Informe de pruebas OWASP

Integrantes: Sebastián Orrego, Benjamín Mora, Francisco San Juan

Sección: SSC5501-004D

Profesor: Mauricio Vázquez

**Índice**

[Introducción 3](#_Toc517868044)

[Descripción del sitio para hacer las pruebas 3](#_Toc517868045)

[Descripción de pruebas 3](#_Toc517868046)

[Resultados de la prueba 3](#_Toc517868047)

[Detalles resultados OWASP 2017 4](#_Toc517868048)

[A1 – Inyección 4](#_Toc517868049)

[A2 – Pérdida de Autenticación y Gestión de Sesiones 4](#_Toc517868050)

[1. Almacenamiento de contraseñas 4](#_Toc517868051)

[A3 – Exposición de Datos Sensibles 4](#_Toc517868052)

[1. Criptografía 4](#_Toc517868053)

[A4 – Entidades Externa de XML (XXE) 4](#_Toc517868054)

[A5 – Pérdida de Control de Acceso 5](#_Toc517868055)

[1. Secuestro de clics: Cabecera X-Frame-Options faltante 5](#_Toc517868056)

[2. Ataque de adivinación de contraseña en autenticación 5](#_Toc517868057)

[A6 – Configuración de Seguridad Incorrecta 5](#_Toc517868058)

[1. Servicio Apache JServ 5](#_Toc517868059)

[2. Ataque de adivinación de contraseña en autenticación 5](#_Toc517868060)

[3. El método OPTIONS está habilitado 5](#_Toc517868061)

[A7 – Secuencia de Comandos en Sitios Cruzados (XXS) 6](#_Toc517868062)

[A8 – Deserialización Insegura 6](#_Toc517868063)

[A9 – Uso de Componentes con Vulnerabilidades Conocidas 6](#_Toc517868064)

[1. Servicio Apache JServ. 6](#_Toc517868065)

[2. Ataque de adivinación de contraseña en autenticación. 6](#_Toc517868066)

[3. El método OPTIONS está habilitado 6](#_Toc517868067)

[A10 – Registro y Monitoreo Insuficientes 6](#_Toc517868068)

# **Introducción**

Este informe ha sido desarrollado para el curso de **Seguridad en Sistemas Computaciones** cursado en el primer semestre del año 2018, clase impartida por el profesor Mauricio Vázquez.

Se analiza un sitio web propio con las pruebas OWASP para obtener el resultado de los diez riesgos más críticos de Aplicaciones Web.

Usaremos el sitio web <http://www.cittsb.cl:8080/InasistenciaTest/> es una aplicación web en su versión test, creada para la administración de Duoc UC San Bernardo en la toma de inasistencia de todos los alumnos de la misma sede, más de 7000 alumnos.

Para el análisis OWASP haremos un escáner con la aplicación web “Acunetix Web Vulnerability Scanner” esta aplicación web analiza la seguridad del sitio web y aplicaciones web contra ataques de piratas informáticos.

# **Descripción del sitio para hacer las pruebas**

El sitio consiste en un sistema de registro de inasistencia, desarrollado en JSP (*Java EE*), cuenta con autenticación (*login*) para acceder a sus funciones principales. Se comunica a una base de datos en MySQL y usa diversos *frameworks* en (*javascript, cs*s) para adaptar el diseño a distintas plataformas (*escritorio y dispositivos móviles*).

# **Descripción de pruebas**

Se realizo una prueba utilizando el software Accunetix, la prueba consiste en un Escaneo Completo (full scan) a la url del sitio web <http://www.cittsb.cl:8080/InasistenciaTest/> y tuvo una duración de 6 minutos y 41 segundos.

# **Resultados de la prueba**

Accunetix entrego como resultado principal un nivel de amenaza 2, esto es una o más vulnerabilidades consideradas medias – severas

# **Detalles resultados OWASP 2017**

|  |  |  |
| --- | --- | --- |
|  | **Nombre** | **N° Alertas** |
| **A1** | **Inyección** | **0** |
| **A2** | **Pérdida de Autentificación** | **1** |
| **A3** | **Exposición de datos sensibles** | **1** |
| **A4** | **Entidades Externas XML (XXE)** | **0** |
| **A5** | **Pérdida de Control de Acceso** | **2** |
| **A6** | **Configuración de Seguridad Incorrecta** | **3** |
| **A7** | **Secuencia de Comandos en Sitios Cruzados (XSS)** | **0** |
| **A8** | **Deserialización Insegura** | **0** |
| **A9** | **Componentes con vulnerabilidades conocidas** | **3** |
| **A10** | **Registro y Monitoreo Insuficientes** | **0** |

**Realizamos la prueba de Accunetix en la versión OWASP 2013.**

**También realizamos pruebas que nosotros mismos sabíamos y que Accunetix no encontró como A1, A2,A3,A6 y A8**

## **A1 – Inyección**

No se presentaron alertar en esta categoría. El sitio utiliza JSP y se comunica con la base de datos a través de mapeo relación de datos (ORM) es decir, los datos ingresados por el usuario no son enviados directamente.

## **A2 – Pérdida de Autenticación y Gestión de Sesiones**

### Almacenamiento de contraseñas

Se almacenan las contraseñas con texto claro

## **A3 – Exposición de Datos Sensibles**

### Criptografía

No se utilizan algoritmo criptográfico para el almacenamiento de contraseñas en texto claro

## **A4 – Entidades Externa de XML (XXE)**

No se presentaron alertas en esta categoría. El sitio no utiliza XML para autenticación, ni tampoco servicios web basados en XML.

## **A5 – Pérdida de Control de Acceso**

Se registraron 2 alertas en esta categoría.

### Secuestro de clics: Cabecera X-Frame-Options faltante

Clickjacking (secuestro de clic) es una técnica maliciosa para engañar a un usuario web en apretar en algo diferente a lo que el usuario percibe que está presionando, y permite revelar información confidencial o tomar control del computador mientras se presiona en páginas web aparentemente inocuas.

El server no devolvió la cabecera x-frame-options lo cual significa que este sitio puede estar en riesgo de recibir este ataque de *Clickjacking*. Esta cabecera puede ser usada para indicar que un navegador puede o no dibujar una página dentro de una etiqueta *frame* o *iframe*.

### Ataque de adivinación de contraseña en autenticación

Una amenaza común que los desarrolladores enfrentan es un ataque de fuerza bruta para adivinar la contraseña. Un ataque de fuerza bruta es un intento de descubrir la contraseña probando sistemáticamente todas las combinaciones de caracteres posibles.

Esta página de autenticación no provee ninguna protección en contra de este tipo de ataques de fuerza bruta, se recomienda utilizar algún tipo de bloqueo para un numero definido de intentos incorrectos.

## **A6 – Configuración de Seguridad Incorrecta**

Se registraron 3 alertas en esta categoría.

### Servicio Apache JServ

El Protocolo JServ de Apache (AJP) es un protocolo binario que recibe solicitudes de un servidor web hacia un servidor de aplicación detrás de este. Se recomienda no tener servicios AJP accesibles públicamente en el internet. Si AJP está mal configurado, un atacante puede acceder a recursos internos.  
En el sitio *Inasistencia*, JSP corre en un servidor Apache Tomcat que utiliza el protocolo AJP y este esta accesible públicamente en el puerto 8009, lo que constituye un riesgo.

### Ataque de adivinación de contraseña en autenticación

Esta página de autenticación no provee ninguna protección en contra de este tipo de ataques de fuerza bruta, se recomienda utilizar algún tipo de bloqueo para un numero definido de intentos incorrectos.

### El método OPTIONS está habilitado

El método HTTP OPTIONS está habilitado en este servidor web. Este método provee una lista de métodos soportados por el servidor web, y representa una solicitud de información sobre los modos de comunicación disponibles o las cadenas de request/response identificables por el recurso URI.

## **A7 – Secuencia de Comandos en Sitios Cruzados (XXS)**

No se presentaron alertas en esta categoría.

## **A8 – Deserialización Insegura**

No se presentaron alertas en esta categoría. El sitio no usa serialización de objetos para manipulación de datos, tampoco utiliza aplicaciones que usen serialización.

## **A9 – Uso de Componentes con Vulnerabilidades Conocidas**

Se registraron 3 alertas en esta categoría.

### Servicio Apache JServ.

En el sitio *Inasistencia*, JSP corre en un servidor Apache Tomcat que utiliza el protocolo AJP y este esta accesible públicamente en el puerto 8009, lo que constituye un riesgo.

### Ataque de adivinación de contraseña en autenticación.

Esta página de autenticación no provee ninguna protección en contra de este tipo de ataques de fuerza bruta, se recomienda utilizar algún tipo de bloqueo para un numero definido de intentos incorrectos.

### El método OPTIONS está habilitado

El método HTTP OPTIONS está habilitado en este servidor web. Este método provee una lista de métodos soportados por el servidor web, y representa una solicitud de información sobre los modos de comunicación disponibles o las cadenas de request/response identificables por el recurso URI.

## **A10 – Registro y Monitoreo Insuficientes**

No se presentaron alertas en esta categoría. Sin embargo, el sitio no cuenta con registro de transacciones, ni inicios de sesión. Tampoco posee un sistema de monitorización y alerta en contra de acciones sospechosas.