INFORME TÉCNICO

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

Tabla de contenido

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 Herramientas

7.1 Navegadores web

Se usaron varios navegadores web para comprobar las secciones del sitio web usando palabras comunes para navegar y conocer el sitio.

7.2 URL Fuzzer / Spider

Se usó para automatizar el conocimiento de las secciones del sitio web usando diccionarios de palabras usadas provenientes de brechas informáticas en el pasado.

7.3 Whois/nslookup

Se usó para conocer para dirección IP e información Whois del servidor web que almacenaba beisbolsafe.ddns.net.

7.4 HTTPViewer

Se usó para detectar que sistema operativo estaba manteniendo el sitio web beisbolsafe.ddns.net y que información se encontraba en las cabeceras HTTP al momento de hacer una petición al servidor.

7.5 Whatweb

Se usó para obtener información más detallada respecto al servidor y el servicio web que mantenía al sitio web beisbolsafe.ddns.net. Además, para ver de rápida que cabeceras HTTP está usando y su impacto en el sitio.

7.6 DMitry

Se usó para automatizar el proceso de obtención de información whois, puertos abiertos e IP del servidor que almacenaba el sitio web beisbolsafe.ddns.net.

7.7 Smtp-user-enum

Se usó para comprobar la seguridad de servicios smtp.

7.8 Nmap

Se usó para detectar servicios estaban escuchando en determinados puertos abiertos al público en el servidor.

7.9 Sqlmap

Se usó para encontrar vulnerabilidades en la base de datos por medio de formularios relacionados con la base de datos.

7.10 Burp Suite

Se usó su proxy y Spider para modificar peticiones HTTP en vivo y encontrar secciones del sitio web no accesibles por la interfaz gráfica en el navegador web.

7.11 Maltego

Se usó para obtener información pública del servidor web en CTAS públicos usando la información recolectada por otros medios.

7.12 GoldenEye

Se usó para probar la protección contra ataques DDoS de capa 7 HTTP.

7.13 OWASP ZAP

Se usó para ejecutar descubrimiento de vulnerabilidades automático y generar reportes con recomendaciones.

8 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	Inyección Remota de Comandos OS
URL	http://beisbolsafe.ddns.net/Equipo/detalleEquipo/
Criticidad	Alto
Complejidad	Moderado

Descripción

Técnica de ataque usada para la ejecución no autorizada de comandos del sistema operativo. Este ataque es posible cuando una aplicación acepta la entrada que no es de confianza para construir comandos del sistema operativo de una manera insegura involucrando desinfección inadecuada de datos, y/o llamada inadecuada de programas externos.

Id	URL	Parámetro afectado	Payload
1	http://beisbolsafe.ddns.net/Equipo/detalleEquipo/14query=query%26timeout+%2FT+%7B0%7D%26	query	query&timeout /T {0}&
2	http://beisbolsafe.ddns.net/Equipo/detalleEquipo/5?query=query%22%26sleep+15%26%22	query	query"&sleep 15&"
3	http://beisbolsafe.ddns.net/Equipo/detalleEquipo/7?query=query%7Ctimeout+%2FT+15	query	query|timeout /T 15

Detalles

Vulnerabilidad detectada por OWASP ZAP 2.6.0 el 09/05/2017 11:34pm

Recomendación

Ejecutar los servicios web en un entorno separado al nivel del sistema operativo. Una alternativa para controlar las entradas y salidas es usar control de codificación ESAPI o similares. Usar filtrado de entradas usando una lista estricta de caracteres permitidos como solo alfanuméricos y espacios.

Vulnerabilidad	DDoS Capa 7 HTTP
URL	http://beisbolsafe.ddns.net/
Criticidad	Alto
Complejidad	Moderado
Descripción	
Es posible hacer ataques DDoS usando peticiones GET y POST sin terminar. Para probar esto se utilizó GoldenEye 1.2.0.	
Detalles	
Vulnerabilidad detectada por GoldenEye 1.2.0 el 09/05/2017 11:00pm	
Recomendación	
Modificar el servicio web para no permitir peticiones HTTP que demoren largo tiempo.	

Vulnerabilidad	Revelación de información privilegiada del servidor
URL	http://beisbolsafe.ddns.net/phpmyadmin
Criticidad	Medio
Complejidad	Trivial

Descripción

Es posible ver información sobre qué servicios se están usando asi como que versión se ejecutan usando un navegador web en la URL provista o usando nmap, HTTP Viewer, Whois, DMitry.

Puerto	Servicio	Version
22	SSH	OpenSSH 6.6.1p1
25	SMTP	
80	HTTP	Apache httpd 2.4.7
135	Msrpc	
139	Netbios-ssn	
443	HTTPS	OpenSSH 6.6.1p1
445	Microsoft-ds	
514	Shell	
3128	http-proxy	Squid http proxy 3.3.8
8080	http-proxy	Squid http proxy 3.3.8
9898	Monkeycom	

Usando whois se detectó que el dominio es provisto por ddns.net el cual re-direcciona a un VPS almacenado en Digital Ocean, Inc.

Detalles

Vulnerabilidad detectada por nmap, HTTP Viewer, Whois, DMitry el 09/05/2017 10:10pm

Recomendación

Utilizar servicios que protegen la información Whois para que herramientas de automatización no puedan acceder a esta sin pasar por un tercero.

Vulnerabilidad	Acceso no autorizado
URL	http://beisbolsafe.ddns.net/
Criticidad	Critico
Complejidad	Trivial
Descripción	
Es posible usar smtp-user-enum para hacer consultas sobre que correos electrónicos funcionan en dicho servidor.	
Detalles	
Vulnerabilidad detectada por smtp-user-enum 1.2 el 09/05/2017 10:30pm	
Recomendación	
Usar algún tipo de autenticación	

Vulnerabilidad	X-Frame-Options Header Not Set
URL	http://beisbolsafe.ddns.net/
Criticidad	Medio
Complejidad	Moderado

Descripción

El encabezado X-Frame-Options no está incluido en la respuesta HTTP para proteger contra ataques 'ClickJacking'.

Id	URL	Parámetro afectado	Payload
1	http://beisbolsafe.ddns.net/app/views/404.php	X-Frame-Options	ClickJacking
2	http://beisbolsafe.ddns.net/Usuario/index/ & /#	X-Frame-Options	ClickJacking
3	http://beisbolsafe.ddns.net/Partido/resultados/ & /#	X-Frame-Options	ClickJacking
4	http://beisbolsafe.ddns.net/Equipo/equipos/ & /#	X-Frame-Options	ClickJacking
5	http://beisbolsafe.ddns.net/Equipo/detalleEquipo/ & /#	X-Frame-Options	ClickJacking

Detalles

Vulnerabilidad detectada por OWASP ZAP 2.6.0 el 09/05/2017 11:34pm

Recomendación

La mayoría de los navegadores web modernos admiten el encabezado X-Frame-Options en la respuesta HTTP. Asegúrese de configurarlo en todas las páginas web que devuelve la aplicación (si espera que la página se enmarque sólo por las páginas de su servidor (por ejemplo, es parte de un FRAMESET), entonces usted querrá usar SAMEORIGIN, de lo contrario si nunca espera que la página se enmarque, usted debe usar DENY. ALLOW-FROM permite que sitios web específicos enmarquen la página web en el Navegadores Web soportado).

Vulnerabilidad	Web Browser XSS Protection Not Enabled
URL	http://beisbolsafe.ddns.net/
Criticidad	Alto
Complejidad	Moderado

Descripción

La protección XSS del navegador web no está habilitada o está deshabilitada por la configuración de la 'protección X-XSS' Encabezado de respuesta HTTP en el servidor web.

Id	URL	Parámetro afectado
1	http://beisbolsafe.ddns.net/app/views/404.php	X-XSS-Protection
2	http://beisbolsafe.ddns.net/Usuario/index/ & /#	X-XSS-Protection
3	http://beisbolsafe.ddns.net/Partido/resultados/ & /#	X-XSS-Protection
4	http://beisbolsafe.ddns.net/Equipo/equipos/ & /#	X-XSS-Protection
5	http://beisbolsafe.ddns.net/Equipo/detalleEquipo/ & /#	X-XSS-Protection

Otra Información: El encabezado de respuesta HTTP X-XSS-Protection permite al servidor web habilitar o deshabilitar el mecanismo de protección XSS del navegador web. Los siguientes valores intentarán habilitarlo:
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=http://www.example.com/xss
Los siguientes valores lo desactivarían:
X-XSS-Protection: 0
Actualmente, el encabezado de respuesta HTTP X-XSS-Protection está soportado en Internet Explorer, Chrome y Safari (WebKit). Tenga en cuenta que esta alerta sólo se plantea si el cuerpo de la respuesta potencialmente puede contener una carga útil XSS (con un tipo de contenido basado en texto, con una longitud distinta de cero).

Detalles

Vulnerabilidad detectada por OWASP ZAP 2.6.0 el 09/05/2017 11:34pm

Recomendación

Asegúrese de que el filtro XSS del navegador web esté habilitado, estableciendo el encabezado de respuesta HTTP X-XSS-Protection en '1'.

Vulnerabilidad	X-Content-Type-Options Header Missing
URL	http://beisbolsafe.ddns.net/
Criticidad	Bajo
Complejidad	Moderado

Descripción

El encabezado Anti-MIME-Sniffing X-Content-Type-Options no se estableció en 'nosniff'. Esto permite que versiones Internet Explorer y Chrome para realizar el sniffing MIME en el cuerpo de la respuesta, potencialmente el cuerpo de la respuesta ha de ser interpretado y visualizado como un tipo de contenido distinto al tipo de contenido declarado. Corriente (Principios de 2014) y las versiones heredadas de Firefox utilizarán el tipo de contenido declarado (si está establecido), en lugar de realizar MIME-sniffing.

Id	URL	Parámetro afectado
1	http://beisbolsafe.ddns.net/app/views/404.php	X-Content-Type-Options
2	http://beisbolsafe.ddns.net/Usuario/index/ & /#	X-Content-Type-Options
3	http://beisbolsafe.ddns.net/Partido/resultados/ & /#	X-Content-Type-Options
4	http://beisbolsafe.ddns.net/Equipo/equipos/ & /#	X-Content-Type-Options
5	http://beisbolsafe.ddns.net/Equipo/detalleEquipo/ & /#	X-Content-Type-Options
6	http://beisbolsafe.ddns.net/app/views/Default/estilos/estilos.css	X-Content-Type-Options
7	http://beisbolsafe.ddns.net/app/views/Default/js/modal.js	X-Content-Type-Options

Otra Información: Este problema aún se aplica a las páginas de tipo de error (401, 403, 500, etc.), ya que esas páginas a menudo se mantienen afectados por problemas de inyección, en cuyo caso sigue habiendo preocupación por los navegadores que olfatean páginas lejos de su tipo de contenido real.
En el umbral "Alto" este escáner no alertará sobre las respuestas de error del cliente o del servidor.

Detalles

Vulnerabilidad detectada por OWASP ZAP 2.6.0 el 09/05/2017 11:34pm

Recomendación

Asegúrese de que el servidor de aplicaciones web establezca el encabezado Content-Type apropiadamente y que X-Content-Type-Options a 'nosniff' para todas las páginas web.
Si es posible, asegúrese que los usuarios del sistema usen navegadores que no permitan la lectura de contenido por byte o MIME sniffing

9 Bibliografía

Lyon, G. (s.f.). *Nmap.Org*. Obtenido de Insecure.Org, Nmap.Org, SecLists.Org, y SecTools.Org: http://nmap.org/book/man.html

Mor-Pah.net. (s.f.). *DMitry*. Obtenido de http://mor-pah.net/software/dmitry-deepmagic-information-gathering-tool/

PATERVA. (s.f.). *Maltergo User-Guide*. Obtenido de paterva.com: https://paterva.com/web7/docs/userguides/user_guide.php

pentestmonkey. (s.f.). *smtp-user-enum*. Obtenido de http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum

Pentest-Tools.com. (s.f.). *Pentest-Tools.com*. Obtenido de https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files

PORTSWIGGER. (s.f.). *PORTSWIGGER WEB SECURITY*. Obtenido de https://portswigger.net/burp/help/suite_usingburp.html

Project, O. W. (s.f.). *OWASP*. Obtenido de https://www.owasp.org/index.php/Web_Application_Penetration_Testing

Security, M. (s.f.). *WhatWeb*. Obtenido de https://www.morningstarsecurity.com/research/whatweb

Swain, R. (s.f.). *Rex Swain's HTTP Viewer*. Obtenido de www.rexswain.com/httpview.html

Whois.com. (s.f.). *Whois.com*. Obtenido de https://www.whois.com/whois/