede generar ataques más avanzados si el código es procesado de alguna manera por elementos que puedan interpretarlo por fuera del dominio de los servicios web.
- **Detalles**: Se muestran los resultados de la inyección generada.

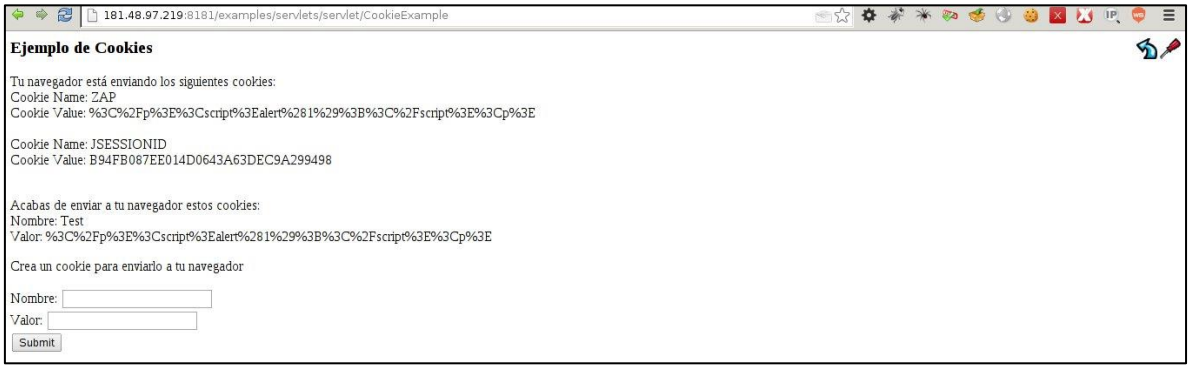


Figura 1. Ejemplo de cookies

Figura 2. Ejemplo de sesiones

- **Impacto**: Medio
- **Recomendaciones**: Hacer filtrado de peticiones que no se encuentren dentro del alcance del servicio, con el fin de evitar respuestas inesperadas del mismo o ejecución de sentencias en la base de datos o el mismo servidor, como esta vulnerabilidad hace parte de la configuración del servidor web se recomienda eliminar las carpetas.

3. CONCLUSIONES

A continuación se presentan las conclusiones de la presente etapa, generando recomendaciones generales, para la mitigación de las vulnerabilidades identificadas en la misma.

- Para el paso a producción de la solución Elefantes Blancos Administrador, se necesita asegurar la capa de transporte de la misma, tanto para servicio como aplicación, para prevenir la fuga de información de autenticación en estos dos elementos, la cual se realizará en la fase de ajustes de seguridad de credenciales.

- Se debe proteger la aplicación en búsqueda de protección de posibles vulnerabilidades enfocadas a inyección de código en los campos disponibles en la misma, eliminando las carpetas de ejemplos de los servidores desplegados.