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

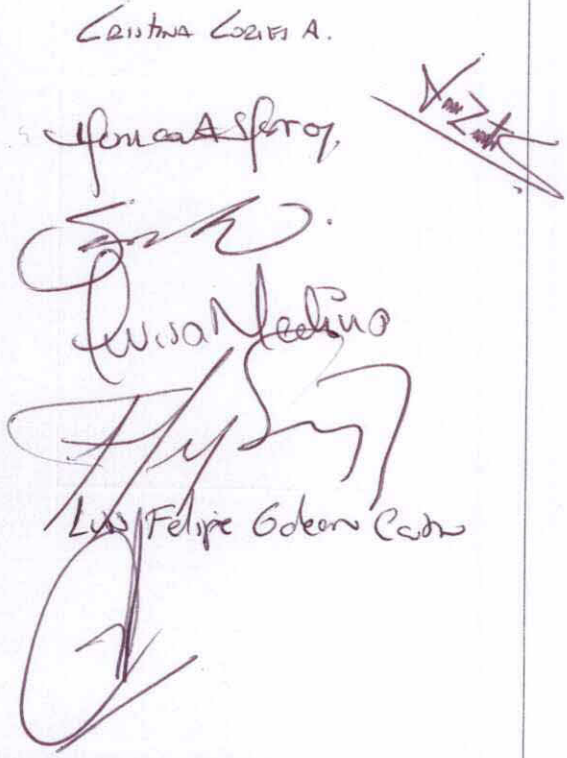
Soluciones y Servicios Tecnológicos
Dirección de Gobierno en línea

Bogotá, D.C, mayo de 2014

FORMATO PRELIMINAR AL DOCUMENTO

Título:	**INFORME DE PRUEBAS DE VULNERABILIDAD**				
Fecha elaboración aaaa-mm-dd:	2014-04-03				
Sumario:	Este documento presenta el resultado de las pruebas de vulnerabilidad realizadas a la aplicación Elefantes Blancos Administrador del proyecto Soluciones Móviles 4.				
Palabras Claves:	Informe, Pruebas, Vulnerabilidad, producción.				
Formato:	DOC		Lenguaje:		Español
Dependencia:	Ministerio de Tecnologías de la Información y las Comunicaciones: Dirección 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	2014-04-02	No aplica	UT Software Works	Creación del documento
1.1	2014-04-08	No aplica	UT Software Works	Ajustes solicitados por Interventoría, GEL y Entidad
1.2	2014-04-25	No aplica	UT Software Works	Ajustes solicitados por Interventoría, GEL y Entidad
2.0	2014-05-05	No aplica	UT Software Works	Aprobación del documento

TABLA DE CONTENIDO

LISTA DE TABLAS

1. INTRODUCCIÓN

En este documento, se presentan los resultados de las pruebas de vulnerabilidad realizadas para los componentes “Servicios Web” y “Elefantes Blancos Administrador” de la solución Elefantes Blancos Administrador en su ambiente de producción.

Dentro de este informe, se documentan las vulnerabilidades encontradas a nivel de aplicación para el administrador web y a nivel de servicios en la solución Elefantes Blancos Administrador.

El desarrollo de las pruebas incluye: pruebas a nivel de la aplicación, vulnerabilidades a nivel de código para las aplicaciones de la solución. El objetivo de estas pruebas es determinar las vulnerabilidades en los componentes objetivos y documentar las mismas, seguidas de la generación de recomendaciones específicas para su mitigación. La explotación de las vulnerabilidades se hace en las pruebas de Ethical Hacking que se encuentran documentadas en otro informe para esta solución.

La presentación de las vulnerabilidades encontradas en la plataforma, muestra el nivel de las mismas y genera como conclusión unas recomendaciones para aseguramiento basado en el riesgo que genera cada una de ellas para la plataforma.

El informe busca documentar las pruebas realizadas, y los resultados de cada una de ellas. Las pruebas son realizadas en base a las características propias de la aplicación y la plataforma. Todas las pruebas realizadas se basan en las metodologías usadas para el desarrollo de las pruebas (OSSTMM, SP800-115) y a nivel de aplicación es usado a nivel metodológico el Testing Guide de OWASP.

2. INFORME DE PRUEBAS DE VULNERABILIDAD

2.1 ESCENARIO DE LAS PRUEBAS

La plataforma en la que se encontraban alojados los componentes objetivos de estas pruebas de la solución Elefantes Blancos Administrador y a la que se le realizaron las pruebas de vulnerabilidad, es la suministrada y administrada por centro de datos de la entidad en su ambiente de producción.

Las pruebas se realizaron solo con base en los accesos generados para la realización de las mismas, para la revisión de servicios, fueron entregadas credenciales de autenticación con el fin de lograr el acceso a los mismos, y la realización de pruebas desde una perspectiva de autenticación y sin autenticación. Los objetivos evaluados se encontraban ubicados en:

http://www.elefantesblancos.gov.co:8080/elefantes-blancos-servicios

http://www.elefantesblancos.gov.con

2.2 FORMATOS Y HERRAMIENTAS

El formato para presentar las vulnerabilidades se muestra a continuación:

Tabla 1. Formato para presentación de Vulnerabilidades

Nombre de la Vulnerabilidad	
Nivel de Riesgo Calculado	
Critico	El acceso al sistema puede hacerse desde un sitio remoto sin requerir autenticación. El sistema sería fácil y seriamente comprometido de aprovecharse esta vulnerabilidad.
Alto	La explotación de la vulnerabilidad proveería acceso al sistema con privilegios de administración. El sistema seria seriamente comprometido.
Medio	La explotación de la vulnerabilidad permitiría acceso indirecto a datos o archivos de configuración.
Bajo	La explotación de la vulnerabilidad podría conducir al atacante a obtener estadísticas del sistema, cuentas de usuarios o alguna otra información sensitiva que ayudarían a ejecutar un ataque.
Información	Información complementaria
Puerto	Puerto donde se encontró la vulnerabilidad

Nombre de la Vulnerabilidad	
Nivel de Riesgo Calculado	
Categoría	Categoría a la que pertenece la vulnerabilidad
Descripción	Descripción de la vulnerabilidad
Impacto	Impacto que tendría la vulnerabilidad en caso de explotarse
Sistemas o Código Afectado	Sistemas, scripts o páginas web afectados por la vulnerabilidad afectados por la vulnerabilidad

La descripción de las vulnerabilidades, son presentadas al final del documento, como resumen de los hallazgos realizados, dentro de las tareas de las pruebas de vulnerabilidad.

Las herramientas utilizadas para el desarrollo de las pruebas incluyen.

Nmap

ZAP Proxy

PAROS Proxy

W3af

OWASP Mantra

Scripts manuales

Acunetix

SoapUI

Las pruebas realizadas se dividen en dos (2) sets (Elefantes Blancos Web y Servicios Web), cada uno enfocado a encontrar vulnerabilidades en cada uno de los componentes de manera independiente, las pruebas son ejecutadas para cada elemento, realizando revisiones específicas que buscan explotar las vulnerabilidades a nivel de servicio web o aplicación dependiendo del caso.

A continuación se presentan los resultados generales de las pruebas realizadas.

Tabla 2. Pruebas Realizadas a Nivel de Servicio

Prueba	Resultado
Inyección	No fueron detectadas vulnerabilidades en este grupo de pruebas.
Cross Site Scripting	No fueron detectadas vulnerabilidades en este grupo de pruebas
Manejo de Credenciales y Administración de Sesiones	Es necesario revisar el marcado de las cookies utilizadas en el esquema de autenticación.
Referenciación a Objetos de manera Insegura	No fueron detectadas vulnerabilidades en este grupo de pruebas
Cross SiteRequestForgery	No fueron detectadas vulnerabilidades en este grupo de pruebas
Malas Configuraciones de Seguridad	Fue encontrada una instalación por defecto del servidor Apache Tomcat en el servidor de producción, Fue posible identificar errores por defecto del servidor Web.
Fallos en las restricciones de acceso por medio de URL	No fueron detectadas vulnerabilidades en este grupo de pruebas
Protección Insuficiente a Nivel de Transporte	No fueron detectadas vulnerabilidades en este grupo de pruebas.
Redirecciones y reenvíos no validados	No fueron detectadas vulnerabilidades en este grupo de pruebas

Tabla 3. Pruebas Realizadas a Nivel de Aplicación

Prueba	Resultado
SQL Injection (Acceso)	No fueron detectadas vulnerabilidades en este grupo de pruebas
XPath Injection (Acceso)	No fueron detectadas vulnerabilidades en este grupo de pruebas
XML Malformados (Acceso)	No fueron detectadas vulnerabilidades en este grupo de pruebas
Transporte de Credenciales (Acceso)	No fueron detectadas vulnerabilidades en este grupo de pruebas
Caracteres Inválidos	No fueron detectadas vulnerabilidades en este grupo de pruebas
Xpath Injection	No fueron detectadas vulnerabilidades en este grupo de pruebas
Escaneo de Limites	No fueron detectadas vulnerabilidades en este grupo de pruebas
SQL Injection	No fueron detectadas vulnerabilidades en este grupo de pruebas
Uso de XML Malformados	No fueron detectadas vulnerabilidades en este grupo de pruebas
Fuzzing de XML	No fueron detectadas vulnerabilidades en este grupo de pruebas

A continuación se presenta la clasificación de cada una de las vulnerabilidades encontradas en la aplicación Elefantes Blancos Administrador. La descripción de

las vulnerabilidades incluye la información relacionada a la misma a nivel de resumen.

Tabla 4. Documentación de Vulnerabilidades

Instalación por Defecto
Medio
8080 - 443
Recolección de Información
Es posible acceder a toda la documentación del Apache Tomcat instalado en el servidor de producción, ya que no fue eliminado el acceso a toda la documentación por defecto del servidor web
Recolección de Información
http://www.elefantesblancos.gov.co:8080/elefantes-blancos-servicios http://www.elefantesblancos.gov.co
Excepciones en Ejecución
Medio
443
Recolección de Información – Ejecución de Código
Fue posible identificar excepciones de ejecución, realizando peticiones especificas al servidor, las cuales no son interpretadas de manera correcta por el mismo
Recolección de Información
http://www.elefantesblancos.gov.co
Errores por Defecto
Medio
8080 - 443
Recolección de Información
No se encuentran establecidos errores personalizados para la respuesta a recursos no existentes en el servidor.
Recolección de Información

http://www.elefantesblancos.gov.co:8080/elefantes-blancos-servicios http://www.elefantesblancos.gov.co
Configuración de Cookies
Bajo
443
Fuga de Información
La configuración de la cookie permite su transporte por medio de conexiones inseguras
Fuga de Información de Autenticación
http://www.elefantesblancos.gov.co

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.

- Se debe eliminar toda la documentación que no sea necesaria para el correcto funcionamiento del servidor, la documentación que sea necesaria, solamente debe ser consultada desde redes de confianza.

- Se debe establecer un esquema general de errores para toda la aplicación, que evite la posible fuga de información del servidor web.

- Se deben proteger las cookies, ya que son los elementos utilizados para la generación de sesiones en la autenticación del servidor.

- Se debe limitar el procesamiento de peticiones al servidor, teniendo en cuenta solamente peticiones válidas dentro del funcionamiento de la aplicación.

- El grupo de desarrollo de la UTSW revisará y realizará los ajustes de las vulnerabilidades halladas en las presentes pruebas, e implementara los cambios en el ambiente de producción del centro de datos de la Entidad.