UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE SAN FRANCISCO XAVIER DE CHUQUISACA
FACULTAD DE TECNOLOGÍA

TÍTULO DEL PRÁCTICO:

Análisis de riesgo de una Auditoria de Sistemas.

ESTUDIANTE:

Colque García Ariel Rodrigo

Cepeda Choque Álvaro Sebastian

Perka Casillas Celedonio

CARRERA: Ing. Ciencias De la Computación

MATERIA: Auditoría de Sistemas (SIS316)

Sucre-Bolivia

Análisis de Riesgos en una Auditoría de Sistemas

CASO de Estudio : Auditoría a la Seguridad de Aplicaciones Web , caso Dominio *.usfx.bo

1. Establecimiento del Contexto

El dominio usfx.bo, actualmente alberga a varios subdominios y aplicaciones web que son importantes sistemas de nuestra universidad,
en ese sentido surge la necesidad de saber en que medida se tienen ciertos controles de seguridad que esten protegiendo estos activos de
amenazas externas a aplicaciones web, en que medida existen vulnerabilidades y como poder mejorar el control de las mismas.

El alcance de esta auditoría abarca la evaluacion de las principales aplicaciones web y web sites de la universidad, los test son de caja negra o tambien llamadas pruebas dinámicas, se utilizaran ciertas herramientas automatizadas y tambien se podran hacer algunas pruebas manualmente.

No se requiere permisos especiales y en todo caso cualquier análisis que implique una denegacion o corrupcion del sitio web analizado, no debera ser ejecutado pero si reportado.

Estándares de Referencia:
Owasp TOP TEN : https://owasp.org/www-project-top-ten/
The WASC Threat Classification
v2.0: http://projects.webappsec.org/w/page/13246978/Threat%20Classification
Guia de Pruebas de Seguridad de OWASP : https://owasp.org/www-project-web-security-testing-guide/stable/
Criterios de Evaluacion de Aplicaciones WEb usando Scanners
: http://projects.webappsec.org/w/page/13246986/Web%20Application%20Security%20Scanner%20Evaluation%20Criteria

Objetivo : Evaluar la seguridad de las aplicaciones web del dominio *.usfx.bo , utilizando pruebas dinámicas y basadas en estándares internacionales, de tal manera que garanticen un análisis completo, y permitan inferir conclusiones sobre este aspecto con evidencia materia

2. Identificación de Riesgos:

Desarrollar un listado de las amenazas y la explicación resumida de cada una, en un solo párrafo por Amenaza (por lo menos 10 amenazas)

Asignar un código de identificación a cada una, que servirá para referenciarla en todo el proceso, este código deberá ser de la forma R1, R2, R3, R4, R5 , y asi sucesivamente

3. Evaluación de los Riesgos:

3.1 Perfilamiento de los Riesgos :

Se debe **Modelar cada amenaza**, identificando claramente las vulnerabilidades y la manera de explotar estas para que la amenaza se concrete, asi como el Agente de Amenaza, y los activos amenazados. Utilice las tablas del Tema 1 sobre **Modelado de Amenazas.**

3.2) Evaluación del Impacto (en una escala de 1 a 10): Utilizar Delphi para llegar a un consenso, el criterio de evaluación será : " Mas critico para el usuario" o "más crítico para la organización" , también podrían usar "mayor pérdida económica", o "más dificil de recuperarse", o "más tiempo perdido". Cada grupo ve que criterio se acomoda mejor a su caso. Al usar Delphi, el riesgo que obtenga el mayor valor puede considerarse como "catastrófico" o "crítico", y en descenso de escala los demás riesgos. Describir todo el proceso Delphi que siguió el grupo. Considerar la siguiente referencia genérica

NIVEL	CONCEPTO	DESCRIPCIÓN
1	**Despreciable**	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización
3	**Marginal**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.
5	**Moderado**	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.
7	**Crítico**	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.
10	**Catastrófico**	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.

3.3) Evaluación de la Probabilidad o Frecuencia de Ocurrencia (en una escala de 1 a 10): Utilizar Delphi para llegar a un consenso, el criterio de evaluación será : "más frecuente de ocurrir". Incluir toda la información del proceso Delphi de cada experto.

Niveles de Probabilidad		**Descripción**
10	**Muy alta**	Riesgo cuya materialización es recurrente (Casi seguro).
7	**Alta**	Riesgo que puede materializarse de manera habitual (Probable).
5	**Moderada**	Riesgo que se presenta de forma casual o accidental (Posible).
3	**Baja**	Riesgo que puede presentarse de manera eventual (Raro).
1	**Muy baja**	Riesgo cuya probabilidad de materializarse es mínima (Improbable).

3.4) Acomodar los Riesgos sin control en la Matriz de Riesgo

MATRIZ DE RIESGOS

	IMPACTO / PROBABILIDAD	DESPRECIABLE (1)	MARGINAL(3)	PROMEDIO (5)	CRITICO (7)	CATASTROFICO (10)
CASI SIEMPRE	MUY ALTO (10)			R5	R1	
MUY FRECUENTE	ALTO (7)				R2	
MEDIANAMENTE	NOMINAL (5)		R3		R4/R10	
POCO FRECUENTE	BAJO (3)				R6/R7	R8
CASI NUNCA	MUY BAJO (1)					

Descripción de las Amenazas.

ID	AMENAZA	DESCRIPCIÓN
R1	Ataque fuerza Bruta	El ataque consiste en probar todas las combinaciones posibles de contraseñas hasta encontrar la correcta, utilizando un programa automatizado.
R2	Inyección SQL	Implica insertar código malicioso en una aplicación web para manipular la base de datos subyacente.
R3	Fingerprinting	Es una técnica que recopila información única de un sistema informático para realizar ataques más efectivos, tales ser; sistema operativo, software instalado, versión del navegador, entre otros detalles.
R4	Credential/Session Prediction	Técnica de predecir credenciales o sesiones de usuario utilizando información previa, como contraseñas filtradas o patrones de uso predecibles, con el fin de obtener acceso no autorizado a sistemas o información confidencial.
R5	Denial of Service	DoS es un ataque que sobrecarga un sistema o red con tráfico falso o excesivo, impidiendo que los usuarios legítimos accedan a los recursos.
R6	Content Spoofing	Es manipular el contenido de una página web para engañar a los usuarios y robar información confidencial a través de ataques de phishing.
R7	Abuse of Functionality	Consiste en utilizar de manera malintencionada características legítimas de una aplicación o sistema, con el objetivo de obtener beneficios maliciosos o acceder a información privilegiada.
R8	Path Traversal.	Explota una vulnerabilidad en una aplicación web para acceder a recursos fuera del directorio raíz, permitiendo a los atacantes acceder a archivos o carpetas sensibles.
R10	Null Byte Injection	Es un ataque que aprovecha la incapacidad de algunos programas para manejar correctamente los caracteres nulos en la entrada de datos

4) Priorizar, de mayor a menor impacto total (Impacto total = P x I)
Impacto (I)

Probabilidad (P)

Amenaza	P (1-10)	Justificación consensuada de P	I (1 a 10)	Justificación Consensuada de I	Impacto Total IT
R1	10	Son muy comunes y ahora pueden ser efectuados por cualquier persona sin importar el conocimiento en programación gracias a los que venden programas de automatización de estos.	10	De llegar a efectuarse uno de estos ataques sería catastrófico para la empresa internamente, hacia los clientes y hacia la imagen de la empresa.	100
R2	7	Pueden ocurrir con frecuencia, y al estar conectados a internet, con frecuencia aun, y además sin ningún tipo de protección que otras amenazas puedan vulnerar.	10	De llegarse a efectuar esta amenaza, causaría un caos dentro de la organización, destruyendo o robando la mayor cantidad de información a la cual tengan acceso.	70
R3	5	De no existir un control adecuado ocurrirá con mucha más frecuencia, pero tomando en cuenta que se tenga un control sobre este, no es tan frecuente pero puede ocurrir con regularidad.	3	Su impacto no por si solo no es muy peligroso, pero si se juntara con alguna otra tecina podría llegar a ser significativo, pero no causar grandes daños antes de ser controlado.	30
R4	5	Al ser un sistema de predicciones, tiene que tener una gran complejidad matemática, pero además de los conocimientos en estadística y programación para lograr ser automatizada, tendría que tener un gran poder de cómputo, antes de que se ejecute un control para los usuarios.	7	De acertar en algún credencial de alto mando dentro de la organización, puede comprometer de sobremanera los activos de información que posea la organización.	35
R5	10	La denegación de servicio es una amenaza que se trata de ejecutar contantemente en el dominio en cargo, a pesar de su complejidad.	10	De llegar a ocurrir en varios sitios de este dominio pude ocasionar, un daño serio a la imagen de la organización y	100

				afectar a los clientes en su día día.	
R6	3	Es complejo que realice con frecuencia este tipo de amenaza, además de requerir muchos conocimientos en el área de la programación y seguridad de la información e informática.	7	Si la amenaza se ejecuta, dañaría severamente la imagen de la organización y también la confianza de sus usuarios.	35
R7	3	Requiere de bastantes conocimientos sobre la programación, para lograr encontrar los puntos débiles del dominio, por lo tanto por su complejidad, no debería de ocurrir de manera frecuente.	7	De darse el caso de que ocurra, pues daña severamente la app como tal y ocasionado el cambio y /o actualización de todo el sistema.	35
R8	3	Es una amenaza compleja de ejecutarse, con vastos conocimientos en programación (back-end) y conocimientos sobre el funcionamiento de las bases de datos	10	De lograr efectuarse tendrían acceso a toda información del dominio, a la base de datos, robando, exponiendo y hasta destruyendo información sensible para la organización.	30
R10	5	Es una amenaza compleja de ejecutarse, con vastos conocimientos en programación (back-end) y conocimientos sobre el funcionamiento de las bases de datos	7	De que se logre efectuar esta amenaza, la organización, empezaría a perder control de su sitio web, inseguridad, dentro y fuera de la organización, causando vulnerabilidades que otras amenazas puedan aprovehcar.	35