REPORTE EJECUTIVO

Truerandom.bid

Elaboró: Leal González Ignacio

26/03/2019

Contenido

RESUMEN EJECUTIVO

Objetivos

- Identificar vulnerabilidades, vectores de ataque y riesgos que estos vectores de ataque pueden exponer, a la dirección IP 167.99.232.57.
- Listar las vulnerabilidades y los hallazgos encontrados.

Antecedentes

Se tomó el curso de “Pruebas de penetración”, siendo estas pruebas de penetración el proyecto final. La evaluación de seguridad involucra lo siguiente:

- Pruebas de penetración.

Alcances

- Solo se harán pruebas de penetración a la dirección IP de interés, no se harán pruebas de denegación de servicios, a los servicios que tenga montado la dirección IP.
- Se harán las pruebas de penetración del día 24 de marzo del 2019 al 25 de marzo del 2019 por el C. Leal González Ignacio.

Resumen de resultados

En la Tabla 1 se muestra un resumen de los resultados obtenidos divididos de acuerdo a la severidad de la vulnerabilidad, las pruebas de penetración fueron realizadas del 24 de marzo del 2019 al 25 de marzo del 2019, realizadas por el C. Leal González Ignacio.

Tabla 1. Resumen de vulnerabilidades encontradas.

Escala de riesgo	Número de vulnerabilidades
Critica	1
Alta	2
Regular	0
Baja	0
Informativa	0

Vulnerabilidades

En la Tabla 2, se muestran detalles de las vulnerabilidades encontradas.

Tabla 2. Detalles de las vulnerabilidades encontradas.

Riesgo	CVSS Base Score v 3.0	CVSS Temporal Score	Nombre	Servicio afectado
Alta	8.3	7.7	Se permite inicio de sesión anónimo de FTP.	FTP
Alta	8.3	7.7	Autenticación de la base de datos por bypass.	MySQL
Crítica	10	9.3	Ejecución de código remoto en Apache Struts 2	Apache Tomcat/ Coyote JSP