UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

DICIEMBRE 2022 - MAYO 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMA DE INFORMACIÓN

TEMA:

ANÁLISIS DE METODOLOGÍAS DE ATAQUE TIPO CLICKJACKING Y TOUCHJACKING, EN ENTORNO WEB

ESTUDIANTE:

IRENE MERCEDES VALERO SANCHEZ

TUTOR:

ING. IVAN RUBEN RUIZ PARRALES

AÑO 2023

CONTENIDO

ANALISIS DE METODOLOGIAS DE ATAQUES DE TIPO CLICKJACKING Y TOUCHJACKING, EN ENTORNOS WEB.

RESUMEN

El presente trabajo de titulación es de análisis de metodologías de ataque clickjacking y touchjacking en un entorno controlado, siendo el objetivo fundamental determinar cuál es el nivel de eficiencia de cada uno de estos ataques que podrían ser sometidos a ciertas condiciones que podrían ser serán planteadas en los diferentes escenarios, de igual forma se implementan las posibles medidas de mitigación sugeridas por autores dentro del análisis realizado, para el desarrollo de este caso de estudio se realizaron los siguientes pasos: 1) Análisis de un posible escenario de Ataque 2) Evaluación de posibles amenazas del escenario de ataque 3) Desarrollo de matrices de posibles ataques 4) Determinar posibles vectores críticos del escenario planteado 5) Evaluación de posibles técnicas de ataque y mitigación.

Para el desarrollo del presente caso de estudio se utilizó un método experimental con el fin de modificar cada una de las variables de los escenarios planteados y determinar los efectos que causa en cada uno de ellos, también se implementa un método cualitativo con el fin de determinar características y condiciones que pueden presentar un mayor riesgo frente a este tipo de ataques.

El resultado del análisis de las técnicas de clickjacking y touchjacking en este caso de estudio busca establecer posibles medidas de sanitización e implementación de buenas prácticas, así como también la utilización de estándares en el desarrollo web para mejorar la seguridad dentro de las aplicaciones web.

Palabras clave: Clickjacking, Touchjacking, Eficiencia, Sanitización.

ABSTRACT

The present degree work is the analysis of clickjacking and touchjacking attack methodologies in a controlled environment, the main objective being to determine the level of efficiency of each of these attacks that could be subjected to certain conditions that could be raised in the different scenarios, in the same way the possible mitigation measures suggested by authors are implemented within the analysis carried out, for the development of this case study the following steps were carried out: 1) Analysis of a possible attack scenario 2) Evaluation of possible threats of the attack scenario 3) Development of matrices of possible attacks 4) Determine possible critical vectors of the proposed scenario 5) Evaluation of possible attack and mitigation techniques.

For the development of this case study, an experimental method was used in order to modify each of the variables of the proposed scenarios and determine the effects that it causes in each of them, a qualitative method is also implemented in order to determine characteristics and conditions that may present a greater risk against this type of attack.

The result of the analysis of clickjacking and touchjacking techniques in this case study seeks to establish possible sanitation measures and implementation of good practices, as well as the use of standards in web development to improve security within web applications.

Keywords: Clickjacking, Touchjacking, Efficiency, Sanitization.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad es importante ir de la mano con los avances tecnológicos, en el área de la informática este tipo de avances y nuevas técnicas sirven para mejorar diferentes sistemas informáticos pero como es conocido las mejoras en muchos de los casos generan nuevos riesgos o vulnerabilidades, por ello es necesario tener un conocimiento sobre los diferente tipos de riesgos a los que estamos expuestos, el internet se ha convertido una herramienta de acceso de información a nivel mundial es el lugar indicado para obtener datos privados o información de usuarios de manera ilegal, actualmente existen diversas técnicas de ataques pero es importante identificar cuáles son las más comunes y plantear medidas de mitigación ante las mismas.

JUSTIFICACIÓN

El presente caso de estudio tiene como objetivo análisis las metodologías y explicar el funcionamiento de las técnicas de ataques de clickjacking y touchjacking, se han escogido estas técnicas entre muchas existentes debido a las siguientes circunstancias: la primera se debe al constante aumento de plataformas web orientadas a: e-comerce, educativas e institucionales, este tipo de plataformas se encuentran mucho más expuestas a delincuentes informáticos con fines de robo de información o sustracción de datos personales; y la segunda es motivada por las falencias con respecto al desarrollo web y desconocimiento de medidas de prevención contra este tipo de ataques que se evidencian en la actualidad.

OBJETIVO DEL ESTUDIO

OBJETIVO GENERAL

Analizar la eficiencia de las metodologías de ataques de tipo clickjacking y touchjacking en contra de páginas web con iframes vulnerables.

OBJETIVOS ESPECIFICOS

- Analizar las técnicas de ataques clickjacking y touchjacking y su nivel de eficiencia utilizando diferentes navegadores web.
- Determinar las características funcionales que podrían hacer de un sistema web, un objetivo vulnerable a potenciales ataques de clickjacking y touchjacking.
- Evaluar la eficiencia de ejecución de estos ataques, contrastando su potencial impacto con algunas técnicas de mitigación propuestas por estándares y buenas prácticas de desarrollo y sanitización web existentes.

LÍNEA DE INVESTIGACIÓN

Sistemas de información y comunicación, emprendimiento e innovación.

Este caso de estudio se realizó bajo unos análisis previos dados, buscando facilitar una adecuada manipulación de los datos con el uso del desarrollo tecnológico de la empresa.

SUBLÍNEA DE INVESTIGACIÓN

Redes y tecnologías inteligentes de software y hardware aplicado.

MARCO CONCEPTUAL

En esta sección se analiza la literatura de trabajos relacionados al tema de investigación con el fin de identificar técnicas de ataques y medidas de mitigación sugeridas por los diferentes autores, también se especifica la contribución que se hará con respecto a los ataques de clickjacking y touchjacking.

De los trabajos de literatura investigados se mencionan técnicas utilizadas para los ataques de clickjacking, y touchjacking, que darán la pauta para comprender el funcionamiento de este tipo de ataques, de igual forma en la bibliografía investigada los autores plantean medidas de mitigación que son analizadas durante el desarrollo de este caso de estudio.

Cajías Borja, E. F. (2020), El autor indica que el término de clickjacking fue descubierto en el año 2008 por Jeremiah Grossman y Robert Hansen. El término touchjacking fue acuñado posteriormente con la introducción de pantallas táctiles en dispositivos móviles Estas técnicas consisten en ejecutar ataques de dominio cruzado para persuadir al usuario que realice un clic en un elemento especifico de una página HTML, mientras que en realidad la víctima estaría interactuando con un sitio web diferente al original sin percatarse de ello. Para la realización de este ataque, es necesario cargar una página maliciosa dentro de la página HTML vulnerable utilizando iFrame y la modificación de nuestro archivo CSS (Cascading Style Sheets) para ocultar todos los elementos excepto la región objetivo de la página web, generalmente se utilizan transparencias en la ventana que se sobrepone a la original para no hacerla visible a la víctima. Debido a que la factibilidad de este ataque depende de la ingenuidad del usuario, hoy en día los navegadores más utilizados como Chrome, Edge y Firefox son víctimas de estos ataques, sin que se pueda hacer mucho para prevenirlos, siendo mayormente vulnerables páginas web del gobierno, bancarias e instituciones.

Dentro de este análisis se han identificado los siguientes tipos de ataque de clickjacking:

- **Esconder el elemento objetivo:** Consiste en que el atacante oculta el elemento objetivo mediante la utilización de código HTML o CSS, pero los eventos que realiza el mouse se mantienen trabajando, este ataque puede estar hecho por un

elemento transparente sobrepuesto sobre la página web con el valor de opacidad en cero.

- **Múltiple Iframe:** El atacante trata de engañar a la víctima únicamente cargando un doble iframe en la página original ocultando una parte del elemento web, con el fin de eliminar las seguridades de los navegadores web.

- **Ataque Redimensionado:** Este tipo de ataque inserta un elemento web muy pequeño sobre un elemento de mayor tamaño con el objetivo de hacerlo parecer un botón y de esta forma despistar a la víctima.

Otro tipo de ataque mencionado en este caso de estudio es la técnica de touchjacking que está enfocada a los navegadores que utilizan tecnología táctil, como los dispositivos móviles que utilizan un componente denominado WebView el cual permite la comunicación y despliegue de páginas HTML, permitiendo que este tipo de ataque se realice mediante las siguientes técnicas:

- **Ataque Cross Site Scripting:** Este tipo de ataque consiste en robar las cookies del dispositivo de la víctima ya que en estas se almacena información persistente del navegador permitiendo hacer uso de información personal de la víctima.
- **Ataque Invisible:** En este tipo de ataque se sobrepone una plantilla web sobre otra y se la oculta con el fin de que el usuario crea que está actuando sobre una página web original mientras por detrás se encuentra embebida una página maliciosa.
- **Ataque de Teclado**: Este ataque consiste en insertar plantillas web maliciosas ocultas sobre formularios o campos en donde el usuario deberá insertar información desde el teclado, con el fin de robar los datos y claves de acceso.

Los ataques mencionados son muy comunes en la actualidad cuya ejecución requiere que el atacante calcule la posición en donde el usuario tocará la pantalla. Aunque parezca complicado, esto en realidad no lo es ya que existen técnicas de posicionamiento para poder agregar páginas webs invisibles sobre elementos que pueden ser seleccionados por el usuario.

La relativamente moderada complejidad para replicar estos ataques motiva su estudio para poder implementarlos y evaluarlos en entornos controlados, permitiendo experimentar con las posibles formas en las que un atacante podría comprometer páginas web en distintos navegadores usando clickjacking y/o touchjacking.

Metodología OTA: La metodología OTA (Operational Threat Assessment) es aplicada para implementar una matriz con el fin de caracterizar y diferenciar las amenazas contra objetos de nuestro interés, el propósito principal de la matriz es identificar los atributos que podrían ayudar a un analista a caracterizar las amenazas con respecto a cada una de las capacidades generales.

Esta caracterización permite tener un panorama amplio de las amenazas sin asignar etiquetas a una amenaza específica, ya que resulta muy complicado analizar cada tipo de amenaza de forma coherente.

El objetivo principal de la Metodología OTA es clasificar las amenazas de un vocabulario común, además que permite identificar posibles rutas de ataques que se respalda en la capacidad de identificar los pasos de mitigación adecuados para evitar cualquier tipo de ataque.

Metodología STRIDE: Es una técnica de modelado de amenazas que se usa para descubrir la seguridad y debilidades de un sistema de software.

El uso de esta metodología sugiere una serie de pasos que se describen a continuación:

1. Modelar el sistema mediante un diagrama de flujo de datos (DFD), para ese paso es necesario definir las actividades iniciales para determinar el alcance del modelo del sistema.

2. Asignar cada uno de los elementos del DFD (Diagrama de flujo de dato) a las categorías de las amenazas, en STRIDE las amenazas se dividen en seis categorías:
    - **Spoofing:** Que se refiere a suplantar a un usuario o programa legítimo.
    - **Tampering**: Se refiere a una amenaza que pretende modificar aplicaciones o recursos de forma ilegítima.
    - **Repudiation:** Se refiere a que un usuario legitimo o malicioso intentara de negar la ejecución de una acción dentro de un sistema.
    - **Information Disclosure:** Se refiere a la obtención de información privada a la que comúnmente un usuario no debería tener acceso.
    - **Denial of service:** Se refiere a una amenaza cuyo fin es no dejar disponibles recursos de un sistema para los usuarios que lo usan.
    - **Elevation of privilege:** Se refiere a la acción de obtener acceso privilegiado a ciertos recursos que se encuentran normalmente protegidos.

3. Obtener las amenazas para cada uno de los mapeos, la metodología STRIDE proporciona una lista de verificación de amenazas que deben ser consideradas, como un árbol de amenazas esta estructura está destinada a facilitar la navegación u proporcionar una justificación detrás de cada amenaza.

4. Finalmente se deberá documentar las amenazas, la metodología STRIDE no impone ningún formato específico para este procedimiento**.**

Vectores de Ataque: Mendez Fonseca, V. J. (2020), El autor indica que los vectores de ataque son medios por los cuales una amenaza puede aprovechar alguna vulnerabilidad y lograr un

resultado, para comprender el funcionamiento de un vector de ataque es importante conocer las tácticas, técnicas y procedimientos de su funcionamiento, que en general se refiere a gestionar, orquestar y supervisar un ataque, existen 5 vectores de ataques más comunes que se enumeran a continuación:

- **Atacar el elemento humano:** Mieres, J. (2009), El autor indica que sin duda uno de los vectores de ataque más comunes ya que el objetivo principal es explotar vulnerabilidades de las personas a través de ingeniería social, phishing o ataques de redes sociales.

- **Web y navegador basados en vectores de ataque:** Gómez Coronell, O. (2014), E autor refiere que cuando se utilizan sitios webs comprometidos o falsos para enviar código malicioso o exploits a sus víctimas.

- **Activos expuestos en internet:** Niño, F. Y. A. (2023), Niño refiere que es un vector de ataque que afecta servicios que no se encuentran suficientemente protegidos y están expuestos, utilizando esta vulnerabilidad para la entrega de malware o ataques de ransomware.

- **Explotación de vulnerabilidades o malas configuraciones:** Son vectores de ataque utilizados para acceder a un sistema u organización.

- **Red o fallas de seguridad de protocolo**: Monterroza Barrios, R. E. (2019), Al igual que la explotación de vulnerabilidades el objetivo de este vector de ataque es encontrar fallas de configuración a nivel de red con el fin de ganar acceso.

- **Ataques a cadena de suministro:** Tarazona, T., & Cesar, H. (2007), el autor indica que son vectores de ataque cuyo objetivo es el dañar elementos a nivel de infraestructura de software o hardware**.**

Niveles de Amenazas: El propósito de estimar el nivel de amenaza es mejorar el análisis integral de estas y priorizar los gastos que se deban realizar para mitigar dichas amenazas, el tipo de amenazas se pueden caracterizar en niveles subdivididos en los siguientes atributos:

NIVEL DE AMENAZA	PERFIL DE AMENAZA						
	COMPROMISO			RECURSOS			
	INTENSIDAD	OCULTACION	TIEMPO	PERSONAL TECNICO	CONOCIMIENTO		ACCESO
					CYBER	KINETEC	
1	A	A	Años a Décadas	Centenas	A	A	A
2	A	A	Años a Décadas	Decenas de decenas	M	A	M
3	A	A	Meses a Años	Decenas de decenas	A	M	M
4	M	A	Semanas a meses	Decenas	A	M	M
5	A	M	Semanas a meses	Decenas	M	M	M
6	M	M	Semanas a meses	uno	M	M	B
7	M	M	Meses a Años	Decenas	B	B	B
8	B	B	Días a semanas	uno	B	B	B

Figura 1. Matriz genérica de amenazas.

Fuente: Irene Valero

- **Intensidad:** Gruber, S. L. A. (1982). Se refiere a la determinación o perseverancia que tiene una amenaza hacia su objetivo, se refiere a que tan dispuesto esta un atacante en arriesgarse para alcanzar su objetivo, las amenazas que presentan mayor intensidad son las consideradas como más peligrosas.

- **Ocultación:** Se refiere a la capacidad que tiene una amenaza en mantenerse en secreto durante la consecución de su objetivo, esto puede implicar ocultar detalles sobre el

objetivo, estructura y funciones internas lo que dificulta el tomar medidas preventivas o prevenir ataques de este tipo de amenazas.

- **Tiempo:** Este atributo cuantifica el periodo durante el cual una amenaza es capaz de dedicarse a planificar, desarrollar y desplegar métodos para alcanzar un objetivo, tomando en cuenta estos detalles se puede concluir que mientras más tiempo esté dispuesto a dedicar una amenaza a preparar un ataque tiene mayor potencial de impacto.

- **Cyber:** Este atributo se refiere al conocimiento teórico y práctico relacionado con la informática, redes o sistemas automatizados.

- **Kinetic:** Este atributo se refiere a la competencia teórica y práctica relacionada a la física de sistemas, movimiento de cuerpos y fuerzas asociadas.

- **Acceso:** Se refiere a la capacidad de colocar a un usuario dentro de un sistema restringido que se base en privilegios o credenciales a través de vulnerabilidades de un sistema desprotegido, el acceso de una amenaza puede provocar múltiples consecuencias como manipulación y robo de información.

Matriz de Riesgo: Una matriz de riesgo se utiliza para evaluar cada uno de los parámetros que conlleva una actividad con el fin de tener información precisa de áreas sensibles dentro de un proceso, una matriz efectiva nos permite realizar comparaciones con cada uno de los procesos y plantear medidas de mitigación.

Los elementos que deben considerarse en una matriz de riesgo son los siguientes:

- **Factores de Riesgo:** Sáinz, J. P. P., & Salas, M. M. (2004), Es importante identificar los riesgos inherentes que no son más que actividades que surgen de los cambios de cada uno de los procesos evaluados, se debe mencionar que cada uno de estos riesgos pueden ser más relevantes que otros.

- **Probabilidad:** Romero, J. C. R. (2004), Consiste en determinar la probabilidad de que el riesgo ocurra, el riesgo se compone de un análisis de la probabilidad

de ocurrencia y el efecto que tiene esta ocurrencia, puede ser efectuada en métodos cualitativos o cuantitativos dependiendo de la disponibilidad de la información.

- **Evaluación de controles internos:** Quinaluisa, N., Ganchozo, M., Reyes, M., & Arriaga, G. (2017). La evaluación de los de cada uno de los riesgos o controles internos se pueden utilizar los siguientes métodos:
    - **Cualitativos:** Emplea escalas descriptivas que permiten evaluar la probabilidad de cada evento, este método se utiliza cuando un riesgo no justifica tiempo y recursos para ser evaluado de forma más profunda.
    - **Cuantitativos:** Se emplean valores numéricos para evaluar la probabilidad de ocurrencia de un evento, este método brinda información más precisa sobre la ocurrencia de un riesgo.

Una vez obtenida la información con respecto a técnicas de ataque y mitigación de clickjacking y touchjacking se realizan las siguientes tablas resumen aplicadas a diferentes autores:

Autores	ANALISIS CLICKJACKING									
	TECNICAS DE ATAQUES					TECNICAS DE MITIGACION				
	Hiding the target	Partial overlays	Cropping	Multiframe	Cross site Scripting	X-frame options	Java Script	Plug-ing	UI randomization	Visibility Detection on Click
[1]	X	X	X			X	X			
[2]	X	X				X	X			
[3]	X			X	X		X	X		
[4]	X					X	X			
[5]	X					X	X		X	X
[6]	X					X	X			X
[7]		X				X	X	X		
[8]	X			X				X	X	
[9]	X						X			
[10]	X									

Tabla1: técnicas de ataques y mitigación tipo clickjacking según autores

Fuente: Irene Valero

Autores	ANALISIS TOUCHJACKING								
	TECNICAS DE ATAQUE					TECNICAS DE MITIGACION			
	Origin Hiding	WebView Ul Attacks	Main-Frame Attcks	Redressing Attacks	Cross Site Scripting	Iframe Sandbox	Origin Validation	Alert Message	Mobile Authenticator
[1]	X				X				X
[2]	X	X	X	X		X			
[3]	X	X							
[4]	X	X							
[5]					X				
[6]	X							X	X
[7]		X			X			X	
[8]		X			X		X	X	
[9]		X						X	X
[10]		X							

Tabla1: técnicas de ataques y mitigación tipo touchjacking según autores

Fuente: Irene Valero

En base a las técnicas de ataque y mitigación identificadas por los autores se puede determinar qué condiciones son las propicias para que se lleven a cabo los ataques de clickjacking y touchjacking midiendo su impacto, con el fin de contribuir con la generación de contramedidas, mediante la aplicación de buenas prácticas de desarrollo y sanitización web.

Los autores coinciden en que se deben de aplicar un método experimental en la cual se define como la creación de situaciones en las condiciones exactas que se desea, permitiendo manipular diferentes variables, con el fin de probar, elaborar y refinar el conocimiento, hasta alcanzar a comprender el comportamiento de las variables relevantes que intervienen en estos fenómenos. Dentro de este método intervienen tres principales momentos: el objeto de observación, el observador y un sistema de registro cuantitativo o cualitativo.

Posteriormente, para la implementación de estos tipos de ataques se deben de utilizar herramientas para realizar el análisis de los escenarios e identificar las principales amenazas a las que se ve expuesto un modelo de sistema y de esta forma plantear medidas de mitigación en base a las evaluaciones obtenidas.

Los autores indican que, una vez realizadas las pruebas de estos escenarios, se debe de proceder a llevar un registro cualitativo acerca del comportamiento de cada uno de los ataques simulados.

Finalmente, se debe evaluar la eficiencia de estos ataques, contrastando a los resultados obtenidos en cada uno de los escenarios, con técnicas de mitigación que se han planteado como mejores prácticas de desarrollo y sanitización web, identificando oportunidades de mejora y recomendaciones para desarrolladores y administradores de sistemas.

HERRAMIENTA

Microsoft Threat Modeling: Hernández Bejarano, M., & Baquero Rey, L. E. (2020)., Esta herramienta de modelado de Microsoft puede ser utilizada durante el ciclo de desarrollo de proyectos, debido a que permite identificar y mitigar posibles inconvenientes con respecto a seguridad de forma temprana, optimizando el tiempo y recursos, el diagrama de funcionamiento de la herramienta se basa en los siguientes aspectos.

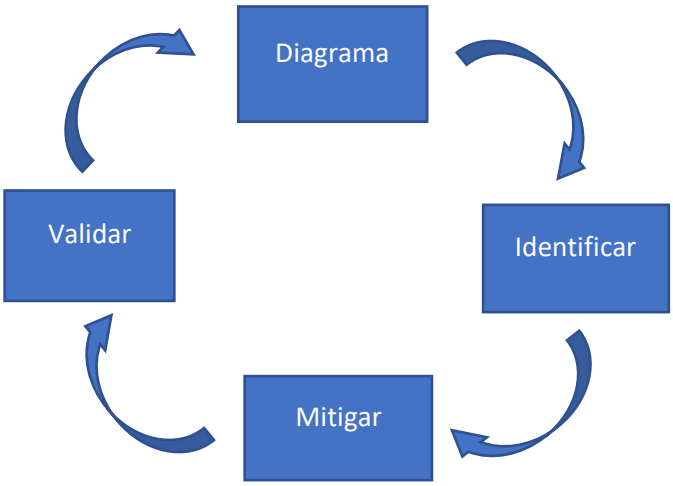

Figura . Etapas Microsoft Threat Modeling.

Fuente: Irene Valero

Las ventajas de la utilización de esta herramienta son las siguientes:

- Analizar cada uno de los diseños planteados y evidenciar posibles problemas de seguridad.
- Plantear diversas alternativas de solución con respecto a las vulnerabilidades detectadas.
- Realizar mejoras y optimizaciones a nivel de diseño.

MODELO EXPERIMENTAL A PROPONER

Dentro del diseño del entorno experimental los autores plantean que se deben de realizar dos tipos de modelos:

Modelo del Sistema: En este modelo es en el cual se explica la arquitectura de software y hardware sobre la cual se realiza el modelo del sistema.

Modelo de Ataque: En este modelo se especifica los actores y mecanismos mediante los cuales se lleva a cabo los ataques planteados para el modelo definido.

MODELO GENÉRICO DEL SISTEMA

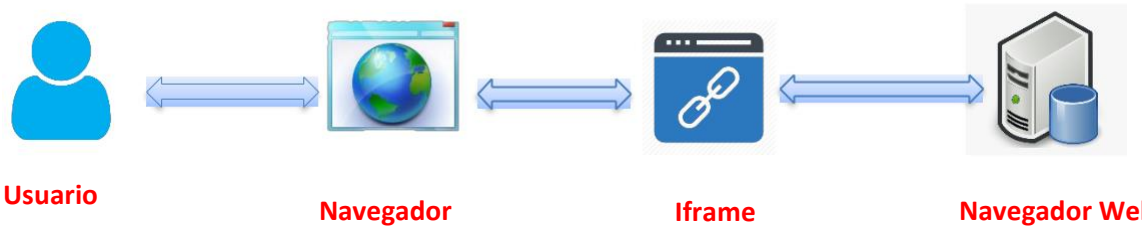

Figura: modelo genérico del sistema

Usuario: Para el modelo del sistema se estimará que el usuario que se encuentre bajo este tipo de ataques será considerado como un usuario que tiene un nivel de conocimiento medio-alto en seguridad (usuario avanzado o experto).

Navegador: Para el planteamiento del modelo del sistema es necesario especificar el tipo de navegador y sus características:

Iframe: Para la implementación del iframe en el sistema se debe desarrollar una página web en HTML y se implementa el elemento <iframe> </iframe> para la página web.

Servidor Web: Para la implementación del servidor web local se utiliza la herramienta XAMMP en cualquiera de las versiones (Este servidor es utilizado para evaluar los escenarios de clickjacking y touchjacking planteados).

MODELO DE ATAQUE

Para implementar este escenario práctico se debe de utilizar las herramientas mencionadas anteriormente, las cuales permiten identificar las vulnerabilidades y los tipos de ataques a los que está expuesto el escenario planteado, para aquello se debe definir el siguiente modelo de ataque:

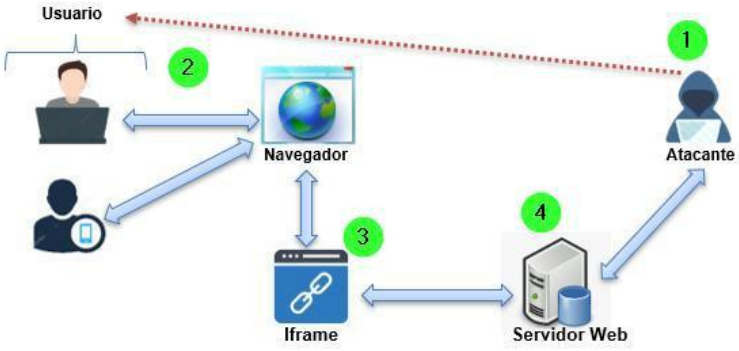

Figura: modelo genérico de ataque

Una vez finalizadas las etapas de reconocimiento y análisis de vulnerabilidades se deben identificar los vectores de ataque para el escenario planteado.

EJEMPLO DE VECTORES DE ATAQUES USANDO NAVEGADORES SEGUN EL MODELO GENERICO

Tabla . *Vectores de Ataques genéricos*

ID VECTOR DE ATAQUE	VECTORES DE ATAQUES GENERICOS	TECNICA
V1	Phishing	CLICKJACKING
V2	A1- Interfaz Gráfica	
V3	A2-Interfaz Gráfica	
V4	B1^B2-A3- Interfaz Gráfica	
V5	A4-Interfaz Gráfica	
V6	B6-A6-Spoofing	
V7	C1-B7-A6-Spoofing	
V8	C2-B7-A6-Spoofing	
V9	A7-Spoofing	
V10	A8- Cross Site Scripting	
V11	A10- Cross Site Scripting	
V12	A9- Cross Site Scripting	TOUCHJACKING
V13	B3-A5- Interfaz Gráfica	
V14	B4-A5- Interfaz Gráfica	
V15	B5-A5- Interfaz Gráfica	

Fuente: Irene Valero

NIVELES DE AMENAZA

Para el análisis de los niveles de Amenaza, los autores indican que debe de tomar como línea base los atributos genéricos de intensidad, ocultación, ciber y acceso con el fin de evaluar el perfil de amenaza, considerando parámetros de compromiso y nivel de conocimiento del atacante, que afectarían directamente al sistema.

Perfil de Amenaza: Para el perfil de amenaza se debe de subdividir en dos grandes características que serán el nivel de compromiso y el nivel de conocimiento.

Nivel de intensidad: Con respecto al nivel de intensidad se debe de tomar en cuenta el número de intentos o métodos posible de ataques que se pueden efectuar de forma recurrente hasta llegar al objetivo.

Tabla: Niveles de intensidad propuestos

Nivel	DESCRIPCION
Alto (3)	Cuando la amenaza está altamente determinada a alcanzar su objetivo, aceptando todas las consecuencias.
Medio (2)	Cuando la amenaza esta moderadamente determinada a alcanzar su objetivo, aceptando algunas de las consecuencias
Bajo (1)	Cuando la amenaza está determinada a alcanzar su objetivo, sin aceptar las consecuencias.

Fuente: Irene Valero

Nivel de Ocultación: Para el nivel de ocultación hemos determinado que tan silencioso es el ataque hasta llegar al objetivo.

Tabla: Niveles de Ocultamiento propuestos

Nivel	DESCRIPCION
Alto (3)	La amenaza es altamente capaz de mantenerse en secreto hasta alcanzar el objetivo
Medio (2)	La amenaza es moderadamente capaz de mantenerse en secreto hasta alcanzar el objetivo
Bajo (1)	La amenaza no es capaz de mantenerse en secreto hasta alcanzar el objetivo

Fuente: Irene Valero

Nivel de conocimiento

Cyber: Se evalúa el nivel de conocimiento que se debe tener para llevar a cabo los diferentes tipos de ataques.

Tabla: Niveles del Cyber

Nivel	DESCRIPCION
Alto (3)	La amenaza deber ser utilizada por un experto para lograr su objetivo.
Medio (2)	La amenaza puede ser aplicada por un usuario nivel intermedio para lograr su objetivo.
Bajo (1)	La amenaza puede ser aplicada por un usuario novato para lograr su objetivo.

Fuente: Irene Valero

Acceso: En este nivel se determina el acceso que se puede llegar a tener con una amenaza sobre un sistema restringido.

Tabla: Niveles de acceso

Nivel	DESCRIPCION
Alto (3)	La amenaza es capaz de permitir el acceso ilimitado a un sistema restringido.
Medio (2)	La amenaza es capaz de permitir el acceso limitado a un sistema restringido.
Bajo (1)	La amenaza no es capaz de permitir el acceso a un sistema restringido.

Fuente: Irene Valero

NIVEL DE AMENAZA

Para determinar el nivel de amenaza, los autores consideran los valores máximos y mínimos (entre 4 y 12) determinando 3 niveles que se muestran a continuación:

Tabla: Niveles de amenaza

Nivel	DESCRIPCION
Alto (10-12)	La amenaza es capaz de permitir el acceso ilimitado a un sistema restringido.
Medio (7-9)	La amenaza es capaz de permitir el acceso limitado a un sistema restringido.
Bajo (4-6)	La amenaza no es capaz de permitir el acceso a un sistema restringido.

Fuente: Irene Valero

ESTIMACIÓN DE RIESGO DE VECTORES DE ATAQUE

Para la estimación del riesgo se propone que se debe de analizar cada uno de los vectores de ataque mediante la sumatoria de los atributos genéricos de intensidad y conocimiento, con el fin de determinar cuáles son los riesgos de nivel alto que pueden afectar el escenario basados en la Tabla anterior.

Tabla: Genérica de Análisis de vectores de ataque

ID VECTOR DE ATAQUE	VECTORES DE ATAQUES GENERICOS	I	O	C	A	NIVELES DE AMENAZA	TECNICA
V1	Phishing						CLICKJACKING
V2	A1- Interfaz Gráfica						
V3	A2-Interfaz Gráfica						
V4	B1^B2-A3-Interfaz Gráfica						
V5	A4-Interfaz Gráfica						
V6	B6-A6-Spoofing						
V7	C1-B7-A6-Spoofing						
V8	C2-B7-A6-Spoofing						
V9	A7-Spoofing						
V10	A8- Cross Site Scripting						
V11	A10- Cross Site Scripting						
V12	A9- Cross Site Scripting						TOUCHJACKING
V13	B3-A5-Interfaz Gráfica						
V14	B4-A5-Interfaz Gráfica						

V15	B5-A5- Interfaz Gráfica						

I: Intensidad **O:** Ocultación **C:** Cyber **A:** Acceso
Fuente: Irene Valero

Una vez realizado el análisis mediante la matriz genérica de amenazas se podrá reducir el árbol de ataque e identificar los niveles de amenaza altos según los vectores de ataque con respecto a clickjacking y con respecto a touchjacking los vectores.

MARCO METODOLOGICO

Diseño de Investigación

El presente caso de estudio es de tipo descriptivo ya que se analizará la bibliografía utilizando métodos investigativos para recolectar información y analizar los resultados que arrojen de los objetivos definidos.

Tipo de Investigación

En esta investigación se plantea analizar el problema utilizando los siguientes tipos de investigación:

Investigación Descriptiva

(Tatiana Mejia Jervis, 2020), La investigación descriptiva es un tipo de investigación que se encarga de describir la población, situación o fenómeno alrededor del cual se centra su estudio. Procura brindar información acerca del qué, cómo, cuándo y dónde, relativo al problema de investigación, sin darle prioridad a responder al "por qué" ocurre dicho problema. Como dice su propio nombre, esta forma de investigar "describe", no explica.

Nos permite realizar un análisis para identificar y observar las características de la población.

Como primer paso se analizaron escenarios procedentes de las investigaciones realizadas sobre los ataques clickjacking y touchjacking que han sido detectados durante el análisis de cada una de las investigaciones sugeridas.

Posteriormente, para el análisis de estos tipos de ataques se definieron las herramientas para realizar el análisis de los escenarios e identificar las principales amenazas a las que se ve expuesto.

Finalmente, se realizaron un análisis de la eficiencia de estos ataques, contrastando a los resultados de la bibliografía en cada uno de los escenarios, con las técnicas de mitigación que se han planteado como mejores prácticas de desarrollo y sanitización web, identificando oportunidades de mejora y recomendaciones para desarrolladores y administradores de sistemas.

RESULTADOS

Durante el análisis bibliográfico se pudo analizar que existen un grupo de herramientas y matrices que permiten evaluar y definir la protección referente a los ataques a nivel web sin embargo todo dependerá de la estructura o nivel de complejidad que se aplique en el desarrollo del ataque. Se evidencio también la importancia de realizar un análisis previo del diseño de posibles ataques para de esta forma mediante la utilización de herramientas como Microsoft Threat modeling y el diseño de árboles de ataque permitan evidenciar posibles falencias en el diseño bajo ciertas condiciones con el objetivo de determinar las correcciones necesarias que deben ser aplicadas.

Clickjacking: Referente a los ataques de clickjacking su implementación es mucho más frecuente con respecto a los ataques de touchjacking, destacando el método de ocultación debido a que muy sencillo de implementar y sin medidas de mitigación se torna imperceptible para los usuarios, sin embargo, se pudo observar además que la técnica de email spoofing es muy factible de ser usada por los atacantes en vista de que puede aplicarse ingeniería social que puede resultar muy efectiva incluso para usuarios con conocimientos de informática, en el desarrollo de los escenarios también se evidencio que la técnica de cursor spoofing y dom XSS se encuentran mitigadas con respecto algunos navegadores aunque son mucho más complejas de implementar.

Touchjacking: Este tipo de ataque se usa con menor frecuencia pero mediante la utilización de herramientas como beef se puede llevar acabo, con respecto a la implementación del método de ocultación con WebView este tipo de ataque resulta ser más complejo en vista de que existe un mayor esfuerzo por parte del atacante en realizar aplicaciones que permitan el robo de información y que logren camuflarse como una aplicación que no represente mayor riesgo a simple vista, no siendo el caso de aplicaciones web que representan un mayor riesgo y una mayor factibilidad de ser ejecutadas.

CONCLUSIONES

Con respecto a las técnicas de clickjacking y touchjacking analizadas en este caso de estudio se puede concluir que debido a la facilidad de implementación las técnicas de clickjacking son las más optadas por los atacantes. Mientras que las técnicas de touchjacking resultan ser más complejas debido a que deben ser implementadas dentro de una aplicación móvil nativa con la utilización de WebView.

En el análisis de evaluación con respecto a los entornos web tomando en cuenta que se implementaron los vectores de ataque y medidas de mitigación bajo las mismas condiciones se podría evidenciar y contrastar cual es más eficiente contrarrestando las técnicas de ataque de clickjacking y touchjacking.

Se pudo determinar mediante el análisis bibliográfico que de acuerdo con las evaluaciones de cada uno de los escenarios que se podría plantear que las principales características que facilitan la ejecución de los ataques de clickjacking y touchjacking. se podrían dar por una mala configuración del servidor web, la falta de sanitización y validación en las entradas de datos, así como también la poca utilización de plugins como medidas de protección en los navegadores.

Durante la etapa de estimación del riesgo mediante el análisis de las características referentes a nivel de compromiso y nivel de conocimiento se podría determinar que vectores de ataque fueron los más críticos tomando en cuenta los que se encontraban en un nivel de amenaza entre el rango medio-alto.

RECOMENDACIONES

Se recomienda para futuras investigaciones un planteamiento del estudio aplicando la información detallada con el fin de generar una biblioteca digital que especifique la aplicación de estos y su efectividad bajo ciertas condiciones, de igual forma se puede ampliar el estudio tomando en cuenta una mayor cantidad de entornos web que los considerados en esta investigación con el fin determinar la mejor opción del mercado con respecto a prestaciones.

Cabe recalcar que al momento de desarrollar un sitio web es importante evaluarlo desde el punto de vista de un atacante con el fin de evidenciar las falencias en el diseño e implementación, para estos casos se recomienda la ocultación del código fuente para impedir que el atacante encuentre falencias en el desarrollo y explotar esa vulnerabilidad.

REFERENCIAS

Cajías Borja, E. F. (2020). *Evaluación de la eficiencia de ataques de tipo clickjacking y touchjacking en entornos controlados* (Master's thesis, Quito, 2020.).

[1] Mendez Fonseca, V. J. (2020). Marco Tecnológico de un SOC de nueva generación.

Mieres, J. (2009). Ataques informáticos. *Debilidades de seguridad comúnmente explotadas). Recuperado http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf*.

[2] Gómez Coronell, O. (2014). *Estrategias de la seguridad de la Información para combatir el Fraude Bancario en Colombia* (Bachelor's thesis, Universidad Piloto de Colombia).

[3] Niño, F. Y. A. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*, *24*(49), 92-119.

[4] onterroza Barrios, R. E. (2019). Análisis, explotación y definición de estrategias de mitigación de vulnerabilidades en un sistema GNU/Linux.

[5] Tarazona, T., & Cesar, H. (2007). Amenazas informáticas y seguridad de la información. *Derecho penal y criminología*, *28*, 137.

[6] Gruber, S. L. A. (1982). *Historia social de los obreros industriales de Tampico, 1906-1919*. El Colegio de México.

[7] Sáinz, J. P. P., & Salas, M. M. (2004). De la oportunidad del empleo formal al riesgo de exclusión laboral. Desigualdades estructurales y dinámicas en los mercados latinoamericanos de trabajo. *Alteridades*, (28), 37-49.

[8] Romero, J. C. R. (2004). *Métodos de evaluación de riesgos laborales*. Ediciones Díaz de Santos.

[9] Quinaluisa, N., Ganchozo, M., Reyes, M., & Arriaga, G. (2017). Evaluación del sistema de control interno en empresas privadas. *Revista de Estrategias del Desarrollo Empresarial*, *3*(8), 25-30.

[10] Villarán, K. W. (2009). Plan de negocios. *Herramientas para evaluar la viabilidad de un negocio, USAID Perú y Ministerio de la Producción, Perú*.

Ruiz Guillen, H. F. (2022). *Gestión del software fénix para la administración de los inventarios en la Empresa Detodo. Com en la ciudad de Babahoyo* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2022).

Hernández Bejarano, M., & Baquero Rey, L. E. (2020). *Ciclo de vida de desarrollo ágil de software seguro*. Editorial Los Libertadores.

ANEXOS

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACION

Babahoyo 29 de Marzo del 2023

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de: el/la, Sr./Sra./ Srta.: **VALERO SANCHEZ IRENE MERCEDES**, cuyo tema es: **ANALISIS DE METODOLOGIAS DE ATAQUES DE TIPO CLICKJACKING Y TOUCHJACKING, EN ENTORNOS WEB** , certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de **[8 %]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.


CERTIFICADO DE ANALISIS

CASO DE ESTUDIO IRENE VALERO

Fuentes principales detectadas

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Ing. Sist. Iván Rubén Ruiz Parrales, Msg
DOCENTE DE LA FAFI.