Conference: Congreso Interdisciplinario de Energías Renovables - Mantenimiento Industrial - Mecatrónica e Informática

Booklets

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - E-Revistas - Google Scholar

DOI - REBID - Mendeley - DIALNET - ROAD - ORCID

Title: Implementación de mecanismos de seguridad en la aplicación web "BITA"

Authors: Luz María HERNÁNDEZ CRUZ, Ángel Leonardo MORA CANUL

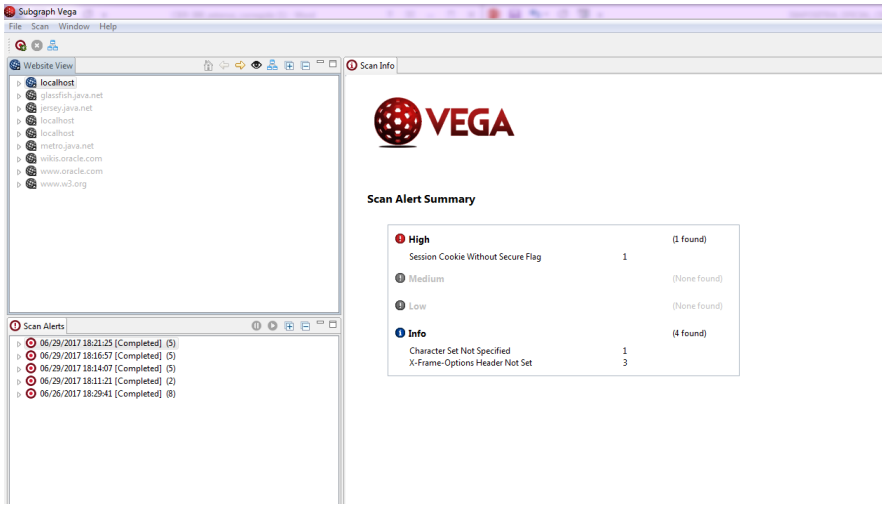
Editorial label ECORFAN: 607-8324
BCIERMIMI Control Number: 2017-02
BCIERMIMI Classification (2017): 270917-0201

Pages: *24*
Mail: *lmhernan@uacam.mx*
RNA: 03-2010-032610115700-14

La investigación tiene como objetivo primordial mitigar las vulnerabilidades en la aplicación web “BITA”

Esta investigación utiliza una metodología cualitativa, que inicia con el estudio del arte de la seguridad informática (SI) abarcando los conceptos básicos, la seguridad en sistemas de información (SSI), los diferentes tipos de ataques informáticos y los principales mecanismos de seguridad.

Con el uso de la herramienta VEGA se identifican las vulnerabilidades en la aplicación y el equipo de desarrollo de software, utilizando la técnica Delphi

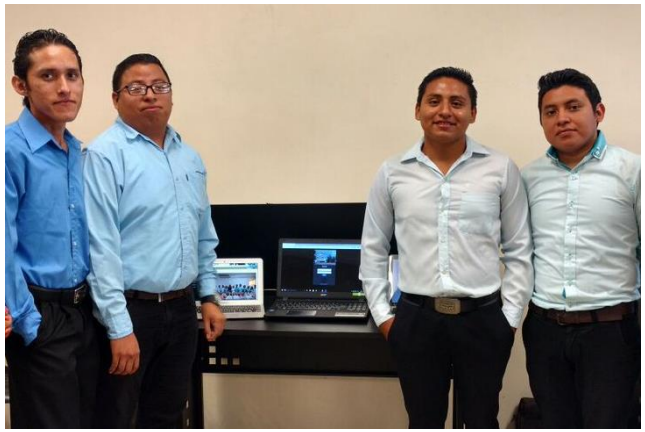


La Facultad de Odontología (FO)

Brinda servicios odontológicos para contribuir con la sociedad Campechana, ofreciendo atención dental especializada en cinco clínicas dentro de su campus.

FACULTAD DE ODONTOLOGÍA

BITA es una aplicación web diseñada por estudiantes de Ingeniería en Sistemas Computacionales (ISC) de la Facultad de Ingeniería (FI) que utiliza como lenguaje de programación JSP y como sistema gestor de base de datos MySQL.



Debido al tipo de información, de carácter crítico y confidencial, que involucra directamente la salud del paciente y el derecho a la privacidad de datos personales, surge la preocupación del personal directivo de la FO por analizar y mitigar los riesgos de seguridad dentro de aplicación web “BITA”.

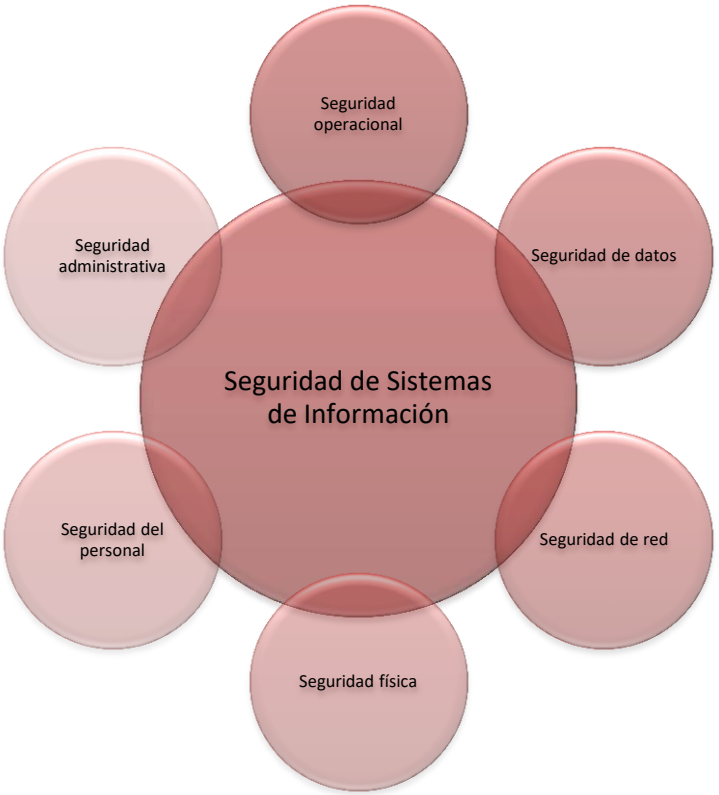
Esta investigación documenta la metodología y el análisis de vulnerabilidades de la aplicación web “BITA”, así como los mecanismos de seguridad propuestos para mitigar dichas vulnerabilidades

El presente estudio se divide en las secciones que se mencionan en seguida:

a) Justificación: Apoya la importancia significativa de la investigación.
b) Estudio del arte: Fundamento teórico acerca de la Seguridad en los Sistemas de Información (SSI).
c) Metodología: Expone paso a paso el desarrollo del estudio de la investigación.
d) Resultados: Enfatiza los beneficios obtenidos.

BITA es una aplicación web que manipula los expedientes clínicos es por ello que es de suma importancia considerar el cumplimiento de la Ley Nº 25.326 “Protección de los Datos Personales” de Salud Pública en México, Capítulo II “Principios generales relativos a la protección de datos”.

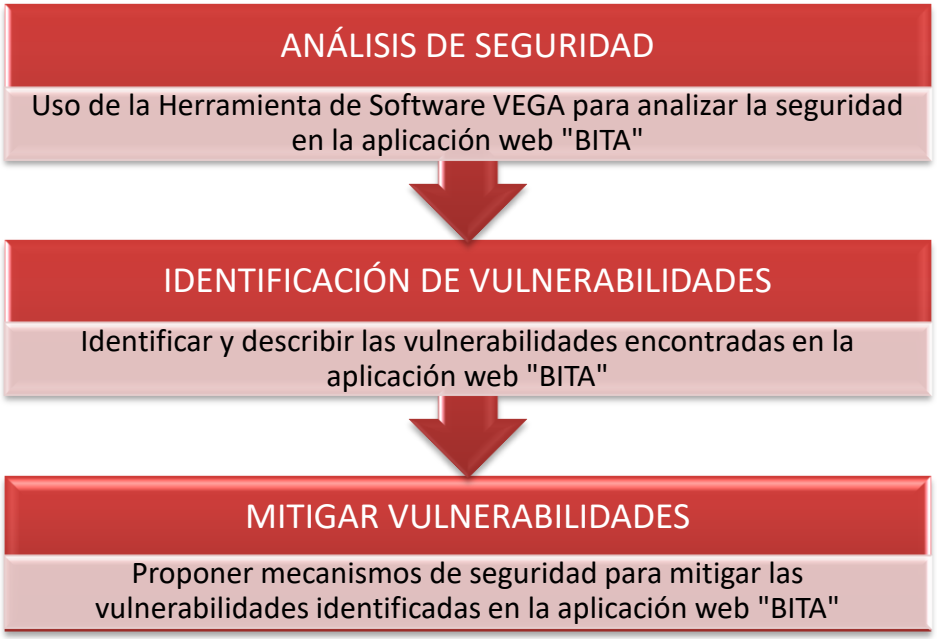
Areitio (2008) menciona, en todo sistema de información, las principales actividades englobadas en el marco de la seguridad



Según la asociación ACISSI (Auditoría, Consejo, Instalación y Seguridad de Sistemas de Información), existen dos ataques comunes para aplicaciones web: Inyección SQL y XSS (Cross-Site-Scripting).

Por otro lado, también existen diversas normas y estándares que sirven de guía para administrar la seguridad en los sistemas de información, entre las que podemos mecionar, por su aceptación a nivel mundial, a ITIL e ISO.

La metodología experimental se divide en tres fases principales a seguir



Primeramente, se detallan las principales características del proyecto “BITA” e inmediatamente cada una de las herramientas de software del entorno de prueba para llevar a cabo la fase de Análisis de Seguridad.

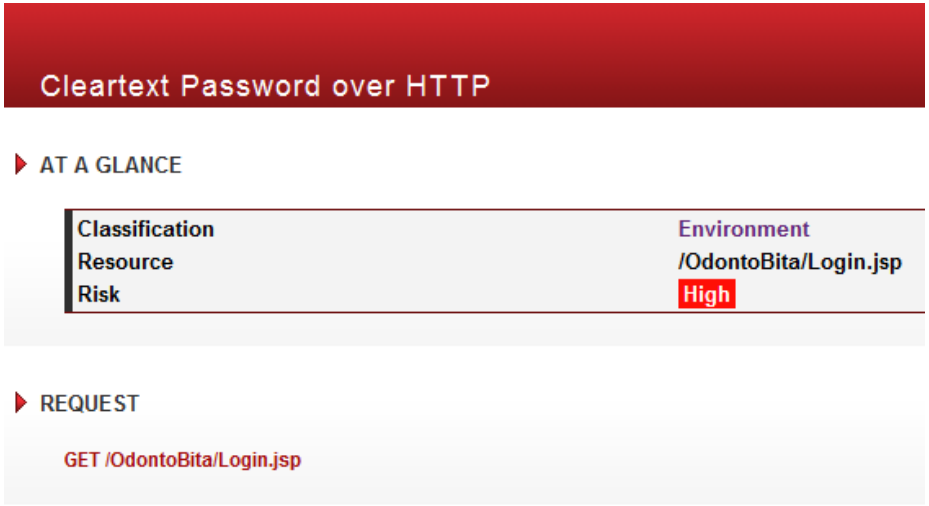
La aplicación web “BITA” fue desarrollada bajo el uso de la metodología de desarrollo de software SCRUM.

Para la aplicación web BITA usamos como herramientas:

Java con tecnología JSP.
MySQL como sistema gestor de base de datos.
El IDE Netbeans.
GitHub como plataforma de desarrollo colaborativa.
VEGA como herramienta de software para análisis de vulnerabilidades.

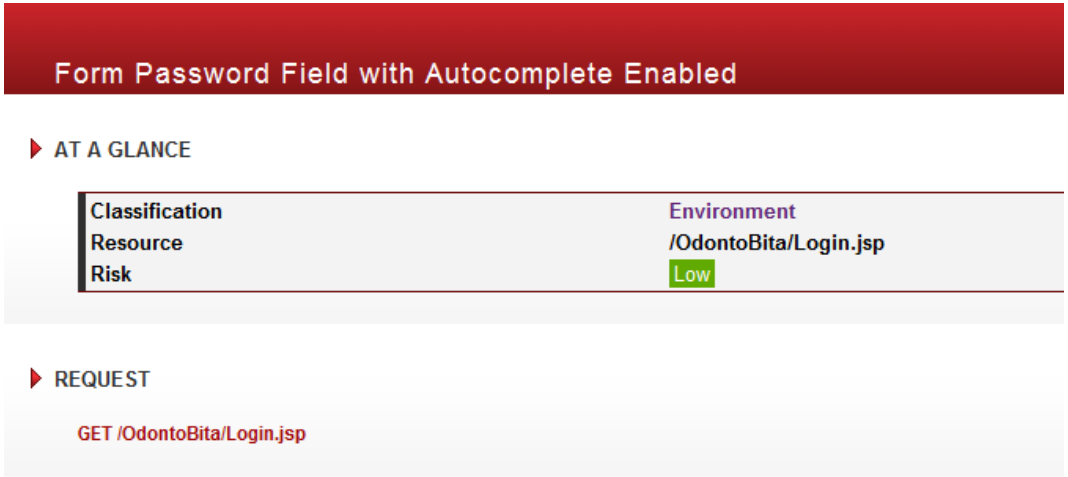
Identificación de vulnerabilidades

VEGA detecta un riesgo ALTO (High) indicando "Cleartext Password over HTTP"



Una segunda vulnerabilidad encontrada es “Sessión Cookie without secure flag”. VEGA ha detectado que una cookie de sesión conocida puede haber sido establecida sin el indicador seguro, lo cual produce un riesgo ALTO (High)

VEGA detecta una tercera vulnerabilidad en la aplicación web "BITA", "Form Password Field with Autocomplete Enabled" en este caso, el nivel de riesgo es BAJO (Low).



Mitigar vulnerabilidades

Después de terminada la fase de Identificación de Vulnerabilidades, el equipo de desarrollo del proyecto "BITA" hace uso de la técnica Grupo de discusión para decidir los mecanismos de seguridad a implementar dentro de la aplicación

VIn	Vulnerabilidad	VDn	Mecanismo de Seguridad
VI_1	Vulnerabilidad Cleartext Password	VD_1	Cifrado (SHA-256)
VI_2	Session Cookie Whithout Secure Flag	VD_2	Manejo de Servlet (cookies y sesiones)
VI_3	Form Password Field with Autocomplete Enabled	VD_3	Configurar propiedad Autocomplete (con deshabilitado)

Resultados

El análisis de resultados se examina a partir de los controles de seguridad de acceso y operativa según la Norma ISO 27002 alineados a la metodología experimental propuesta.

CONTROLES DE SEGURIDAD (ID)	Status	Referente asociado
ACCESO		
Control de acceso a sistemas y aplicaciones		
CA1. Restricción del acceso a la información	×	VI_1, VI_3
CA2. Procedimientos seguros de inicio de sesión	×	VI_2
CA3. Gestión de contraseñas de usuario	×	VI_1, VI_3
CA4. Control de acceso al código fuente de los programas	✓	SA
OPERATIVAS		
Protección contra código malicioso		
CO1. Controles contra el código malicioso	×	SA, SR, SBD
Copias de seguridad		
CO2. Copias de seguridad de la información	×	SBD
Gestión de la vulnerabilidad técnica		
CO3. Gestión de las vulnerabilidades técnicas	×	VI_1, VI_2, VI_3, SA, SR, SBD
CO4. Restricciones en la instalación de software	✓	SR

Fuente: Fuente propia.
VI_1=Vulnerabilidad Cleartext Password, VI_2=Session Cookie Whithout Secure Flag, VI_3=Form Password Field with Autocomplete Enabled, SA = Seguridad en la Aplicación, SR = Seguridad en la red y SBD = Seguridad en la base de datos.

A las vulnerabilidades detectadas se les asigna el nivel de riesgo resultado del análisis con la herramienta de software VEGA, considerando nivel alto igual a 3, nivel medio igual a 2 y nivel bajo igual a 1.

CONTROL DE SEGURIDAD	Nivel de Riesgo (NR)	Nivel de Riesgo
CA1	3	ALTO
CA2	3	ALTO
CA3	3	ALTO
CA4	-	N/A*
CO1	3	ALTO
CO2	3	ALTO
CO3	3	ALTO
CO4	-	N/A**

Nivel de riesgo.

***El acceso al código fuente de la aplicación web "BITA" sólo es parte del equipo de desarrollo, obedeciendo a las políticas propias de la Universidad. **La instalación de software es restringida por las políticas propias de la DGTI (Dirección General de Tecnologías de la Información) de la Universidad.**

Para finalizar la tabla intetiza los mecanimos de seguridad implantados en la aplicación web "BITA" como resultado del seguimiento al estudio realizado

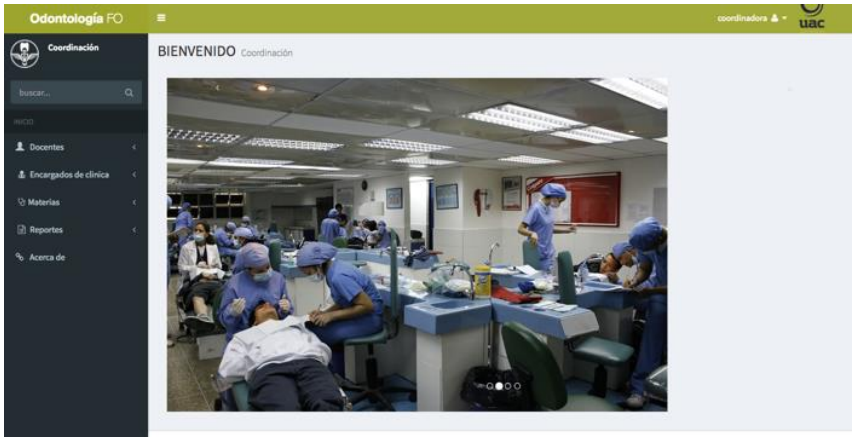
Objetivo de Seguridad	Mecanismo de Seguridad
Confidencialidad	Cifrado (SHA-256)
Integridad	Manejo de Servlet (Cookies y Sesiones)
Confidencialidad	GUI (Interfaz Gráfica de Usuario) (Configurar propiedad Autocomplete con deshabilitado)
Confidencialidad	Contrafuegos (Firewall)
	Filtrado de Puertos
Integridad	Uso de Software Legítimo
Disponibilidad	Uso de Software periódico para el Escaneo de la Red
Confidencialidad	Usuario (Nivel de acceso y Política de seguridad en la contraseña)
Integridad	Backups
Trazabilidad	Configurar el Registro Binario, Registro de Consultas y Registro de Errores en el Sistema Gestor de Base de Datos.

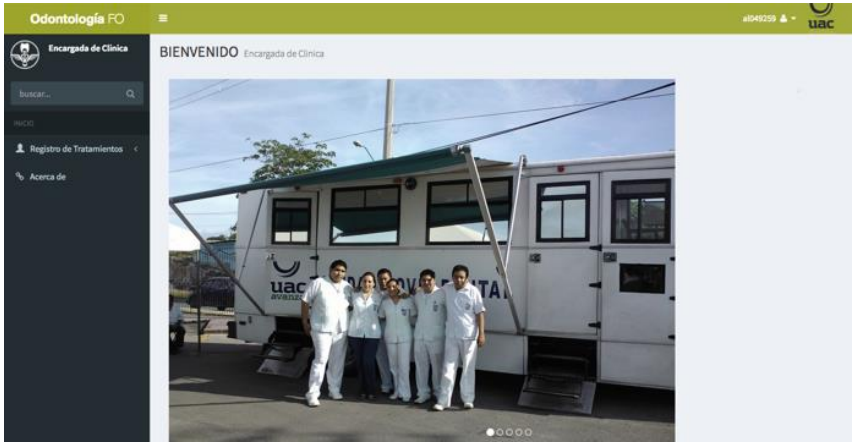
Conclusión

El presente artículo ha servido para el análisis de la aplicación web “BITA”, un caso de estudio para ilustrar el uso básico de seguridad en una aplicación web.

Las oportunidades de considerar mecanismos de seguridad en Sistemas de Información (SI) específicamente en Aplicaciones Web es innumerable, ya que la creciente aparición de diferentes tipos de ataques y delitos informáticos hace que existan nuevas vulnerabilidades.


Bienvenido
Usuario
Contraseña
Entrar


Odontología FO
Coordinación
BIENVENIDO Coordinación
Docentes
Encargados de clínica
Materias
Reportes
Acerca de


Odontología FO
Encargada de Clínica
BIENVENIDO Encargada de Clínica
Registro de Tratamientos
Acerca de

ECORFAN®