INFORME EJECUTIVO

PRUEBA DE PENTESTING

beisbolsafe.ddns.net

"La seguridad no es un producto, es un proceso constante"

ESTUDIANTES:

AMAURY RAFAEL ORTEGA CAMARGO

RAMIRO JOSE VERBEL DE LA ROSA

PRESENTADO A:

HEYBERTT MORENO

UNIVERSIDAD DE CARTAGENA

PROGRAMA DE INGENIERÍA DE SISTEMAS

Cartagena, Colombia

2017

1 Introducción

El presente documento pretende demostrar la falta de control y parámetros de seguridad en el manejo del servidor y demás elementos involucrados en la prestación de la aplicación web Liga de Béisbol, mostrando de forma inequívoca, las deficiencias encontradas en el manejo de contraseñas, posibilidad de accesos no autorizados al servidor, así como la deficiencia en el manejo de información sensible, la cual es enviada por la red sin el uso de elementos que aseguren su integridad, disponibilidad y confidencialidad.

2 Alcance de las pruebas

Se harán pruebas de penetración y análisis a sus resultados del servidor que alberga el sitio web *beisbolsafe.ddns.net*. Se centró en el servidor de almacenamiento, controladores de dominio, bases de datos y en la información que se envía por la red para conocer si es susceptible a un ciberataque, así como las personas que manejan estos elementos de red.

3 Objetivos

3.1 Objetivos Generales

- Identificar, analizar y documentar vulnerabilidades de la aplicación Liga de Béisbol.
- Documentar todas aquellas recomendaciones y configuraciones de seguridad necesarias para resolver las vulnerabilidades encontradas.
- Obtener información sensible que pueda ser usada de forma mal intencionada aprovechando las brechas de seguridad presentes en la aplicación web.

3.2 Objetivos Específicos

- Detectar vulnerabilidades y/o problemas de seguridad que puedan ser aprovechadas por los atacantes.
- Evaluar la efectividad y respuesta de los sistemas de seguridad implementados.
- Presentar recomendaciones concretas que permitan corregir los problemas y brechas de seguridad detectados y minimizar los riesgos asociados basados en los criterios de Confidencialidad, Disponibilidad, Integridad, Autenticidad, Responsabilidad, No repudio y Confiabilidad.
- Determinar el nivel de exposición presente en la red ante ataques que permitan obtener contraseñas de elementos de red importantes.
- Determinar la calidad de las contraseñas usadas para el acceso a servidores, y demás elementos de red.

4 Suposiciones iniciales

El sitio web utiliza PHP tecnología debido a que los desarrolladores son estudiantes de la Universidad de Cartagena en el programa Ingeniería de Sistemas donde en séptimo semestre los estudiantes tienen tendencias hacia PHP debido a los docentes previos a ese semestre.

5 Cronograma

Prueba de penetración	Fecha inicial	Fecha final	Encargado
Prueba de penetración 1	09/05/2017	11/05/2017	Amaury Rafael Ortega Camargo
Prueba de penetración 2	09/05/2017	11/05/2017	Ramiro Jose Verbel De La Rosa

6 Metodología

Se usaron diversas técnicas para testear el sistema de seguridad de la aplicación web, buscando los puntos débiles que permitieran ingresar y tener acceso a manipulación de la información con el fin de poder mejorar los sistemas de seguridad. Para esto se siguió la siguiente metodología basada en las etapas de OWASP Testing Guide v4 Web Application Penetration Testing:

- Recolección de información
- Detección de configuración y despliegue
- Detección de configuración y despliegue
- Pruebas para gestores de identidad
- Pruebas de autenticación
- Pruebas de autorización
- Pruebas de gestores de sesión
- Pruebas de validación de entradas
- Manejo de errores
- Criptografía
- Prueba de lógica de negocio
- Pruebas del lado cliente

7 Resumen de vulnerabilidades

Un factor de impacto calificativo (Critica, alta, media o baja) se ha asociado con cada vulnerabilidad, así como una asignación arbitraria del grado de habilidad que un atacante requiere para explotar la vulnerabilidad (Trivial, Moderado, difícil).

Impacto	Definición
Bajo	Mínimo impacto en la aplicación web. La información revelada no es perjudicial o de valor significativo.
Medio	Posible impacto, reputación e imagen de la aplicación web puede verse afectada.
Alto	Impacto en la aplicación web, se exponen datos de carácter privado, que comprometen la integridad de los usuarios y sistemas impactados.
Critico	Impacto en la aplicación web, se compromete la integridad del sistema por completo.

Dificultad de Explotación	Definición
Trivial	Herramientas de fácil disponibilidad para automatizar el descubrimiento y explotación.
Moderado	Requiere un cierto nivel de habilidad en la programación básica o secuencias de comandos y, o un grado de conocimiento y compresión de la plataforma de destino/software/aplicaciones, etc.
Difícil	La explotación requiere un atacante altamente calificado, motivado y apto.

Impacto	Numero de vulnerabilidades
Bajo	1
Medio	1
Alto	3
Critico	1

Vulnerabilidad	Impacto
X-Frame-Options Header Not Set	Bajo
Revelación de información privilegiada del servidor	Medio
Web Browser XSS Protection Not Enabled	Alto
Inyección Remota de Comandos OS	Alto
DDoS Capa 7 HTTP	Alto
Acceso no autorizado	Critico