INFORME DE PRUEBAS DE ETHICAL HACKING PREPRODUCCIÓN
YO CUIDO LO PÚBLICO 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:	2014-03-27				
Sumario:	Este documento describe las pruebas de Ethical Hacking realizadas a la aplicación Yo Cuido Lo Público Administrador del proyecto Soluciones Móviles 4 en ambiente de preproducción.				
Palabras Claves:	Informe, pruebas, Ethical Hacking, 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 Lusa Fernanda Medina Dirección de Gobierno 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	2014-04-14	No Aplica	UT Software Works	Ajustes solicitados por Interventoría, GEL y Entidad
1.2	2014-04-21	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

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 componentes de la solución Yo Cuido Lo Público Administrador, instalada en el ambiente de preproducción en las instalaciones de UT SoftwareWorks.

Las pruebas de vulnerabilidad permitieron identificar las vulnerabilidades en los componentes objetivos de estas pruebas las cuales se busca explotar mediante pruebas de Ethical Hacking.

2. INFORME DE PRUEBAS DE ETHICAL HACKING

Las pruebas de Ethical Hacking, buscan medir el impacto real de las vulnerabilidades identificadas en las pruebas de vulnerabilidad realizadas a la aplicación Yo Cuido Lo Público Administrador.

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 Yo Cuido Lo Público Administrador, como lo realizaría cualquier atacante, el acceso con los usuarios proporcionados para las pruebas, se realizó para comprobar vulnerabilidades específicas de autenticación o de elevación de privilegios.

2.1 EXPLOTACIÓN DE VULNERABILIDADES

2.1.1 Errores Generados por Peticiones Maliciosas

- **Tipo de Vulnerabilidad**: Recolección de Información
- **Descripción**: 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
- **Detalles**: Se realizaron ataques, donde fueron usadas peticiones malformadas, basadas en peticiones generales que se realizarían al servicio web y fue posible identificar errores generados por el mismo, sin compromiso del servicio.
- **Impacto**: Bajo
- **Recomendaciones**: Hacer filtrado de peticiones que no se encuentren dentro del alcance del servicio, con el fin de evitar respuestas inesperadas del mismo.

2.1.2 Error en la Aplicación

- **Tipo de Vulnerabilidad**: Recolección de Información
- **Descripción**: Es posible realizar ciertas excepciones en la aplicación Yo Cuido Lo Público Administrador, donde el procesamiento de la solicitud no permite capturar el error y desplegar una página con el mensaje personalizado y se identifica un error por defecto en la aplicación, en la cual aparece la carpeta “error” en la url de la imagen siguiente que hace parte de los valores por defectos iniciales.
- **Detalles**: Es posible generar errores de procesamiento en la aplicación.

Figura 1. Detalle errores de Procesamiento en la Aplicación.

- Fue posible generar el mismo error con las siguientes URL:
  - http://181.48.97.218:8090/error/notfound?aspxerrorpath=/Account
  - http://181.48.97.218:8090/error/notfound?aspxerrorpath=/bundles
  - http://181.48.97.218:8090/Usuario/RecuperacionContrasena
- **Impacto**: Bajo
- **Recomendaciones**: Revisar los errores generados por la aplicación en búsqueda de las excepciones que se están generando frente a estas peticiones que no permiten el procesamiento de los errores personalizados de la aplicación.

2.1.3 Transporte de Credenciales sin Protección en la Capa de Transporte

- **Tipo de Vulnerabilidad**: Fuga de credenciales de autenticación

- **Descripción**: 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.

- **Detalles**: No se realiza una conexión que permita la protección a nivel de transporte.

- **Impacto**: Alto

- **Recomendaciones**: Configurar el establecimiento de conexiones a nivel de producción por medio de túneles TLS para la aplicación.

2.1.4 Atributo AUTOCOMPLETE Habilitado

- **Tipo de Vulnerabilidad**: Fuga de credenciales de autenticación

- **Descripción**: 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.

- **Detalles**: Fue posible identificar el atributo en el formulario.

- **Impacto**: Bajo

- **Recomendaciones**: Deshabilitar el atributo en el formulario de autenticación.

3. CONCLUSIONES

A continuación se presentan las conclusiones de la presente etapa de la aplicación Yo Cuido Lo Público Administrador, generando recomendaciones generales, para la mitigación de las vulnerabilidades identificadas en la misma.

- Para el paso a producción de la aplicación Yo Cuido Lo Público Administrador, se necesita asegurar la capa de transporte de la misma, tanto para los servicios web como para la aplicación web, con el fin de evitar el robo de una sesión válido en estos dos elementos.

- Se recomienda 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 del 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 de 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.