

Logo ubiquandoINFORME DE PRUEBAs DE VULNERABILIDAD PREPRODUCCIÓN

ELEFANTES BLANCOS administrador

soluciones móviles 4

PROYECTO FÁBRICA DE SOFTWARE GRUPO 2

Soluciones y Servicios Tecnológicos

Dirección de Gobierno en línea

@República de Colombia – Derechos Reservados

Bogotá, D.C, abril de 2014



FORMATO **PRELIMINAR** AL DOCUMENTO

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Título: | **INFORME DE PRUEBAS DE VULNERABILIDAD** | | | | | | |
| Fecha elaboración aaaa-mm-dd: | 2014-03-27 | | | | | | |
| Sumario: | Este documento presenta el resultado de las pruebas de vulnerabilidad realizadas al proyecto Soluciones Móviles 4, aplicación Elefantes Blancos Administrador en preproducción. | | | | | | |
| Palabras Claves: | Informe, Pruebas, Vulnerabilidad, Preproducción. | | | | | | |
| 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 | | | Firmas: | |  | |
| 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 / 05. Preproduccion / 01. Entrega / 02. Pruebas de Seguridad | | | | | | |

CONTROL DE CAMBIOS

| **VERSIÓN** | **FECHA** | **No. SOLICITUD** | **RESPONSABLE** | **DESCRIPCIÓN** |
| --- | --- | --- | --- | --- |
| 1.0 | 2014-03-27 | No aplica | UT Software Works | Creación del Documento |
| 1.1 | 2014-04-21 | No aplica | UT Software Works | Ajustes solicitados por Interventoría, GEL y Entidad |
| 1.2 | 2014-04-24 | No aplica | UT Software Works | Ajustes solicitados por Interventoría, GEL y Entidad |
| 2.0 | 2014-04-29 | No aplica | UT Software Works | Aprobación del documento |

TABLA DE CONTENIDO

[1. INTRODUCCIÓN 6](#_Toc383618306)

[2. INFORME DE PRUEBAS DE VULNERABILIDAD 7](#_Toc383618307)

[2.1 ESCENARIO DE LAS PRUEBAS 7](#_Toc383618308)

[2.2 FORMATOS Y HERRAMIENTAS 7](#_Toc383618309)

[3. CONCLUSIONES 12](#_Toc383618310)

LISTA DE tablas

[Tabla 1. Formato para presentación de Vulnerabilidades 7](#_Toc386616414)

[Tabla 2. Pruebas Realizadas a Nivel de aplicación de Elefantes Blancos Web 8](#_Toc386616415)

[Tabla 3. Pruebas Realizadas a Nivel de aplicación de Servicios Web 9](#_Toc386616416)

[Tabla 4. Documentación de Vulnerabilidades 10](#_Toc386616417)

.

1. INTRODUCCIÓN

E

n este documento, se presentan los resultados de las pruebas de vulnerabilidad realizadas a la solución Elefantes Blancos Administrador en su ambiente de preproducción.

El desarrollo de las pruebas incluye: pruebas a nivel de la aplicación, vulnerabilidades a nivel de código y revisión de servicio(s) web. El objetivo de estas pruebas es determinar las vulnerabilidades en los componentes y documentarlas, 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 el informe correspondiente 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 con base en 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.

1. INFORME DE PRUEBAS DE VULNERABILIDAD
   1. ESCENARIO DE LAS PRUEBAS

La plataforma en la que se encuentran 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 UT SoftwareWorks en su ambiente de preproducción.

Las pruebas se realizaron 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 objetos evaluados se encontraban ubicados en:

<http://181.48.97.219:8181/elefantes-blancos-serviciospreproduccion>

<http://181.48.97.218:8090/Account/Login>

* 1. 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 |
| **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, se presenta al final del documento, como resumen de los hallazgos realizados, dentro de las tareas de las pruebas de vulnerabilidad la aplicación Elefantes Blancos Administrador.

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, 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 aplicación de Elefantes Blancos Web*

| **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 | Se debe realizar la autenticación para la plataforma de administración solamente en redes seguras. |
| 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 | No fueron detectadas vulnerabilidades en este grupo de pruebas |
| 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 | Es necesario revisar la protección a nivel de transporte de credenciales en la aplicación de administración o realizar la conexión solamente dentro de redes seguras |
| Redirecciones y reenvíos no validados | No fueron detectadas vulnerabilidades en este grupo de pruebas |

*Tabla 3. Pruebas Realizadas a Nivel de aplicación de Servicios Web*

| **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) | En producción es necesario asegurar las credenciales a nivel de transporte |
| 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 | El uso de algunos XML malformados dan respuestas inesperadas de parte del servicio. |
| Fuzzing de XML | El uso de algunos XML no esperados por el servicio dan respuestas inesperadas de parte del mismo. |

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*

|  |
| --- |
| Errores Generados por peticiones Maliciosas |
| Bajo |
| 8181 |
| Fuga de Información |
| Por medio del envío de peticiones maliciosas, malformadas o fuera del estándar, es posible obtener información del servicio web de errores generados, no fue posible comprometer el servicio de ninguna manera, pero es posible encontrar información específica del servidor o el servicio dentro de los errores |
| Ataques específicos a servicio web – Recolección de Información |
| <http://181.48.97.219:8181/elefantes-blancos-serviciospreproduccion> |
| Error en la aplicación |
| Bajo |
| 8090 |
| Fuga de Información |
| Es posible realizar ciertas excepciones en la aplicación, donde el procesamiento de la solicitud no permite la carga del error personalizado y se identifica un error por defecto en la aplicación. |
| Ataques específicos a servidor web – Recolección de Información |
| <http://181.48.97.218:8090/Account/Login> |
| Transporte de Credenciales sin Protección en la capa de Transporte |
| Bajo |
| 8090, 8181 |
| Secuestro de sesión, Fuga de información |
| Es posible obtener las credenciales de autenticación, porque no existe protección a nivel de transporte en la aplicación o servicio web. Esta vulnerabilidad se presenta en las pruebas en preproducción, pero es un elemento de seguridad que debe estar presente a nivel de producción. |
| Robo de información de autenticación de usuarios legítimos |
| <http://181.48.97.218:8090/Account/Login>  <http://181.48.97.219:8181/elefantes-blancos-serviciospreproduccion> |
| Atributo AUTOCOMPLETE Habilitado |
| Bajo |
| 8090 |
| Secuestro de sesión, Fuga de información |
| Fue posible identificar el atributo AUTOCOMPLETE habilitado en el formulario de autenticación, lo que puede permitir el robo de una sesión válida en un ataque a nivel de cliente. |
| Robo de información de autenticación de usuarios legítimos |
| <http://181.48.97.218:8090/Account/Login>  <http://181.48.97.219:8181/elefantes-blancos-serviciospreproduccion> |

1. 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.
* Se debe eliminar el atributo AUTOCOMPLETE de todos los formularios, con el fin de mitigar la posible exposición de los datos de autenticación en un posible ataque de lado del cliente.
* Se recomienda filtrar todas las peticiones innecesarias a los servicios, y definir un esquema de errores para cualquier petición no reconocida por los mismos, con el fin de no permitir que exista fuga de información alguna.
* Se debe revisar el procesamiento de las peticiones a la aplicación en búsqueda de que no se generen excepciones frente al esquema de errores planteado en la misma.
* El grupo de desarrollo de la UTSW revisará y realizará los ajustes de las vulnerabilidades halladas en las presentes pruebas; en la etapa de producción se realizarán las mismas pruebas donde se verán ajustadas estas vulnerabilidades.