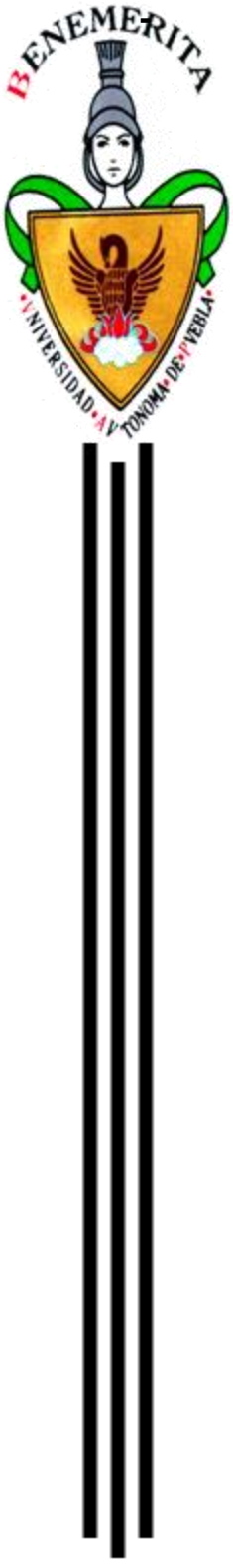
FACULTAD DE CIENCIAS
DE LA COMPUTACIÓN



Benemérita Universidad Autónoma de Puebla

Herramienta de enseñanza aprendizaje para el entrenamiento de Hacking Ético

Tesina para obtener el grado académico de

Licenciado en Ciencias de la Computación

Presenta

Luz Adriana Huerta Rosas
Matrícula: 200013775

Asesor

M.C. Meliza Contreras Gonzalez

Puebla, Puebla Enero de 2021

INDICE

Introducción

Proteger los sistemas y redes hoy en día es una necesidad imperante, la seguridad informática ha pasado de ser un gasto a una inversión en muchas organizaciones alrededor del mundo. Debido a nuestra convergencia al mundo digital la información se ha transformado en un activo intangible pero sumamente valioso y, al ser activo debe ser resguardado por robo, intrusión, pérdida, uso indebido etc.

De acuerdo con Kaspersky (Kaspersky, 2020) a partir de 2019 se generó un incremento de ciberataques debido a ransomware. Para 2020 se vaticina que esto se potencialice ya que los delincuentes cibernéticos siguen generando nuevos ataques y las empresas están cada vez más desprotegidas por la falta información, conocimiento y personal capacitado dentro de sus instalaciones que advierta de estas situaciones.

Tal motivo provoca que sea más indispensable contar con mecanismos y herramientas que permitan no sólo al especialista en seguridad informática o hacking ético atender dichas exigencias sino también al especialista en sistemas de computación o tecnologías de la información contar con conocimientos generales y básicos para poder resguardar la privacidad de una entidad la cual requiere atención para salvaguardar información sensible, conociendo e identificando algunas de las estrategias más comunes de ataque y reconociendo las tácticas, herramientas y motivaciones de los hackers.

Los sistemas existentes de entrenamiento carecen de una estructura específica, son elitistas y se encuentran dispersos en diversas fuentes, por lo cual sería importante contar con un instrumento de apoyo para mostrar cómo detectar eficientemente las vulnerabilidades con pruebas de intrusión controladas sobre sistemas de entrenamiento que permitan progresivamente comprender mejor los procesos para detectar sistemas débiles, por lo que se desprende la necesidad de generar una herramienta que cuente con una estructura que facilite el aprendizaje de la seguridad informática de manera ética(hacking ético).

Objetivos

General. -

Desarrollar herramientas de apoyo para distinguir riesgos en la seguridad informática, generando una secuencia de actividades que nos indiquen el camino para la prevención y corrección de software débil, identificando a su vez cuáles son los elementos que los crackers aprovechan para provocar brechas de seguridad en los sistemas y prevenirlos.

Específicos. -

Los objetivos específicos son los siguientes:

- Identificar algunas vulnerabilidades más frecuentes
- Analizar esas vulnerabilidades y prevenciones pertinentes a las mismas
- Generar lecciones de acuerdo a las vulnerabilidades presentadas

Capítulo I

Estado del Campo o del Arte

1.1 Estado del Arte

Software	Ventajas	Desventajas
www.hacksplaining.com/lessons (Hacksplaning, 2020)	A simple vista es una plataforma amigable para el entrenamiento de hacking, la interfaz con el usuario es gráfica, los botones de interacción son descriptivos. Cuenta con un gran número de ejercicios y vulnerabilidades para practicarlos.	A pesar de que parece una interfaz amigable e intuitiva realmente carece de sencillez y de fácil comprensión respecto a otros softwares comerciales que llevan de la mano al usuario final y no requieren de muchas habilidades para aprender a usarlo por ejemplo Paint (CLUF, 1995). Al explorar el sitio se entiende que el testeador debe tener previos conocimientos de hacking y del idioma inglés.
https://hack.me/102812/easy-admin-login.html (Inc, 2020)	Plataforma donde la comunidad dada de alta en el sitio puede codificar, hospedar o compartir código vulnerable con fines educativos. Por tal razón cuenta con un gran banco de datos para practicar. Está disponible para cualquier persona interesada en	A pesar del acceso aislado que da sandbox cada que ingresamos al sitio no nos ofrece seguridad total de nuestro equipo. El código que se comparte en este sitio puede ser usado y compartido a su vez por quien requiera del mismo, pero el creador del código

	aprender hacking ético	es responsable del uso indebido que se le dé. Página nada amigable, entorno de difícil comprensión y carente de estructura de acuerdo al término usabilidad que indica que el software debe incluir una serie de métricas y métodos que buscan hacer que un sistema sea fácil de usar y de aprender (Beta, 2020). Se requiere previo conocimiento de hacking y del idioma inglés
https://app.cybrary.it/ (HQ, 2020)	Plataforma para estudio y certificación de hacker. Cuenta con una gran cantidad de cursos dividido en especialidades, grado de dificultad o línea de certificación. Se puede formar un equipo para estudiar a la par y tomar la experiencia en grupo.	Los cursos de certificación no son gratuitos y todos ellos se imparten en idioma inglés.

1.2 Justificación

La tecnología ha avanzado de manera exponencial provocando de cierta manera que existan muchas nuevas formas de extorsión y robo. Las brechas en la seguridad han permitido tener acceso a sistemas remotos de forma ilícita

Las herramientas existentes hoy en día para el entrenamiento de hacking ético son bastante robustas para la interacción con el usuario con previos conocimientos en el área de hacking. De acuerdo a todas ellas se puede practicar,

y actualizar al interesado en esta materia, desgraciadamente el usuario que lleve a cabo esta tarea sin conocimientos de seguridad informática previos corre el riesgo de sentirse frustrado en el momento de interactuar con este tipo de software avanzado, tal situación nos motivó a diseñar lecciones que permitan asimilar paulatinamente el contenido valiéndose de varios elementos amigables interactivos e intuitivos que hagan del entrenamiento un evento de aprendizaje y de fácil entendimiento, guiando los pasos del usuario por una ruta organizada y ordenada.
La información estructurada con la que cuenta es de fácil acceso, gratuita, en español, y de fácil comprensión para que los usuarios practiquen hacking ético y puedan perfeccionar e identificar las técnicas de seguridad.

Poder prevenir y solucionar este tipo de situaciones de una forma rápida y eficaz sin hacer gran inversión es lo que nos motiva a llevar a cabo este proyecto.

Capítulo II

Marco Teórico

2.1 Antecedentes

En los últimos años el término de “hacking ético” se ha considerado algo positivo o negativo desde varios puntos de vista ya que el nombre confunde por las palabras que lo conforman. La palabra ético nos indica algo positivo y hacking algo negativo, esto es debido a desconocimiento de esta materia y a la falta de información al público en general (Tori, 2016)

En 1977 la necesidad de la seguridad informática comenzó a generar conciencia, se cayó en cuenta que los hackers éticos podían ayudar a las empresas a proteger su información y ser menos vulnerables y en 2001 se comenzaron a dar estas asesorías. De este modo los hackers blancos trabajando por su cuenta, dentro de una empresa o por medio de consultoras empezaron a ofrecer este tipo de servicio para encontrar vulnerabilidades en sus sistemas, prevenir y corregir este fallo.

Cuando en 1997, la cultura de la seguridad informática comenzó a tomar fuerza, se pensó que los hackers éticos podían ofrecer sus servicios a las empresas para ayudarlas a ser menos vulnerables, y en 2001 arrancaron en forma este tipo de asesorías.

Para 2010, solo el 30 por ciento de las compañías del país habían adoptado medidas de prevención de fraudes, las cuales pueden deberse a fallas en los sistemas, información divulgada consciente o inconscientemente por los trabajadores de las mismas, ataques informáticos, falta de cultura organizacional, entre muchas otras.

Convencer a las compañías de contratar un este tipo de servicios de hacking ha sido muy complicado, conseguir el permiso para que ingrese y manipule los sistemas no ha sido tarea fácil (Soriano, Haking Ético, mitos y realidades, 2017).
Pero poco a poco con las necesidades cada vez más imperantes en este aspecto el término se ha ido asimilando y aceptando, ahora los hackers éticos empiezan a ser conocidos y cada vez más las organizaciones buscan sus servicios.

El hacking ético o prueba de penetración es una auditoria con la cual se pueden detectar vulnerabilidades en un sistema y después se pueden corregir y proteger a la información sensible.

Las pruebas de penetración nacieron a la necesidad de mitigar los primeros ataques informáticos en las organizaciones, los cuales trajeron graves consecuencias, como pérdidas monetarias y de reputación.

Con el paso del tiempo han ido cambiando las cosas, ahora el hacking ético ya no es o no debería ser un conocimiento elitista y paso a paso se va haciendo más accesible la información y la compresión de la problemática que genera la ignorancia sobre este tema, pero desafortunadamente, todavía existe muy poca inversión por parte de las empresas en este tipo de auditorías, ya que no se le presta la debida importancia, y se prefiere invertir en otras áreas que puedan recuperar la inversión a corto plazo, o porque no conocen de este tipo de problemas.

De acuerdo con el Informe Hacker de 2019, la comunidad de hackers éticos se ha ido duplicando año tras año (Ku, 2019)

Esto ha traído demasiado interés a las nuevas generaciones haciendo cada vez más solicitados los cursos o conocimientos sobre el tema ya que las personas que realizan este tipo de servicio tienen grandes ingresos debido a la escasez de los mismos.

2.2 Técnicas de Hacking Ético

A continuación, se mencionarán algunos de los modos más comunes de hacking ético los cuales son (ehack, 2020):

2.2.1 Acceso local

En este tipo de ataque se simula ser o tener acceso autorizado y las defensas que deben ser burladas son: Firewalls, servidores web y medidas de seguridad del servidor.

2.2.2 Acceso Remoto

Este tipo de ataque simula un intruso tratando de accesar por medio de Internet, las metas a alcanzar son HTTP (Hypertext Transfer Protocol, SQl (Structured Query Languaje), SMTP (Simple Mail Transfer Protocol) o cualquier otro servicio. Para lograr esto el primer obstáculo debe ser vencido, esto es el firewall externo, enrutadores entre otros.

2.2.3 Acceso con equipos robados

El robo de un equipo puede ser muy útil cuando se requiere información de una empresa. Con esto se puede hacer vulnerable a una organización ya que podemos penetrar en los archivos más delicados como son contraseñas y archivos importantes para la misma.
Esto puede suceder no solo con un equipo de cómputo, también USB, discos externos, o cualquier medio que una empresa tenga como copias de seguridad.

2.2.4 Acceso por medio de Ingeniería social

En esta prueba se busca evaluar la integridad y el compromiso del Personal de la organización. Se manipula empleados para obtener información privilegiada que solo los empleados en general o de confianza pueden ofrecer.

2.3 Vulnerabilidades

De toda esta problemática reciente podemos mencionar 3 vulnerabilidades más comunes las cuales a grandes rasgos describiremos aquí (viewnext, s.f.):

2.3.1 Carga de Archivos

Permite el enlace de archivos remotos situados en otros servidores a causa de una mala programación de la página que contiene funciones de inclusión de archivos.

2.3.2 Ejecución de código

Un atacante puede aprovechar esta vulnerabilidad con éxito, ya que podría ejecutar código arbitrario en la computadora del cliente que se conecta. Un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario.

2.3.3 Inyección SQL

En esta vulnerabilidad un experto en sintaxis SQL envía entradas falsas en formularios de páginas web con el objetivo de obtener un acceso más directo y profundo a la base de datos administrativa del que puede obtener la aplicación web. Se previene codificando minuciosamente e instalando firewalls entre otros.

2.4 Herramientas existentes

De esta situación se han creado herramientas existentes para el manejo, entrenamiento y resguardo de la información para hacker ético y entestes

2.4.1 Hacksplaning

Es un sitio web recientemente establecido ayuda aprender y protegerse contra los crackers. Combina gráficos animados para mostrar la vulnerabilidad y, al mismo tiempo, a través de ejemplos interactivos, indicaciones e instrucciones para que el estudiante hackee el sitio de prueba como lo haría un hacker profesional.

A pesar de que parece una interfaz amigable e intuitiva realmente carece de sencillez y de fácil comprensión respecto a otros softwares comerciales que llevan de la mano al usuario final y no requieren de muchas habilidades para aprender a usarlo por ejemplo Paint (CLUF, 1995). Al explorar el sitio se entiende que el testeador debe tener previos conocimientos de hacking y del idioma inglés.

2.4.2 Hack.me

Es un proyecto gratuito basado en la comunidad impulsado por eLearnSecurity.
La comunidad puede construir, alojar y compartir código de aplicación web vulnerable con fines educativos y de investigación.
Su objetivo es ser la mayor colección de aplicaciones web vulnerables "ejecutables", ejemplos de código y CMS en línea.
A pesar del acceso aislado que da sandbox cada que ingresamos al sitio no nos ofrece seguridad total de nuestro equipo.
El código que se comparte en este sitio puede ser usado y compartido a su vez por quien requiera del mismo, pero el creador del código es responsable del uso indebido que se le dé.
Página nada amigable, entorno de difícil comprensión y carente de estructura de acuerdo al término usabilidad que indica que el software
debe incluir una serie de métricas y métodos que buscan hacer que un sistema sea fácil de usar y de aprender (Beta, 2020).

2.4.3 App.cybrary.it

Según cybrary son un catálogo de muy rápido crecimiento y de mas

movimiento en la industria. Al trabajar con una comunidad de élite de instructores, expertos y líderes de opinión, así como con proveedores de aprendizaje prácticos de vanguardia, brindan contenido relevante y de alta calidad al que se puede acceder en cualquier momento y en cualquier lugar.
Desgraciadamente el acceso a ellos es complicado y no es para todo el público debido a que los cursos de certificación no son gratuitos y todos ellos se imparten en idioma inglés.

2.4.4 Metasploitable

Es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración y el desarrollo de firmas para sistemas de detección de intrusos.
Lamentablemente no cuenta con entorno gráfico y no tiene versión en español.
Se debe usar en redes privadas debido a la tolerancia a ataques.
Depende de otros softwares para su funcionamiento (virtual box, disco virtual de metasploitable)
Requiere de un correo corporativo para poder descargarlo.
Se necesitan conocimientos previos para su correcto uso.

Los ataques evolucionan día con día, por lo que los sistemas deben ser probados constantemente. Para poder soportar ataques y mantener la confianza de sus clientes, las empresas necesitan protección y estar a la vanguardia en cuanto a ciberseguridad (Villa)
Con cada nueva tecnología que aparece surgen nuevas amenazas. Si bien las defensas siempre van actualizándose es importante estar siempre atentos a los nuevos ataques que se pueden generar, y es por esto que se requiere el trabajo de hackers éticos preparados, capaces y estar actualizados en materia de seguridad.

2.5 Metodología del desarrollo

Se ocupará un modelo secuencial de cascada el cual debido al alcance del proyecto y que es realizado por una persona será más fácil de utilizar para el fin de esta herramienta a desarrollar.
El modelo es un proceso de desarrollo secuencial, en el que el desarrollo de software se concibe como un conjunto de etapas que se ejecutan una tras otra (figura 2.1).
Al final de cada etapa, el modelo está diseñado para llevar a cabo una revisión final, que se encarga de determinar si el proyecto está listo para avanzar a la siguiente fase

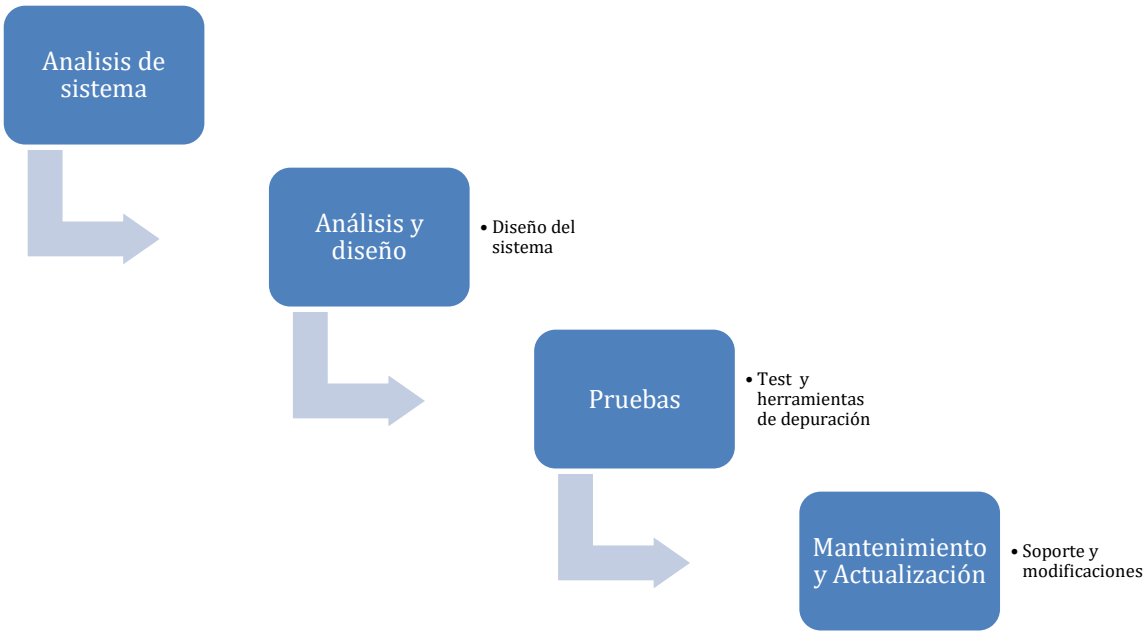


Figura 2.1 Modelo de cascada
Elaboración propia

2.5.1 Software

Para implementar el análisis y diseño de esta herramienta se requiere:
-Visual Paradigm (Paradigm, s.f.)
Herramienta UML de diagramas de casos de uso, la cual nos permite probar la herramienta de manera gratuita en internet y

solamente nos pide registrarnos y podemos utilizar todas sus herramientas.
Entre las ventajas que podemos observar con esta herramienta es:

- Disponibilidad en múltiples plataformas: Microsoft Windows (98, 2000, XP, o Vista), Linux, Mac OS X, Solaris o Java.
- Apoya todo lo básico en cuanto a artefactos generados en las etapas de definición de requerimientos y de especificación de componentes.
- Podemos intercambiar información mediante la exportación de ficheros con otras aplicaciones por ejemplo Visio y Rational Rose.
- Da la posibilidad de generar código a partir de los diagramas para plataformas como .Net, Java y PHP, así como viceversa.
- Brinda la posibilidad de documentar todo el trabajo sin necesidad de utilizar herramientas externas

Las desventajas de esta herramienta son casi nulas, la que se puede mencionar es que las imágenes y reportes generados no son de muy buena calidad.

Para las lecciones se ocupará el siguiente software

a) Virtual Box

Software de virtualización actualmente desarrollado por Oracle.

Entre las ventajas podemos nombrar:

- Es de licencia libre.
- Actualización constante y es cada vez más compatible.
- Virtualiza diferentes sistemas operativos
- Configuración de red con distintas opciones.
- Compatible para distintas arquitecturas.
- Entorno grafico atractivo.
- Múltiples configuraciones muy fáciles de utilizar.
- Compatible para Windows, Linux y Mac OS

Las desventajas

- La configuración en la resolución es un poco estática.

- No reconoce algunos distros de Linux que son poco conocidos.
- Algunas funciones de algunos sistemas operativos están escondidas al ejecutar con el Virtual Box.

b) Metasploitable

Es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración y el desarrollo de firmas para sistemas de detección de intrusos.
Lamentablemente no cuenta con entorno gráfico y no tiene versión en español.
Se debe usar en redes privadas debido a la tolerancia a ataques.
Depende de otros softwares para su funcionamiento (virtual box, disco virtual de metasploitable)
Requiere de un correo corporativo para poder descargarlo.
Se necesitan conocimientos previos para su correcto uso.

c) Kali Linux

Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.
Entre las ventajas podemos ver las siguientes
Es gratis, multilenguaje, totalmente personalizable y tiene un entorno de desarrollo seguro.
Se han añadido nuevas herramientas y actualizado las existentes.
En las desventajas
En ocasiones, las actualizaciones son muy complejas

d) Pip

Es un sistema de gestión de paquetes utilizado para instalar y administrar paquetes de software escritos en Python.
No se menciona ventajas o desventajas pues es la herramienta que se ocupa por default para instalación de paquetes.

e) DnsPython

Es una herramienta de Python. Soporta todos los tipos de registros. Puede ser usado para consultas o actualizaciones dinámicas, no hay otra herramienta que la supla.

f) Knock

Es una herramienta de Python diseñada para enumerar subdominios en un dominio objetivo a través de una lista de palabras. No existe otra herramienta que podamos ocupar en lugar de knock

g) BurpSuite

Completo pack de herramientas para la comprobación de la seguridad de aplicaciones web desarrollado por PortSwigger Web Security.
Las ventajas que tiene esta aplicación es que realiza escaneos de vulnerabilidad web, tiene un gran base de datos con las más nuevas vulnerabilidades, tiene compatibilidad con webs dinámicas y estáticas, tiene un análisis de vulnerabilidades potente gracias al escaneo tanto del cliente como del servidor, provee información personalizada sobre cada análisis, además de que podemos guardar repostes para usarlos más tarde y tiene compatibilidad con proxy

La desventaja registrada es que la versión profesional no cuenta con todas las características del programa como los escaneos programados automáticos

2.6. LMS

Para la implementación de las lecciones se instalarán en el sistema de gestión de aprendizaje (LMS por sus siglas en inglés)

2.6.1 LMS existentes

1. Chamillo
2.Wordpress
3.Evolcampus
4. Canvas
5. Moodle

Los LMS mencionados anteriormente son de las más populares opciones, pero elegí Moodle por encontrar muchas más ventajas que desventajas las cuales mencionaré a continuación:

Entre las ventajas que encontramos son:

-Facilita la comunicación de los docentes y estudiantes fuera del horario de clases.
-En ellos que podemos incluir gran variedad de actividades y hacer un seguimiento exhaustivo del trabajo de los estudiantes
-Ayuda al aprendizaje cooperativo ya que permite la comunicación a distancia mediante foros, correo y chat.
-Dispone de varios temas o plantillas fáciles de modificar
-Se encuentra traducido a más de 70 idiomas.
-Los recursos que el docente entrega a sus estudiantes pueden ser de cualquier fuente y con cualquier formato
-Lleva registro de acceso de los estudiantes y un historial de las actividades de cada estudiante
-Moodle no tiene limitaciones en cuanto al número de cursos, sino las limitaciones se dan en función al servidor, ancho de banda en donde se encuentre instalado.

Entre las desventajas que encontramos podemos destacar:
-La comunicación y colaboración constante es importante puesto que no hay la presencia del docente

2.7 Marco Legal

La ley en sus diversas modalidades aplica tanto en el mundo físico como en el mundo virtual.
Un fraude tipificado como tal lo sigue siendo si dicho fraude usa medios informáticos. En México ya se ha procesado criminales que han cometido delitos informáticos y cuyo rastro ha sido perfectamente identificado y tornado en evidencia. Estos casos no sólo incluyen el acceso no autorizado a equipos informáticos, sino también temas de violación de propiedad intelectual, delitos derivados del acoso y el sexting que pueden entenderse

desde lenocinio, pornografía infantil, estupro, delitos financieros, robo y suplantación de identidad, fraude en grado de tentativa, fraude financiero y de otras índoles, y varios de ellos con agravantes como la asociación delictiva. (Reyes, 2016)
Las multas van de 3 meses a 9 años de prisión dependiendo del agravante, pero haciendo el proceso legal con contrato por parte de las empresas para que autoricen a ingresar a su información podemos poner en práctica lo aprendido en la herramienta de hacking ético o con algún curso de especialización en el tema.

Capítulo III

Análisis

Considerando la metodología de cascada que aplicaremos para el ciclo de vida de desarrollo de este sistema procederemos a realizar el análisis y diseño del sistema.

3.1 Requisitos funcionales

Herramienta que se apoyará de un sistema vulnerable para permitir al usuario que tomará las lecciones conocer e identificar y abordar a los sistemas débiles o mal programados y poder ejecutar acciones para corregir o prevenir las situaciones que provocan la vulnerabilidad del mismo

Para ello nos basaremos en lecciones visuales guiadas paso a paso que invitarán al usuario ocuparlas cuantas veces quieran, entenderlas y probar las lecciones en sus propios equipos de manera que comprendan y practiquen directamente en la comodidad de sus hogares todas estas técnicas y vulnerabilidades sugeridas ya que la práctica es el mejor método para la comprensión y la ejecución correcta de estas técnicas un tanto complejas.

Por medio de estas herramientas se generarán puertas traseras en los tres tipos de vulnerabilidad mencionadas en este documento, las cuales nos permitirán explotar el sistema abordado y dar un informe preciso de todas las debilidades del mismo y como poder prevenir y corregir tal proceso.

3.2 Requisitos no funcionales

Para este la ejecución de estas herramientas es importante tomar en cuenta que se requiere del acceso al equipo físicamente, comprendiendo que este análisis se lleva a cabo completamente en sitio, para poder dar observaciones, prevenciones o correcciones al usuario final.

Si el sistema es subido a un servidor WEB podría ser accesible y portable hacia cualquier plataforma y la disponibilidad de estas herramientas estaría disponible las 24 horas para ver las veces que sea necesarias y repetirlas en caso de requerirlo dando paso a que muchas personas puedan capacitarse con estas herramientas.

Es escalable hacia cualquier línea de aprendizaje y además puede ser modificado y actualizado cuando se requiera por la facilidad que da Moodle a los cambios del mismo, también podemos agregar muchos módulos adicionales a la misma en el caso de mantenimiento y actualización.

Con respecto a la operatividad el sistema debe funcionar en una PC con un solo procesador, que pueda albergar un servidor de páginas web y al mismo tiempo pueda ser cliente.

La Interfaz con el usuario está dada por medio de Moodle la cual hemos podido diseñar debido a su facilidad de uso, muestra menús para opciones a realizar, unas rutas perfectamente divididas y organizadas, haciendo de la página un trabajo muy limpio, estructurado y comprensible en cuanto a que línea de aprendizaje se debe tomar y el paso a paso a seguir.

A continuación, analizaremos el diagrama de casos de uso el cual describe las actividades realizadas en nuestra herramienta.

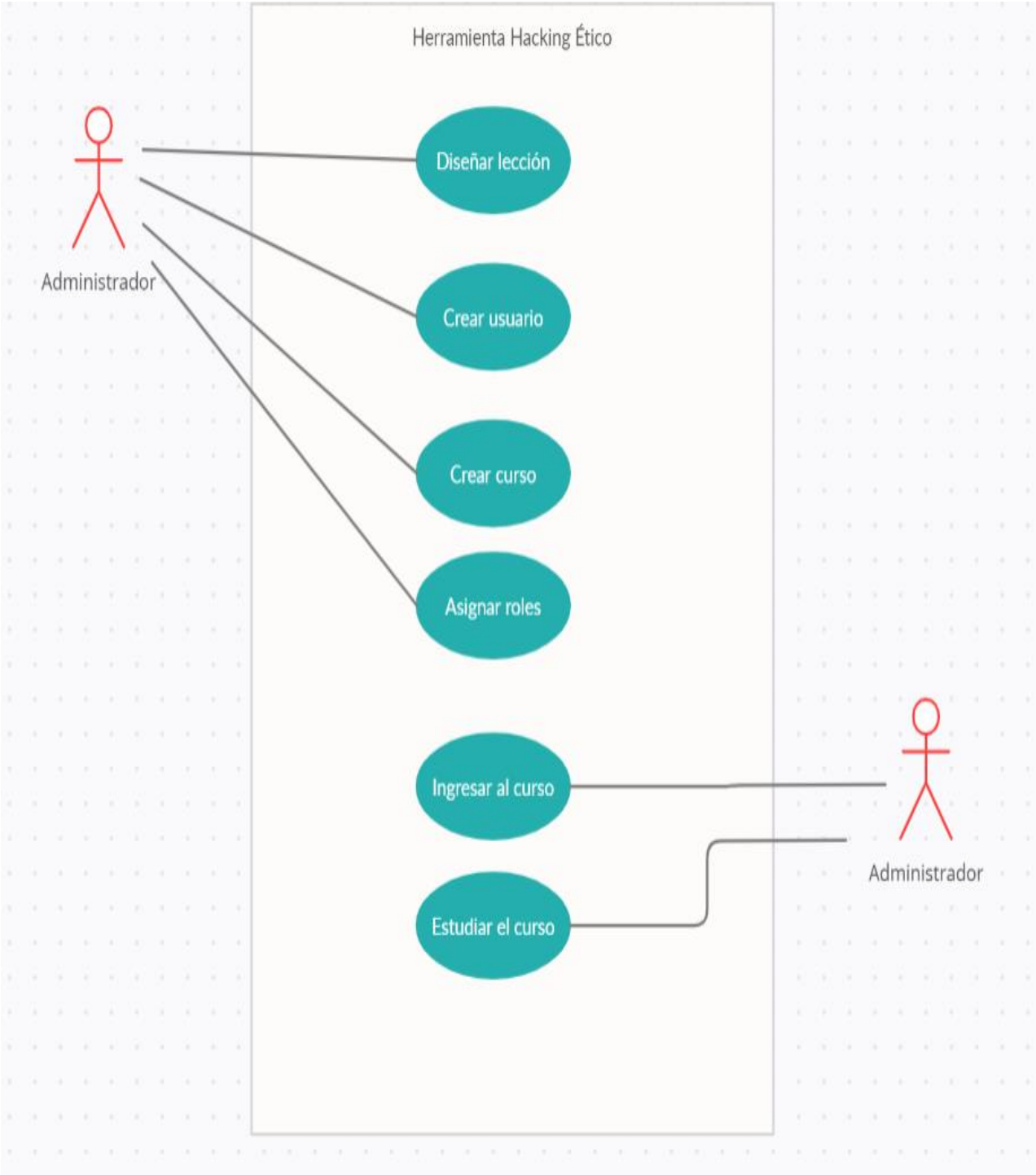


Figura 3. Caso de Uso

3.3. Análisis del sistema

3.3.1 Especificación de casos de uso

1.Nombre	Diseñar lección
2.Autor	Luz Adriana Huerta Rosas
3.Fecha	01-10-2020
4.Descripción	El administrador diseñará el curso

5. Actores:

5.1. Administrador

6. Precondiciones:

6.1. Conocimiento del diseño técnico y didáctico del curso

7. Flujo básico:

7.1. El administrador confirma la información básica del curso, fecha de inicio, acceso a cursos, duración de cada curso, navegación, definir conocimien tos previos etc

7.2. El administrador planifica el curso definiendo tiempo de estudio por curso, numero de estudiantes, accesos permitidos a cursos

7.3. El administrador realiza el diseño didáctico del curso de acuerdo a lo que se ha establecido previamente en la planificación y estructuración de contenido asi como la pedagogía a usar

7.4. El administrador determina el tema y establece objetivos

7.5 El administrador escoge el material didáctico para la lección(video)

7.6 El administrador agrega una actividad de aprendizaje en cada lección

7.7 Termina el caso de uso

7.9 Salir

1.Nombre	Crear usuario
2.Autor	Luz Adriana Huerta Rosas
3.Fecha	01/10/2020
4.Descripción	En este caso de uso, el sistema le permite al administrador crear y dar privilegios al usuario

5. Actores:

5.1. Administrador

6. Precondiciones:

6.1. El administrador entra al sistema Moodle

7. Flujo básico:

7.1. El administrador selecciona la opción administración del sitio

7.2. Moodle muestra pestañas de opciones

7.3. El administrador escoge la pestaña Usuarios

7.4. El administrador escoge la opción “agregar usuario”

7.5. Se despliega la opción General en la cual se va a introducir el nombre de usuario, la contraseña, sus datos generales, una imagen de ser necesario.

7.6. El administrador presiona el botón “crear usuario”

7.6.1 Si el sistema provoca error en el campo contraseña ir al punto **8.1 de flujo alternativo.**

7.7 Termina el caso de uso

8. Flujo alternativo:

8.1. El administrador escoge una contraseña para el nuevo usuario que el sistema no pueda ingresar.

8.1.1. El administrador reintenta con una contraseña adecuada conformada por al menos 8 caracteres, 1 mayúscula, un digito y un carácter especial conforme lo indica el sistema.

8.1.2 Continua el flujo en el punto 7.6 de flujo básico

9. Flujo de excepción:

9.1. El sistema no se puede ejecutar por error en algún componente

1.Nombre	Crear Curso
2.Autor	Luz Adriana Huerta Rosas
3.Fecha	01-10-2020
4.Descripción	El administrador diseñará el curso

5. Actores:

5.1. Administrador

6. Precondiciones:

6.1. El usuario debe entrar en la interfaz de inicio en Moodle

7. Flujo básico:

7.1. El administrador selecciona la opción administración del sitio

7.2. Moodle muestra pestañas de opciones

7.3. El administrador escoge la pestaña Usuarios

7.4. El administrador escoge la opción “Cursos”

7.5 El administrador escoge la sub opción “Agregar un nuevo curso”

7.6 Dentro de esta opción el administrador agrega los detalles del curso nuevo

como: Nombre, descripción, el inicio del curso, la apariencia, y el formato del mismo.

7.7 El administrador da clic al botón “Guardar cambios y mostrar”

7.8 Termina el caso de uso

7.9 Salir

8. Flujo de excepción:

9.1. El sistema no se puede ejecutar por error en algún componente

1.Nombre	Asignar roles de usuario
2.Autor	Luz Adriana Huerta Rosas
3.Fecha	01-10-2020
4.Descripción	El administrador asignará roles a los usuarios

5. Actores:

5.1. Administrador

6. Precondiciones:

6.1. El usuario debe entrar en la interfaz de inicio en Moodle

7. Flujo básico:

7.1. El administrador selecciona la opción administración del sitio

7.2. Moodle muestra pestañas de opciones

7.3. El administrador escoge la pestaña Usuarios

7.4. El administrador escoge la opción “Asignar roles globales”

7.5 El administrador escoge uno de los roles existentes

7.5.1 Si no existe ningún usuario ir al flujo alternativo **8.1**

7.6 El administrador le da clic al botón agregar

7.8 Termina el caso de uso

7.9 Salir

8. Flujo alternativo:

8.1 Ir al caso de uso crear usuario

8.2. El flujo continua en el punto **7.6**

8.3 Salir

9. Flujo de excepción:

9.1. El sistema no se puede ejecutar por error en algún componente

1.Nombre	Ingresar al curso
2.Autor	Luz Adriana Huerta Rosas
3.Fecha	01-10-2020
4.Descripción	El alumno ingresará a la plataforma Moodle para estudiar el curso

5. Actores:

5.1. Estudiante

6. Precondiciones:

6.1. El administrador deberá proporcionar al estudiante el nombre de usuario y contraseña asignado

7. Flujo básico:

7.1. El estudiante va a la página principal del curso

7.2. Introduce el nombre de usuario y contraseña

7.2.1 Usuario incorrecto Flujo alternativo 8.1

7.2.2 Contraseña incorrecto Flujo alternativo 8.2

7.2.3 Usuario o contraseña inexistente Flujo de excepción 9

7.3. El usuario escoge el único curso disponible Hacking Ético

7.4 Entra al curso

7.8 Termina Caso de Uso

8 Flujo alternativo:

8.1 Introducir de nuevo usuario revisando que la tecla Bloq Mayus no esté activada

8.1.1 Ir a flujo básico 7.2

8.2. Introducir una contraseña revisando que la tecla Bloq Mayus no esté activara

8.2.1 Ir a flujo básico 7.2

8.3. Intentar de nuevo o checar con el administrador si el nombre de usuario y contraseña asignado está correcto.

8.3.1 Ir a flujo básico 7.2

8.4 Salir

9. Flujo de excepción:

9.1 Checar con el administrador si el nombre de usuario y contraseña asignado es correcto

9.2 Regresar a flujo básico 7.2

1.Nombre	Estudiar Curso
2.Autor	Luz Adriana Huerta Rosas
3.Fecha	01-10-2020
4.Descripción	El estudiante explora el curso

5. Actores:

5.1. Estudiante

6. Precondiciones:

6.1. Caso de uso ingresar al curso

7. Flujo básico:

7.1. El estudiante escoge la primera opción en el menú

7.2. El estudiante da clic a la subopción activa

7.3. El estudiante avanza hacia el siguiente modulo

7.3.1 Si no concluyo el inmediato anterior ir al punto 7.1

7.4 El estudiante desbloquea el módulo anterior y puede avanzar al siguiente

7.7 Salir

7.8 Termina Caso de Uso

9. Flujo de excepción:

9.1 El usuario no concluye los módulos y la plataforma bloquea hasta que los termine para poder avanzar

9.2 Regresar a flujo básico 7.1

3.3.2 Diagrama de navegación

La navegación lineal autoriza un flujo de información estable, es muy útil cuando se quiere llevar un proceso paso a paso, por tanto, es la indicada para mostrar el flujo de navegación de la herramienta en temas y subtemas

En nuestra herramienta contamos con 6 bloques los cuales cuentan con varias lecciones cada uno (figura 3.1)

Cada lección de esta herramienta lleva de la mano al estudiante, debe ser obligatorio pasar cada una para poder avanzar a la siguiente, lo que se ve en cada una de ellas a grandes rasgos es lo siguiente:

1. Introducción

En estas lecciones podemos identificar lo que es hacking ético, como hackear un sitio web, entender que es una página web y el glosario de términos con casi más de 100 definiciones de las herramientas

2. Instalación del software

Este conjunto de herramientas nos guiará paso a paso a la instalación del software necesario para poder hacer pruebas de pentesting.

3. Recabando información

Estas herramientas enseñan a detectar direcciones ip, las tecnologías que ocupa un sitio web, DNS, dominios y subdominios así como a descubrir archivos ocultos o paginas privadas de los sitios web, esto es importante debido a que se requieren para poder empezar a realizar pentesting, es la antesala del mismo

4.Vulnerabilidad de carca de archivos

Con estas herramientas el estudiante podrá identificar si una página web es vulnerable a través de la carga de archivos, se aprenderá a crear backdoors o puertas traseras en seguridad baja, media y alta así como a prevenir este tipo de vulnerabilidad en un sitio web

5. Vulnerabilidad de ejecución de código

A través de estas herramientas el estudiante podrá identificar si un sitio web permite ejecución de código y como prevenir este tipo de vulnerabilidades, aprenderá a ejecutar el código en un sitio con seguridad baja y también seguridad media.

6. Vulnerabilidad iSQL

Con estas herramientas el estudiante aprenderá a generar vulnerabilidades por medio de inyecciones SQL, podrá detectar si el sitio esta programado en SQL y también podrá introducirse por medio de usuario y contraseña en una pagina incluso como administrador, también aprenderá a prevenir este tipo de vulnerabilidades.

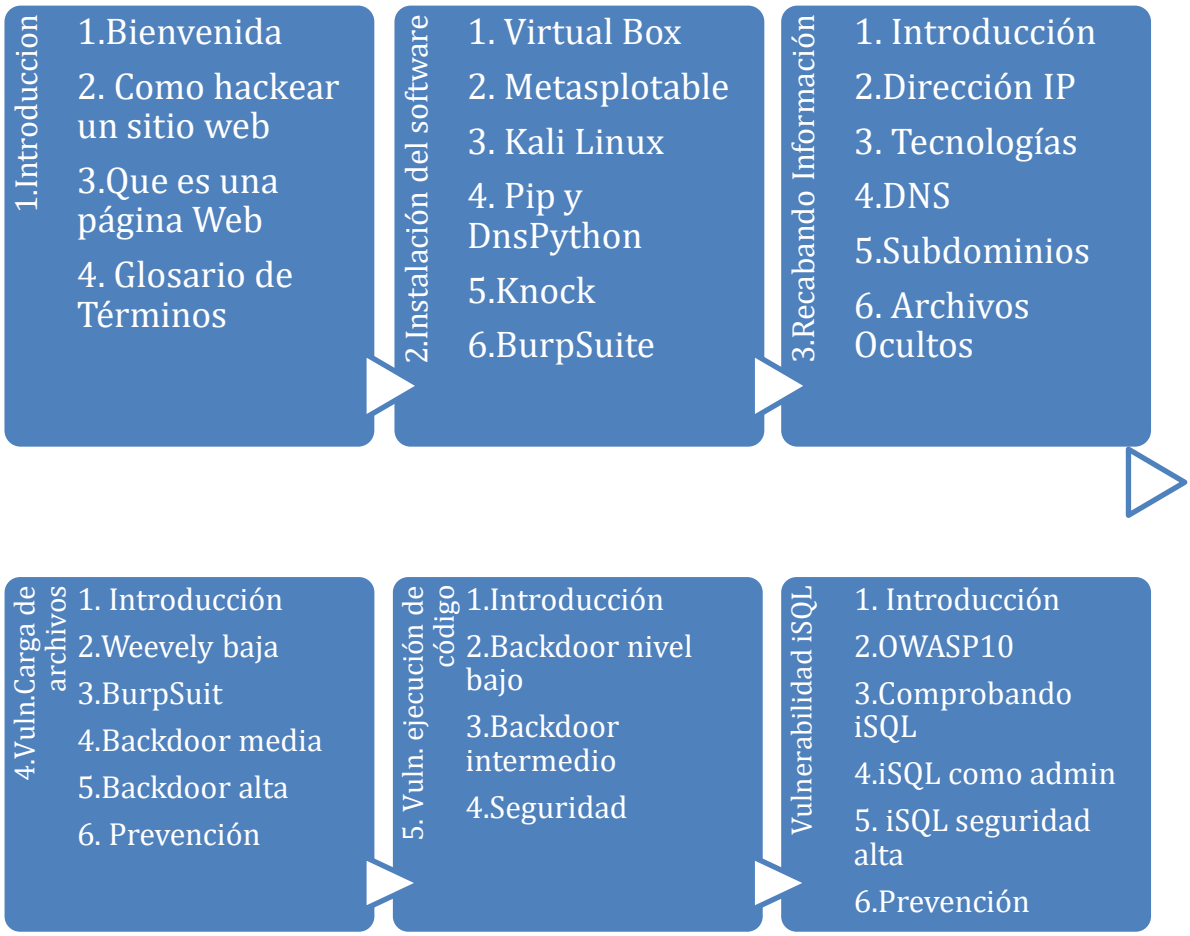


Figura 3.1 Diagrama de navegación

3.3.3 Modelo Conceptual

3.3.3.1 Diagrama de clases

En este apartado se aplicarán los conceptos del paradigma orientado objetos, para poder abstraerlos a clases.

La siguiente figura muestra un diagrama de clases de nuestra herramienta.

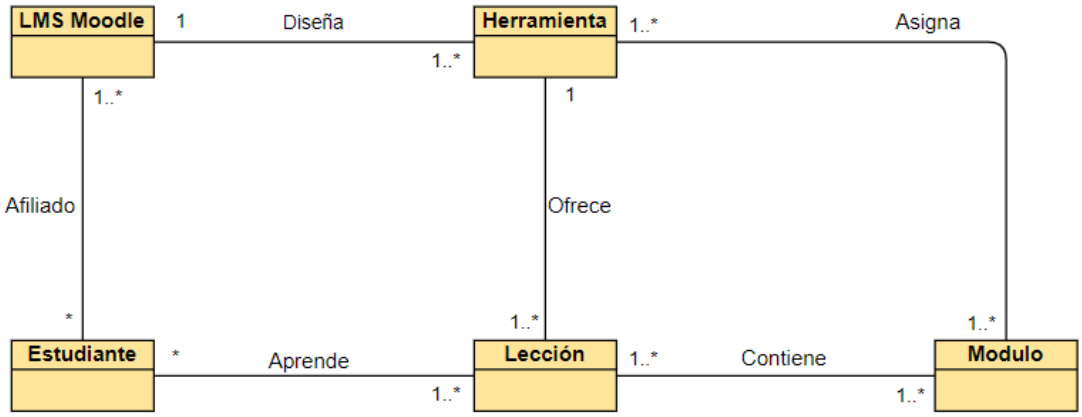


Figura 3.2 Diagrama de clases (mapa conceptual)

3.4 Diseño del Sistema

3.4.1 Diagramas de interacción

Después de que obtuvimos el modelo estático o conceptual podemos describir el modelo dinámico para identificar las propiedades y responsabilidades de los objetos y de las clases

3.4.1.1 Diagrama de secuencia

Los diagramas de secuencia son una solución de modelado dinámico popular en UML porque se centran específicamente en *líneas de vida* o en los procesos y objetos que coexisten simultáneamente, y los mensajes intercambiados entre ellos para ejecutar una función antes de que la línea de vida termine.
La base de datos utilizada en esta herramienta es la que va incluida en el paquete de LMS Moodle.
Se muestra a continuación los diagramas de secuencia para dos casos de uso

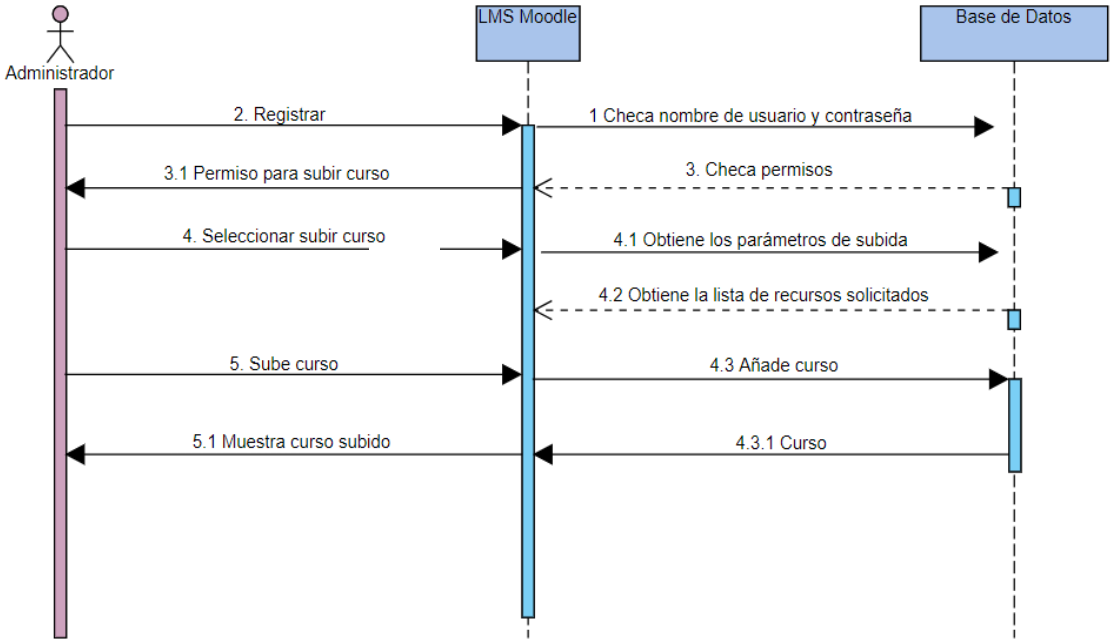


Figura 3.3 Diagrama de secuencia Crear curso

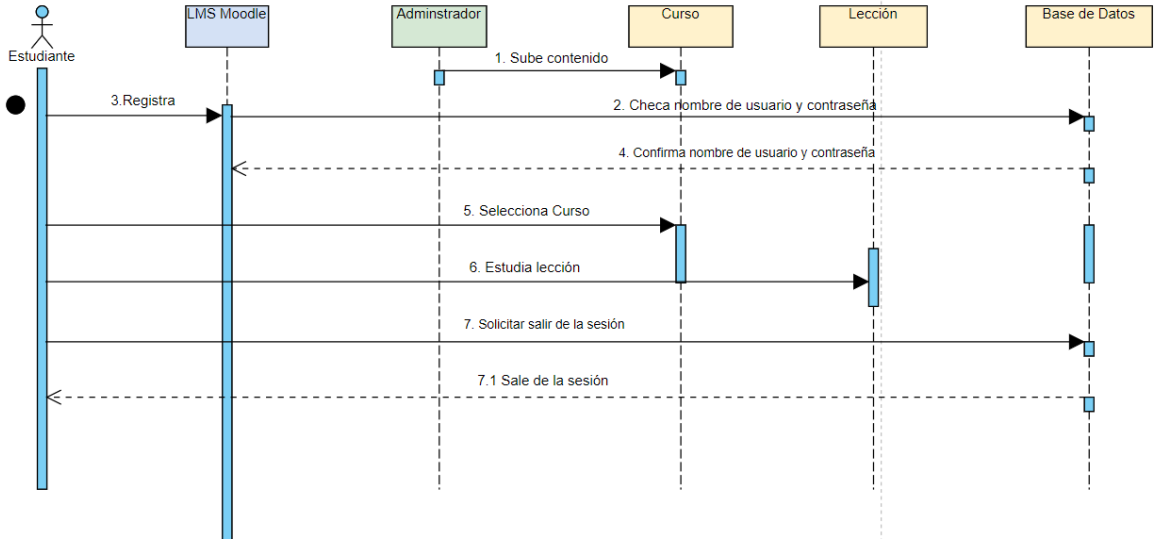


Figura 3.4. Diagrama de secuencia Estudiar curso

3.4.1.2 Diagrama de colaboración

El diagrama de colaboración muestra claramente los objetos con los que interactúa un determinado objeto
Estas colaboraciones tienen una parte estática (diagramas de clase) y una dinámica (diagramas de secuencia)
A continuación, vemos los diagramas de colaboración de la secuencia crear curso como administrador y de interactuar en la herramienta como estudiante

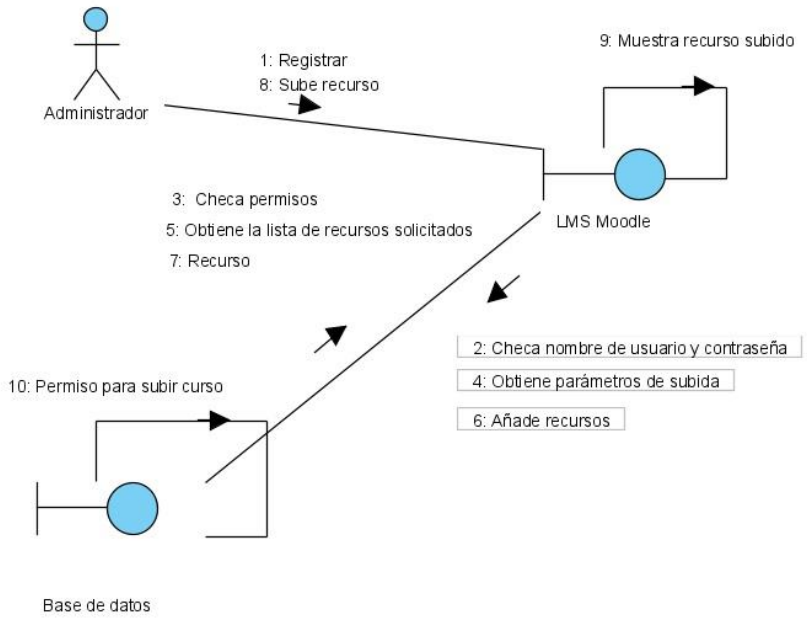


Figura 3.5. Diagrama de colaboración agregar curso

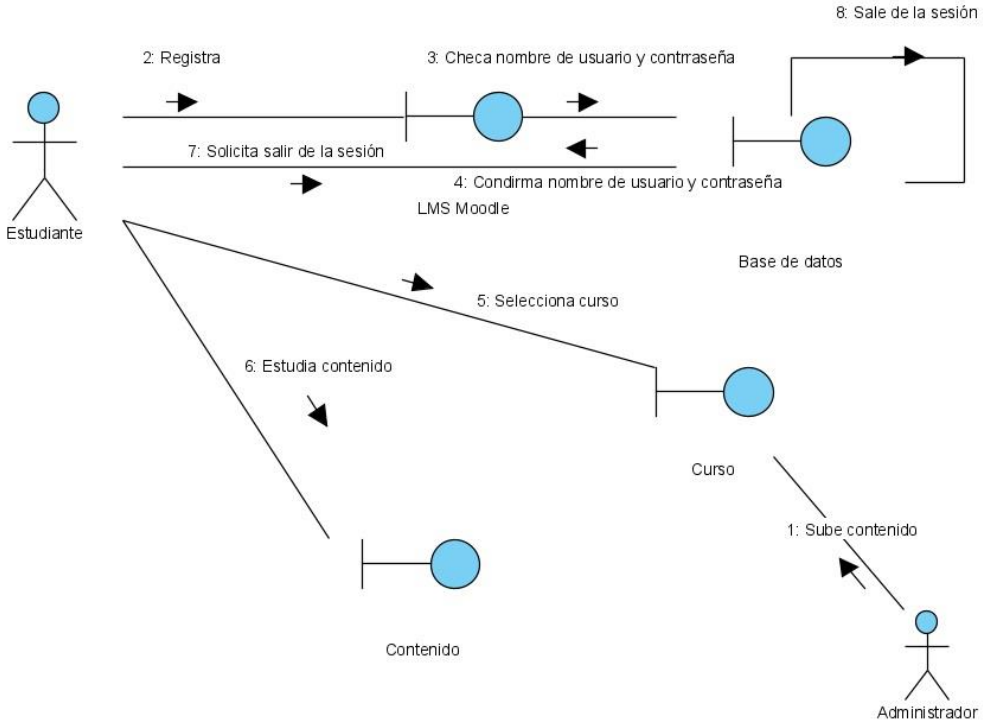


Figura 3.6. Diagrama de colaboración Estudiar curso

CAPITULO IV

Diseño

En este capítulo retomaremos todo lo analizado anteriormente en la etapa de análisis y diseño y lo llevaremos a la fase de implementación, así como realizaremos las pruebas pertinentes al mismo en la fase de diseño.

4.1 Diseño

Para el diseño de la herramienta para el entrenamiento de hacking ético utilizamos un tema preexistente descargado desde la plataforma Moodle con una interfaz amigable, la cual nos ha permitido lograr el propósito de esta tesina.

El sitio donde se descargó la plantilla fue el siguiente http://www.moodle.org y en específico el template ocupado es el llamado Moove para la versión 3.9 con la liga siguiente de descarga https://moodle.org/plugins/theme_moove

En Moodle tenemos la oportunidad de descargar temas gratuitos que nos sirven para darle una vista más personalizada y de acuerdo a lo que queremos proyectar a los estudiantes

4.1.1. Interfaz del Sistema

Ocupando como base el tema Moove mencionada al inicio de este capítulo procedimos a adaptarlo a nuestro proyecto quedando una página llamativa, simple, sencilla y botones fácilmente comprensibles al usuario final (figura 4.1). Como podemos observar es la página de inicio en la cual podemos solicitar introduzcan nombre de usuario y contraseña preasignado

Cuenta con imágenes coloridas y con mucho que ver con el tema que se maneja, así como propaganda para llamar la atención del usuario y hacer más descriptiva la página (figura 4.2)

Podemos observar cómo ampliamos a detalle los cursos y categorías existentes, así como los usuarios dados de alta (figura 4.3)

Figura 4.1 Interfaz de registro

Figura 4.2 Publicidad

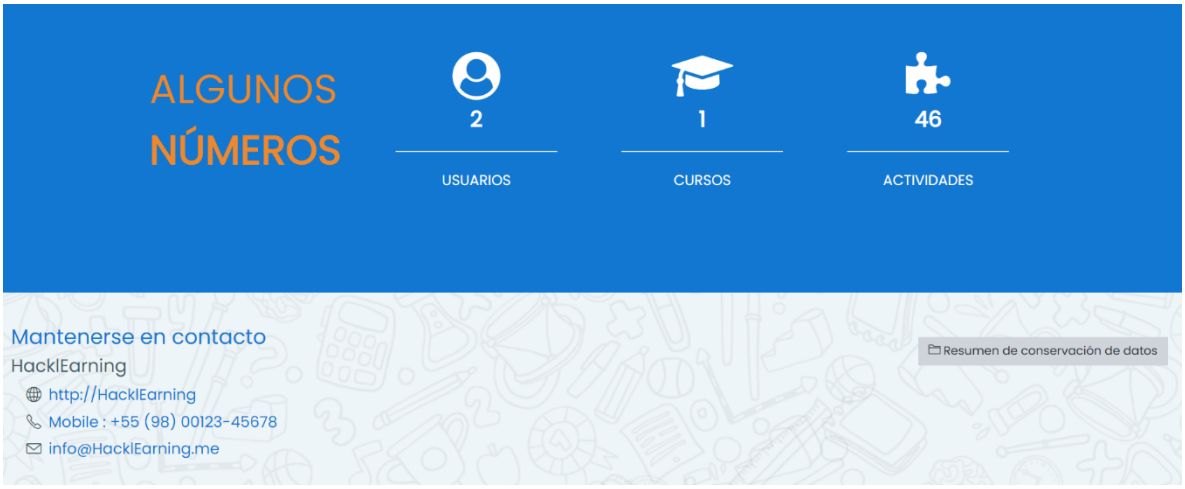


Figura 4.3 Publicidad 2

4.1.2. Interfaz del usuario

Si una persona está registrada e ingresa su usuario y contraseña de manera accederá al curso (figura 4.4)

Después podrá acceder a las lecciones del sistema y navegar en este en forma de cascada con la condición de que siempre debe terminar el curso inmediato anterior para poder abrir la opción del siguiente nivel a estudiar, esto con el fin de que toda la enseñanza sea estructurada y siga una línea correcta para poder instalar y ejecutar software, así como instrucciones y talleres de manera adecuada (figura 4.5)

Figura 4.4 Ingreso al curso

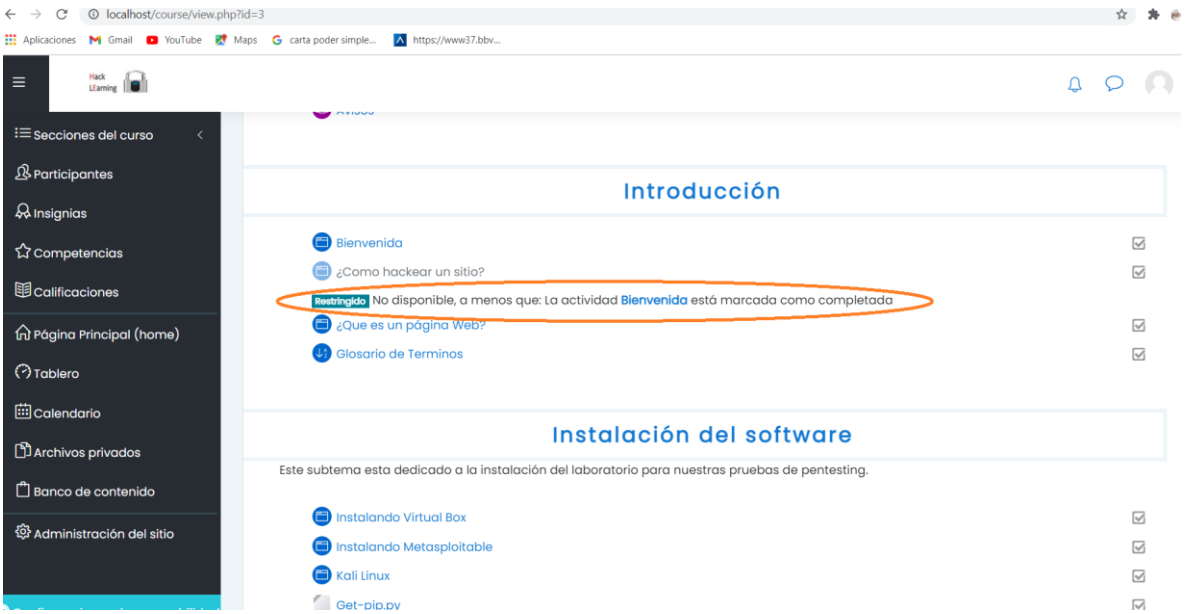


Figura 4.5. Navegando por el curso

El curso cuenta con 5 secciones con varios submódulos en cada sección de acuerdo al diagrama de navegación (figura 3.1)

Todo el curso es un conjunto de video tutoriales para llevar paso a paso al estudiante y hacerle el curso fácil de entender con descripciones detalladas de las actividades y tareas a realizar a continuación mencionamos cada sección

4.1.2.1 Instalación de Software

En este apartado analizaremos el diseño de las lecciones de instalación de software, como podemos ver en la figura 4.6 se procederá a la instalación de virtual box que es necesaria para poder correr las demás aplicaciones para ejecutar las lecciones

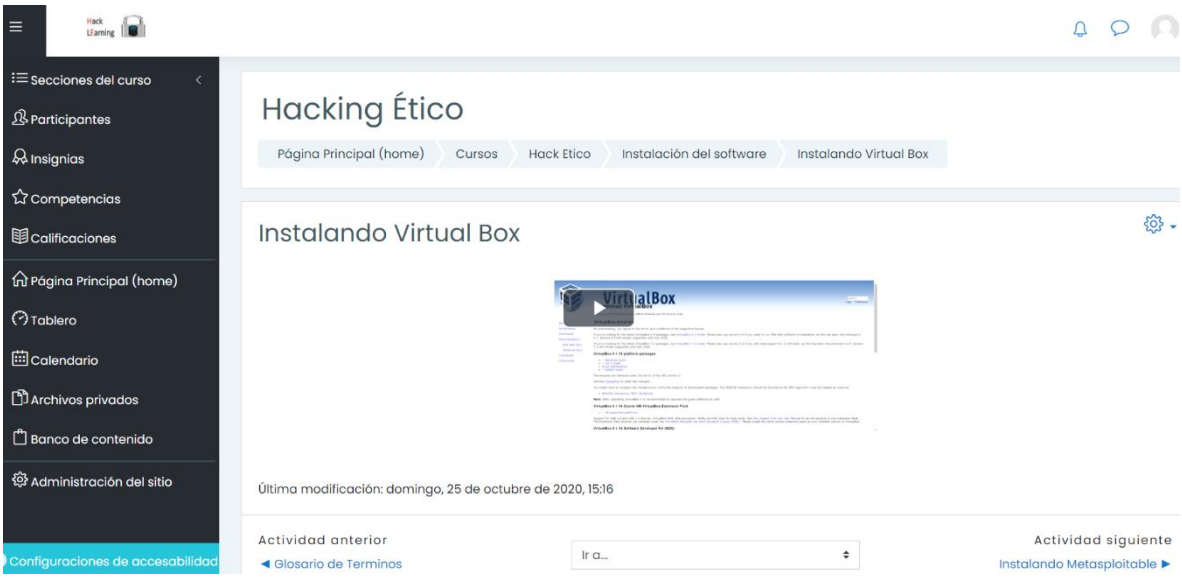


Figura 4.6. Instalando Virtual Box

En la figura 4.7.1 podemos observar una práctica para poder hacer la instalación de metasploitable por medio de la maquina virtual previamente instalada

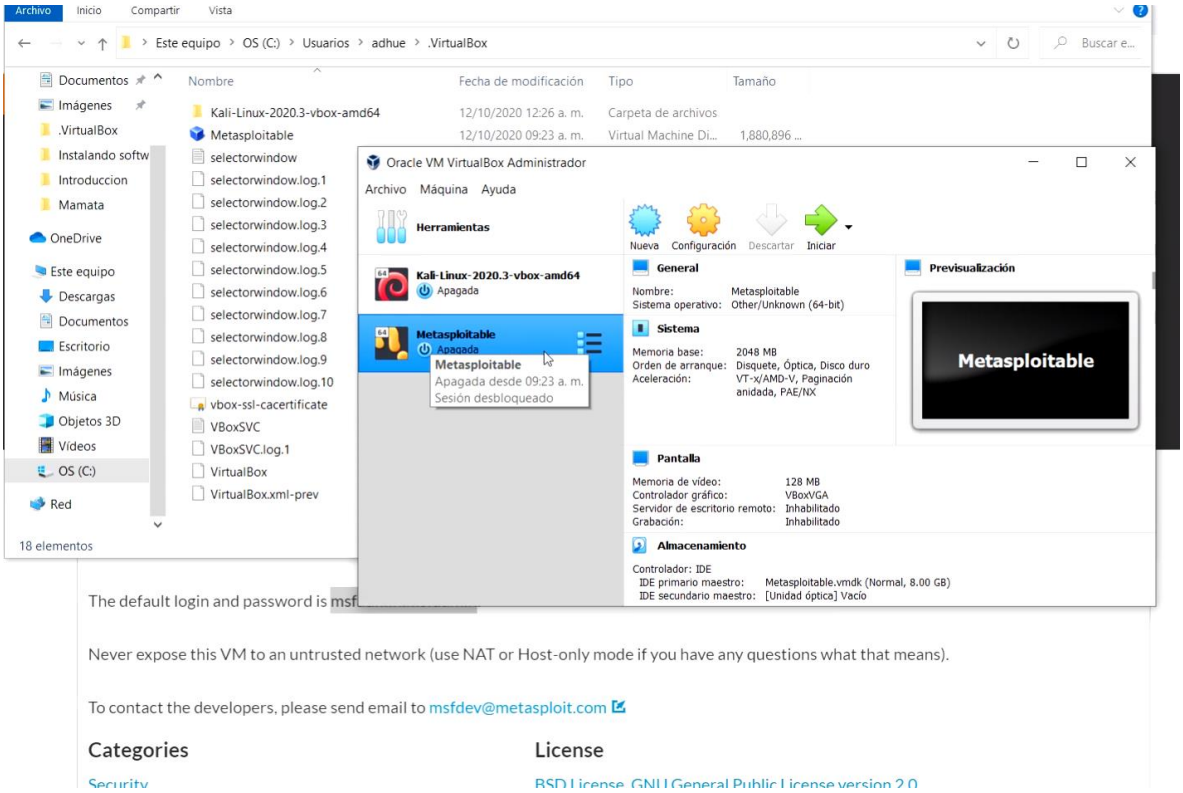


Figura 4.7.1 Instalando Metasploitable

Para poder ocupar las herramientas y aplicaciones para el pentesting necesitamos el sistema operativo KALI, en esta actividad se planea la instalación del mismo paso a paso desde la descarga a la ejecución de la aplicación (figura 4.7.2)

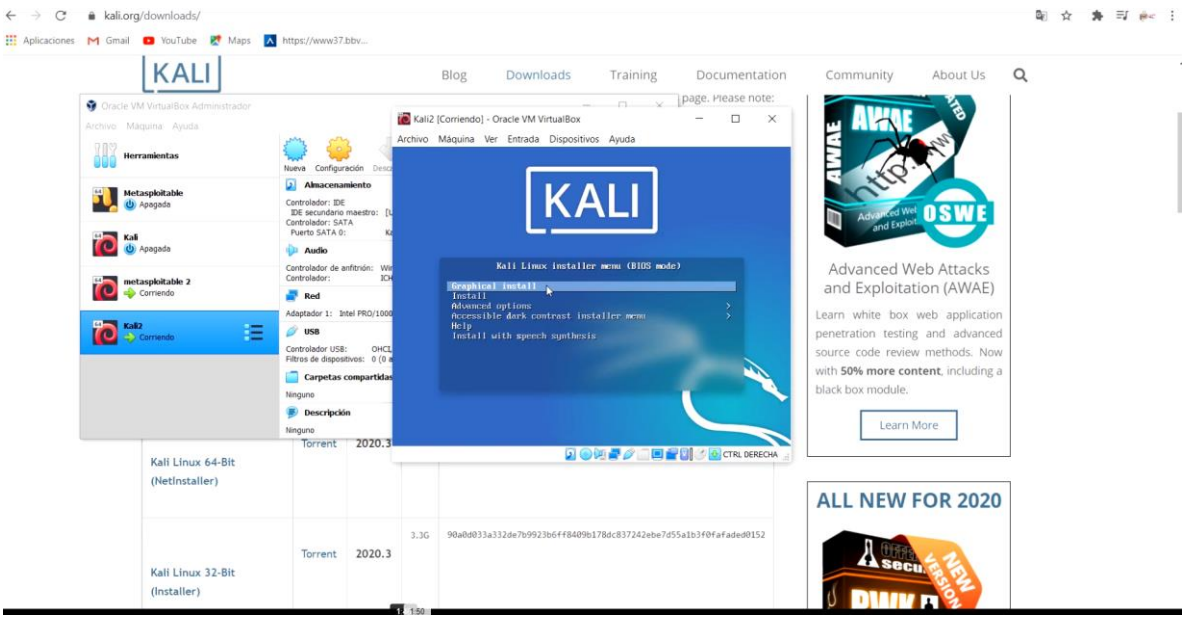


Figura 4.7.2 Instalando Kali Linux

Se debe instalar herramientas para poder ejecutar Knock el cual es importante para pentesting (figura 4.7.3)

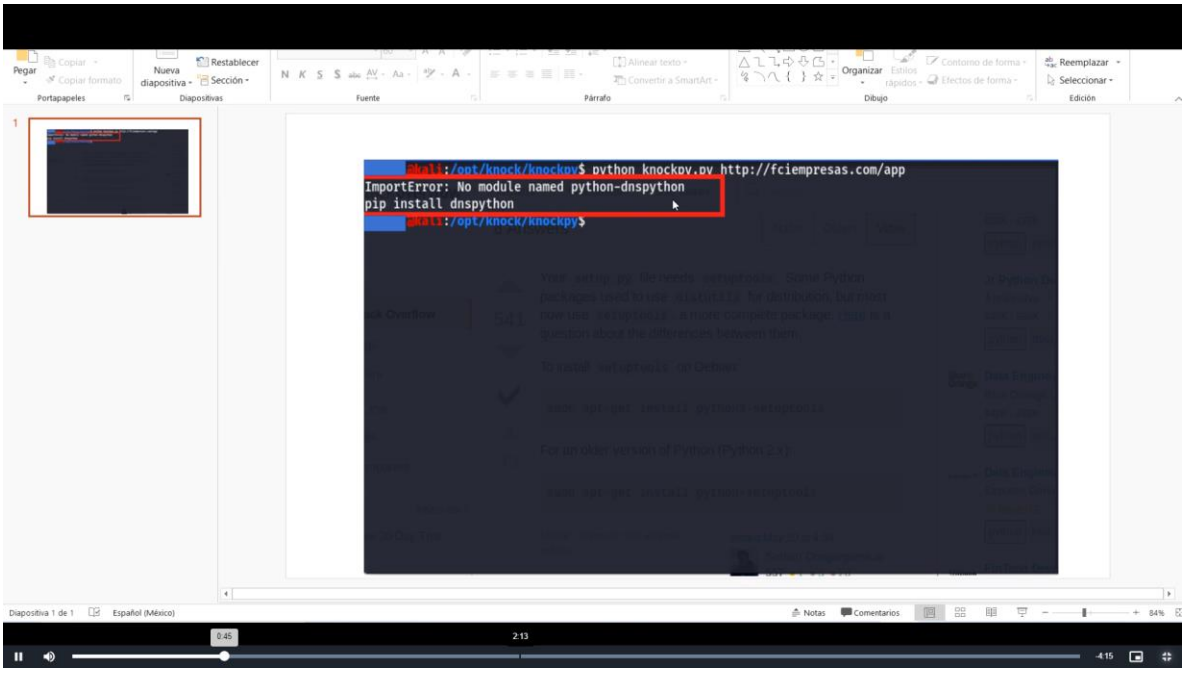


Figura 4.7.3 Instalando DNSPython

Knock es otra herramienta fundamental para poder ejecutar testeo y se implementa desde 0 para poder ocuparlo en las actividades (figura 4.7.4)
Burp suite es una herramienta incluida en KALI pero la mencionamos para que sepan como ejecutar y usar la misma (figura 4.7.5)

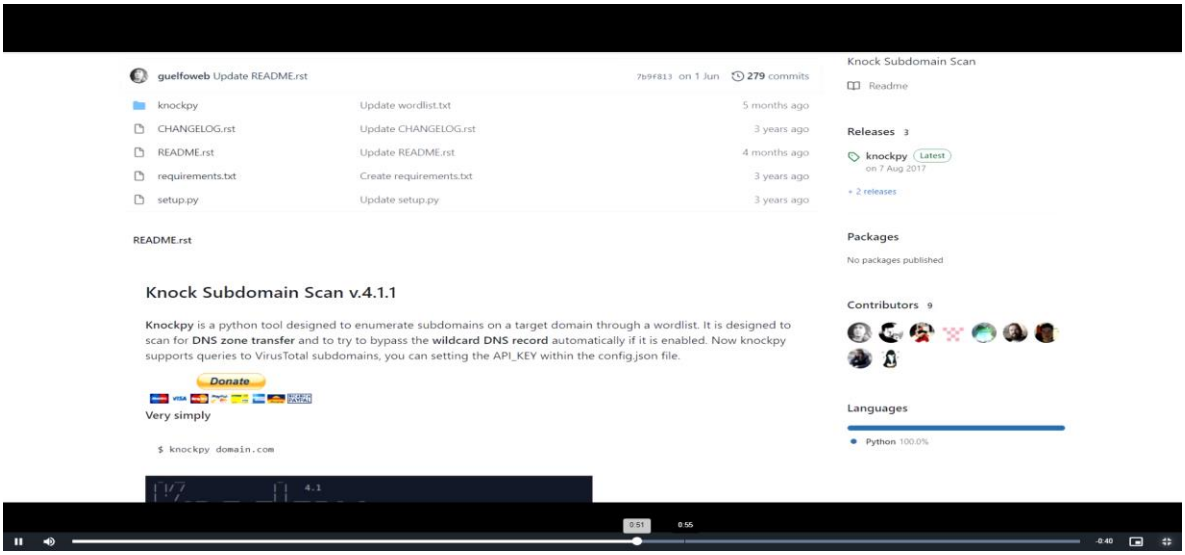


Figura 4.7.4 Instalando Knock

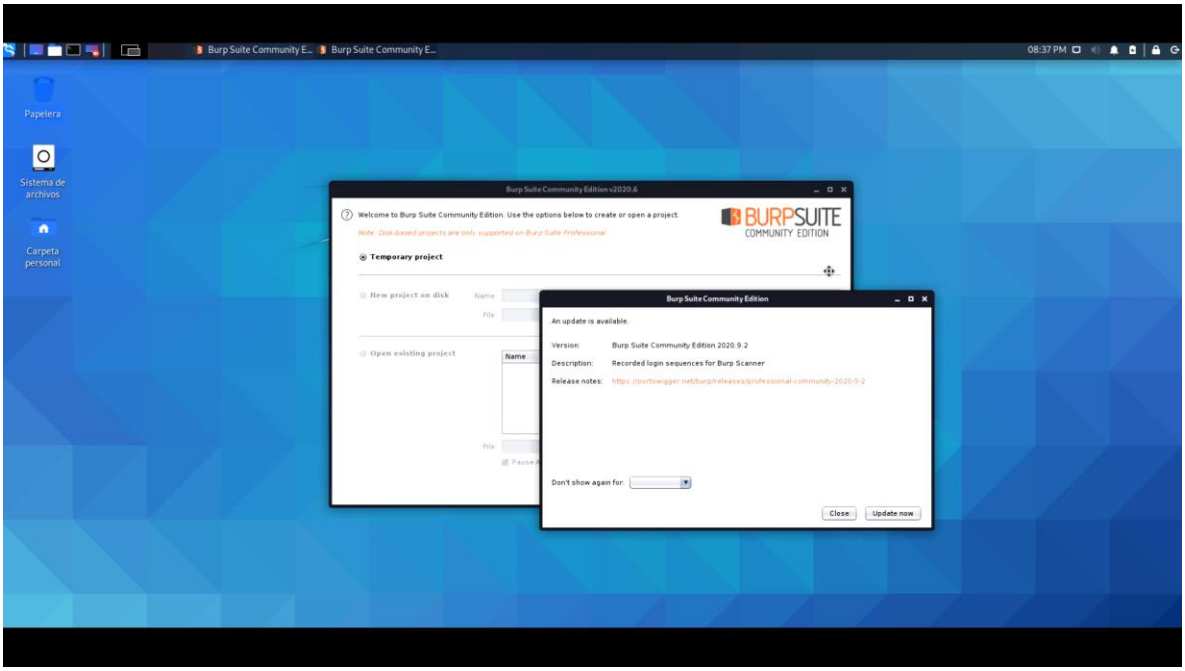


Figura 4.7.5 Instalando Burpsuite

4.1.2.2 Recabando información

Esta parte de la navegación es exclusivamente para las personas que ya terminaron de navegar en las lecciones anteriores de instalación de software y se utilizará para poder obtener información necesaria previa a realizar hacking en algún sitio, será de vital importancia para tener éxito en la penetración de la victima (figura 4.7.6 a la 4.7.9)

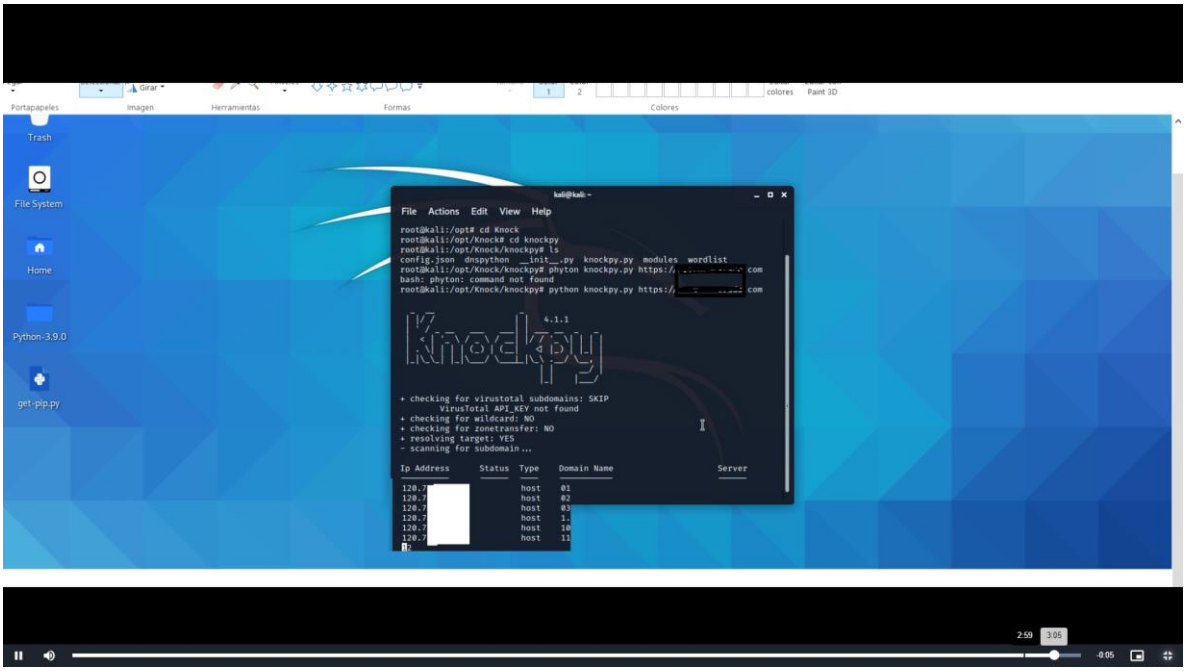


Figura 4.7.6 Conociendo subdominios

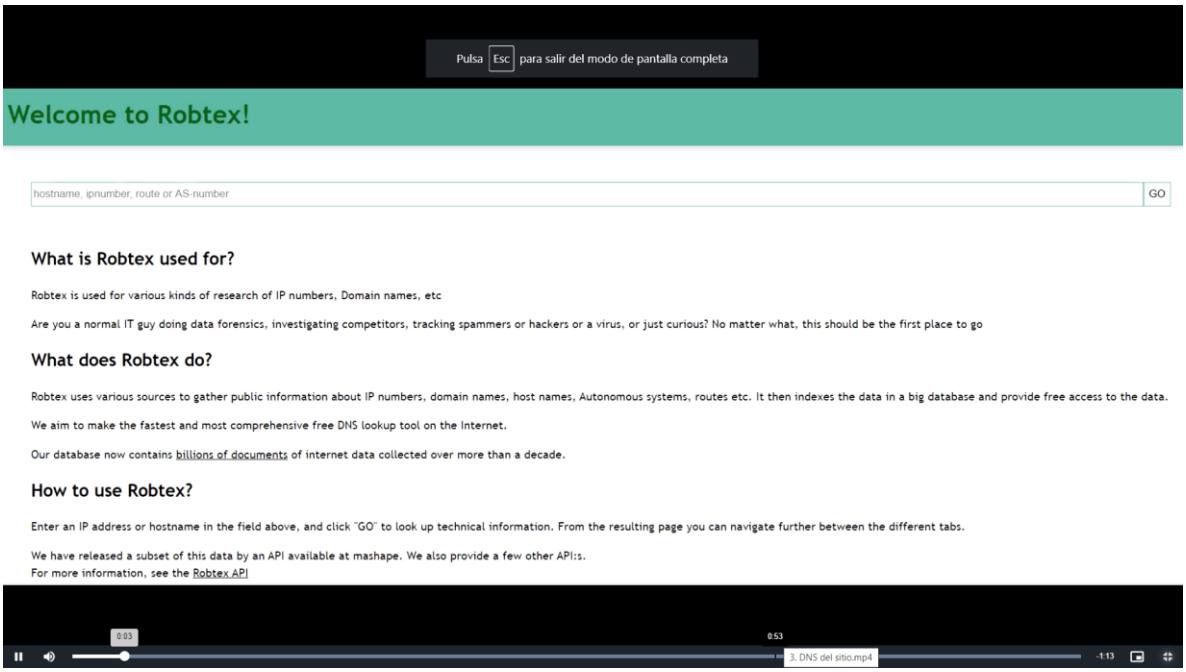


Figura 4.7.7 Conociendo DNS

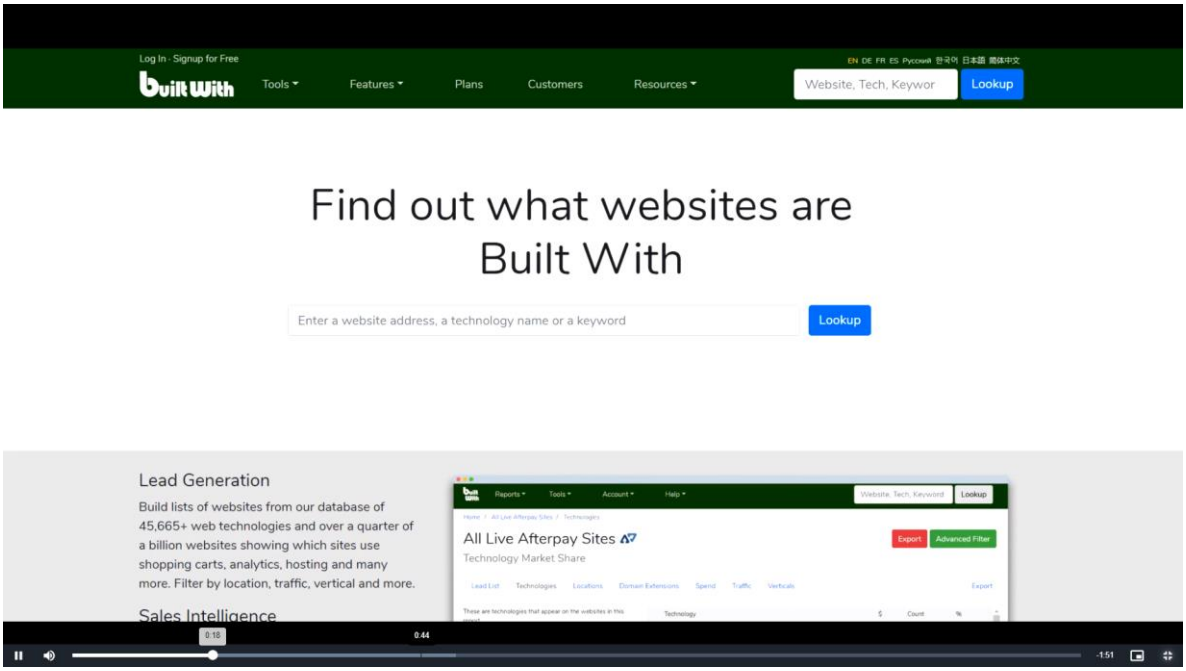


Figura 4.7.8 Conociendo Tecnologías de un sitio Web

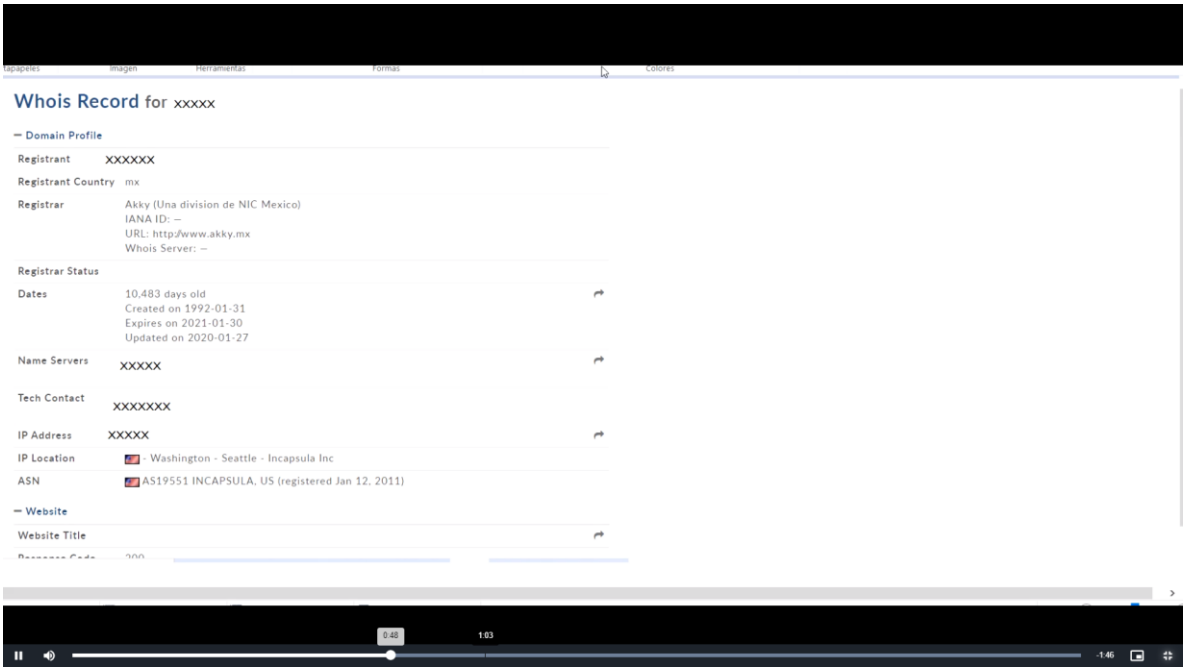


Figura 4.7.9 Descubriendo direccion ip de un sitio Web

4.1.2.3 Vulnerabilidad al subir archivos

En esta parte del curso las lecciones serán dirigidas a identificar si el sitio cuenta con vulnerabilidades a la carga de archivos, están divididas en 6 lecciones(figura 4.8)

Figura 4.8 Vulnerabilidad al subir archivos

Un proxy es de suma importancia para poder conseguir la primera información que el usario envia al servidor, captarla y modificarla a nuestra conveniencia, de este modo podemos acceder a un sitio y podemos jugar con todas las opciones(figura 4.8.1)

Se puede generar backdoors para poder acceder a los sitios, por medio de los proxy también podemos acceder a esto(figura 4.8.2)

El proxy nos servirá y será de vital importancia pues con el mismo nos apoyamos para hacer una lección de una seguridad mucho mas alta (figura 4.8.3)

Podemos realizar ciertas prevenciones al sitio las cuales se muestran en la lección de prevención (figura (4.8.4)

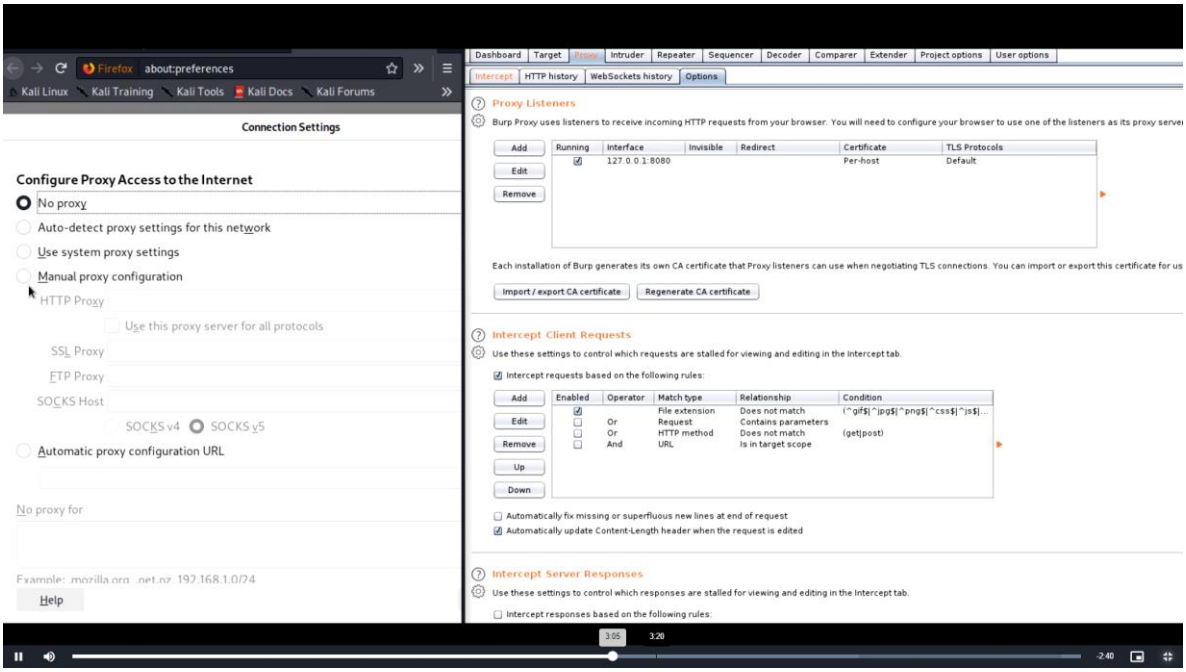


Figura 4.8.1 BurpSuite Proxy

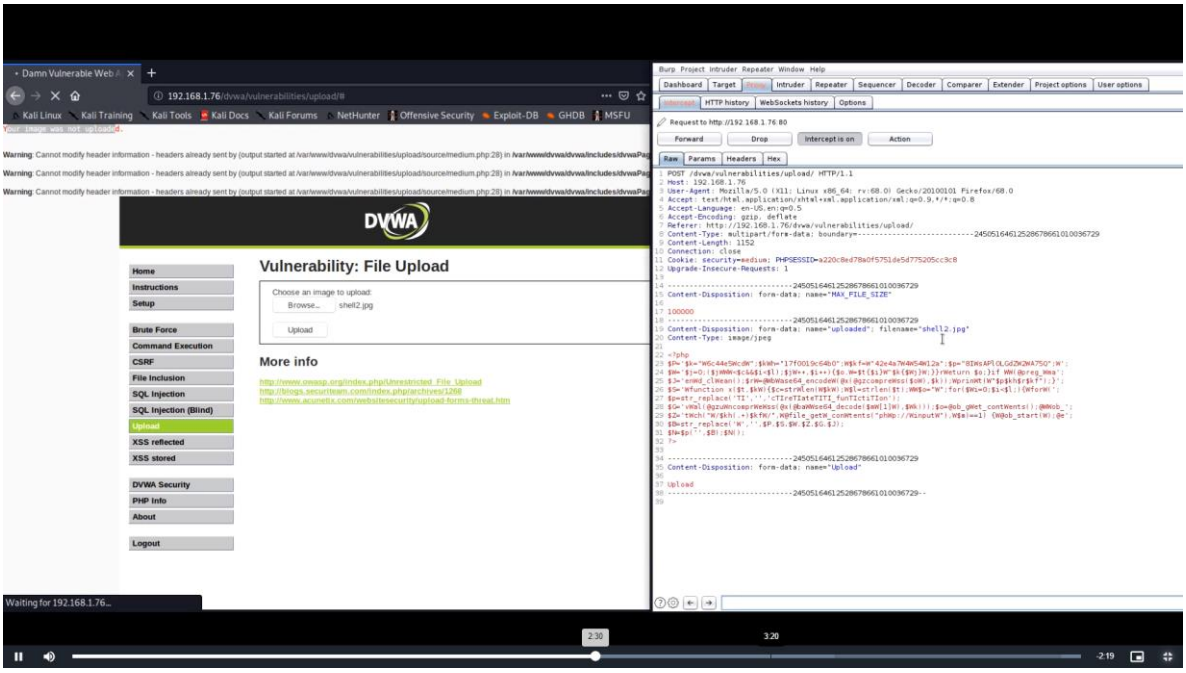


Figura 4.8.2 Backdoor seguridad media

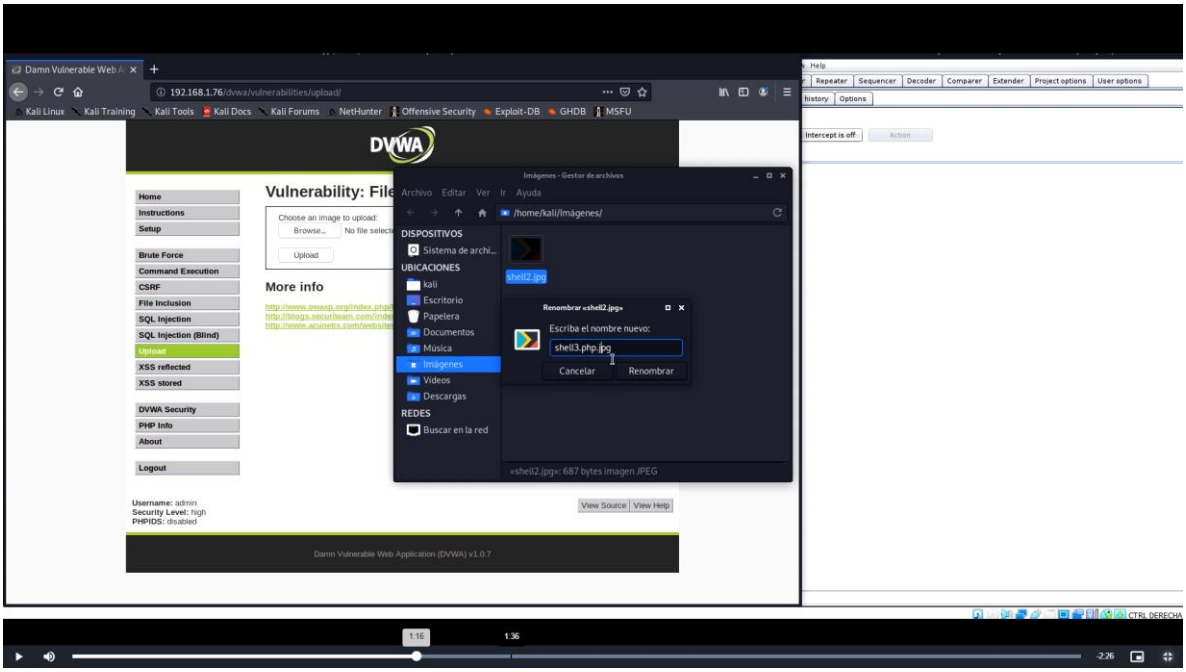


Figura 4.8.3 Backdoor seguridad alta

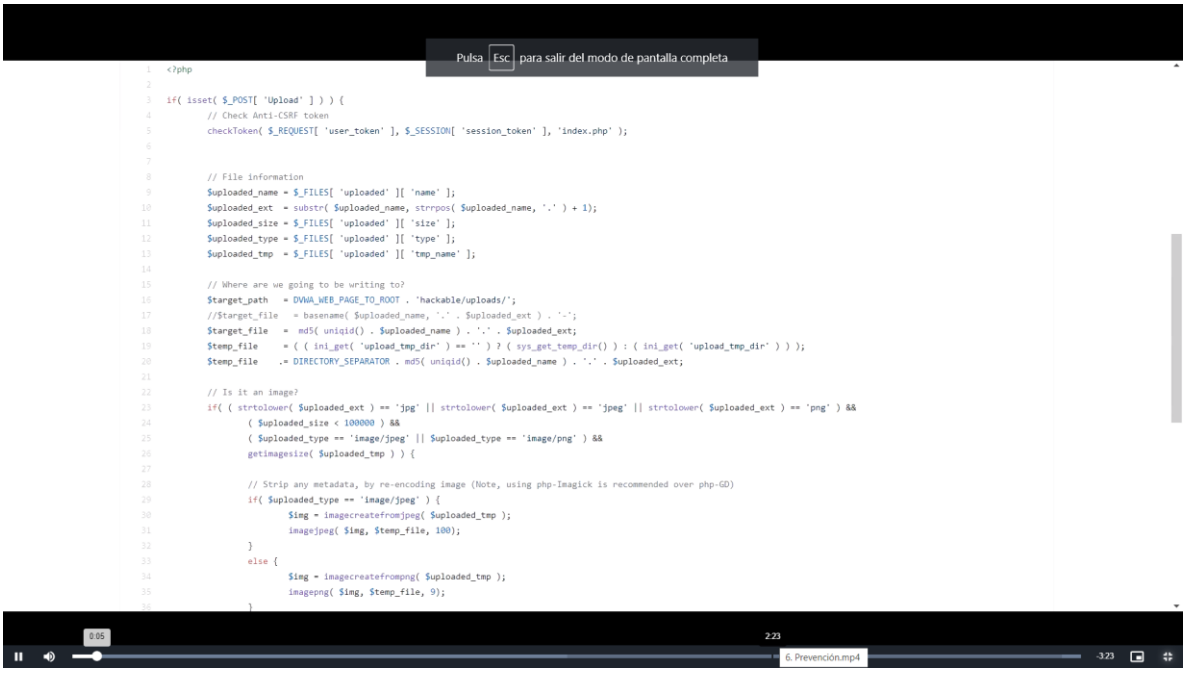


Figura 4.8.4 Prevención carga de archivos

4.1.2.4 Vulnerabilidad por ejecución de código

Para estas lecciones nos apoyaremos en la pagina DVWA que contiene metasploitable la cual esta hecha para que libremente se pueda practicar en la misma las vulnerabilidades mas comúnmente encontradas creando puertas traseras a nivel bajo (Figura 4.9) nivel medio (Figura 4.9.1) y asi mismo poder dar opciones para prevenirse sobre este tipo de ataques en ejecución de código (figura 4.9.2)

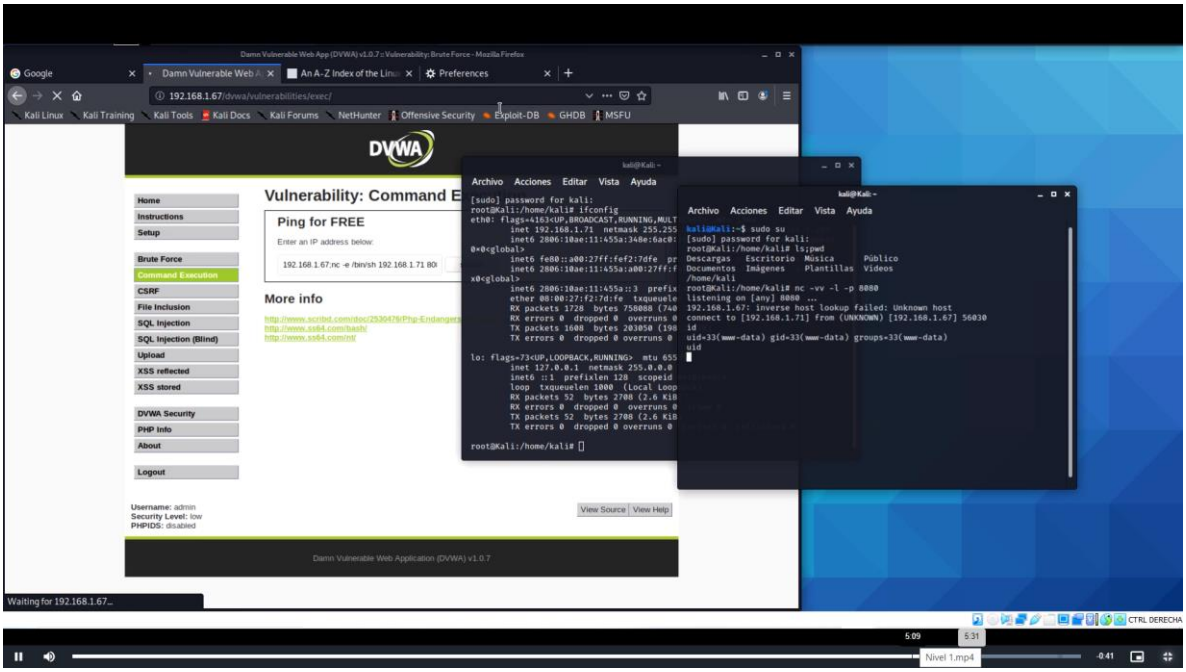


Figura 4.9 Backdoor nivel bajo

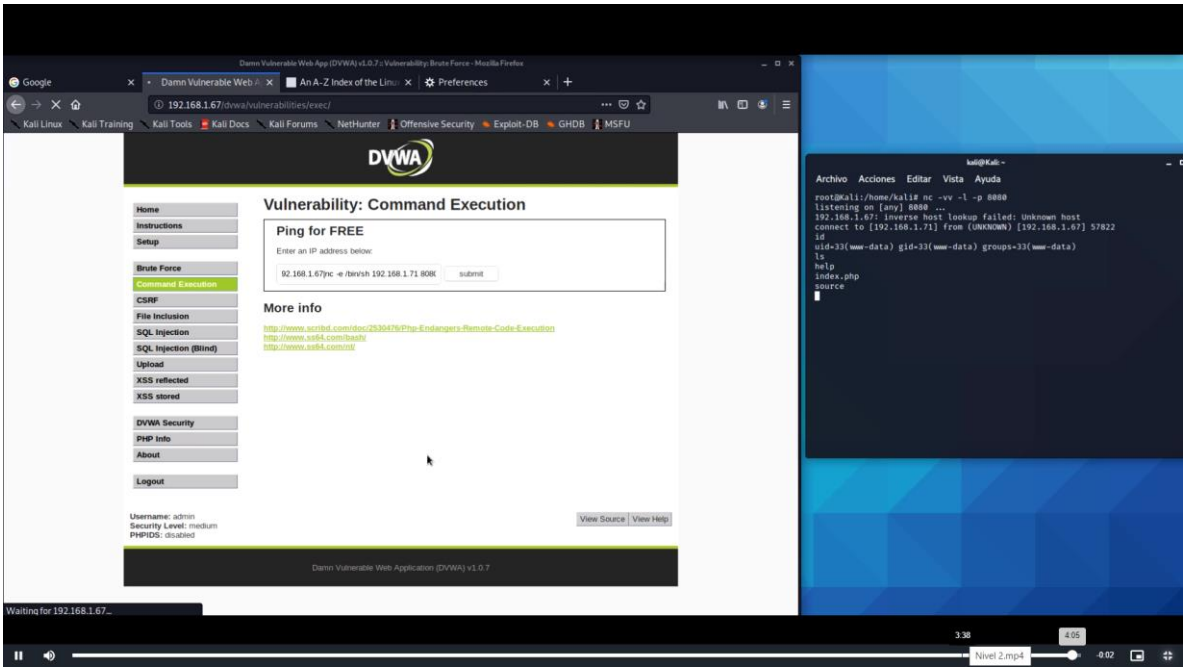
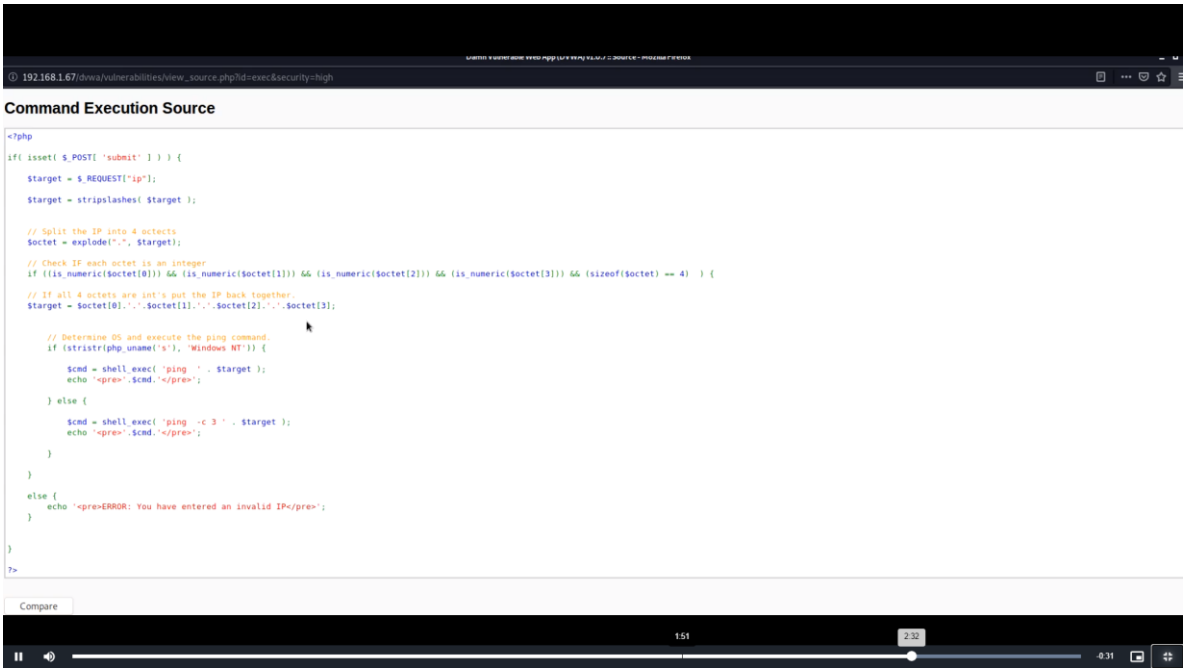


Figura 4.9.1 Backdoor nivel medio



4.9.2 Prevención seguridad ejecución de código

4.1.2.4 Vulnerabilidad iSQL

En esta ultima parte del curso se divide en 6 lecciones (Figura 4.10) para esto se debe modificar un archivo OWASP10 para poder accesar a la información y poder correr de manera correcta las aplicaciones (Figura 4.10.1)
Para estas lecciones lo primero que debemos identificar es si el sitio esta programado en SQL y se revisara en la lección 3 (Figura 4.10.2)
Multillidae es un sitio vulnerable que es parte de metasploitable en el cual nos apoyaremos para poder hacer pentesting con inyecciones sql (Figura 4.10.3)
En este caso en una seguridad mas alta es mas recomendable ocupar proxys para poder interceptar la información (Figura 4.10.4), del mismo modo que en las lecciones anteriores se incluye una para poder prevenir este tipo de ataques (Figura 4.10.5)

Figura 4.10 Vulnerabilidad iSQL

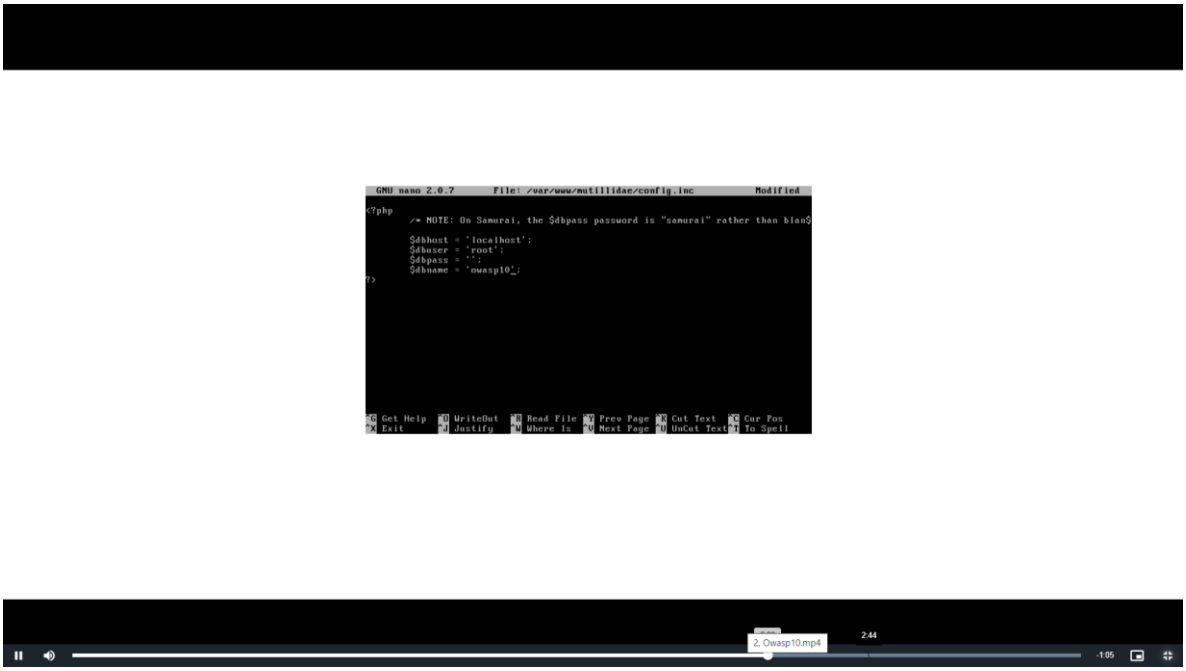


Figura 4.10.1 OWASP10

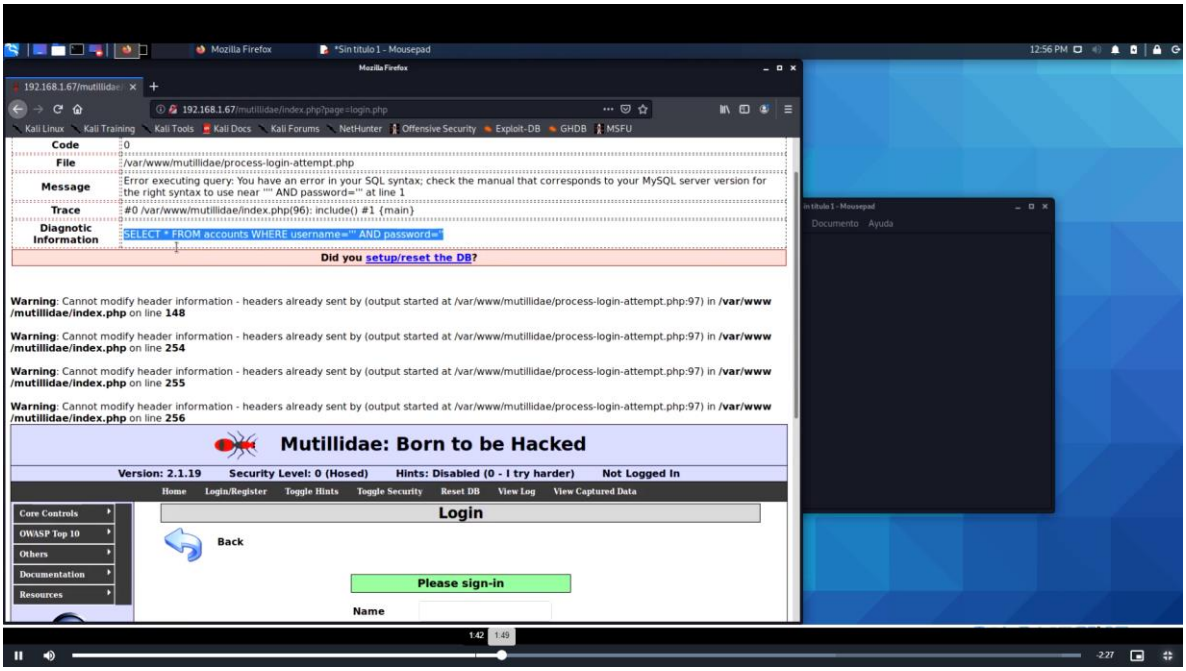


Figura 4.10.2 Comprobando iSQL en sitios web

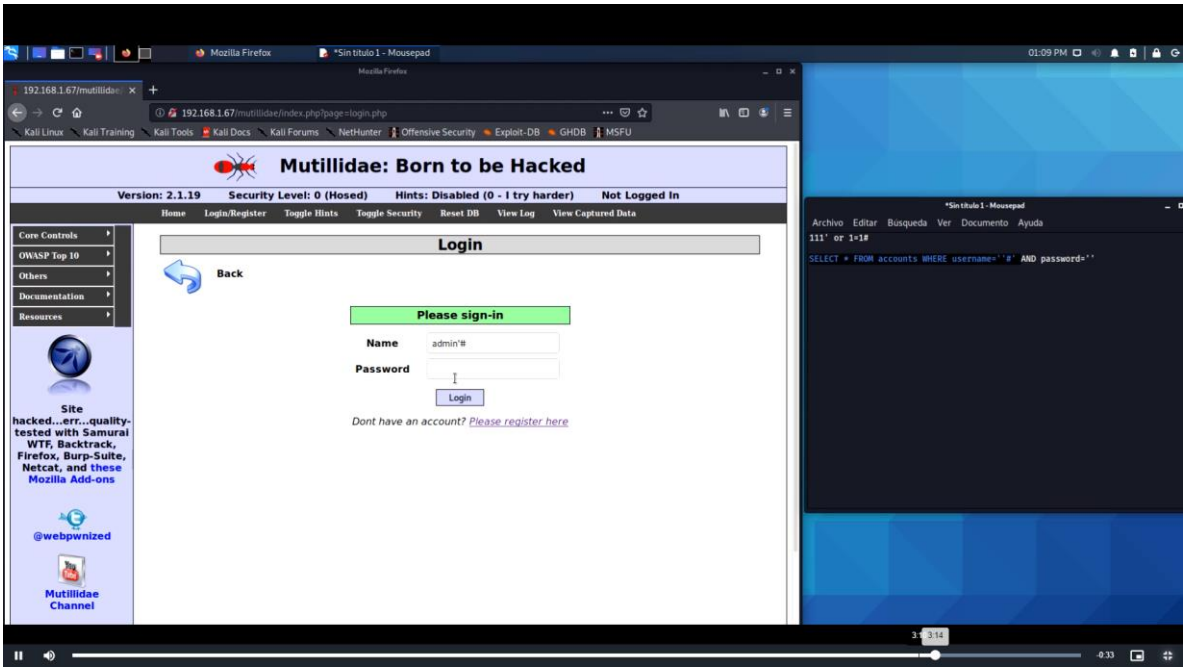


Figura 4.10.3 Entrando como admin

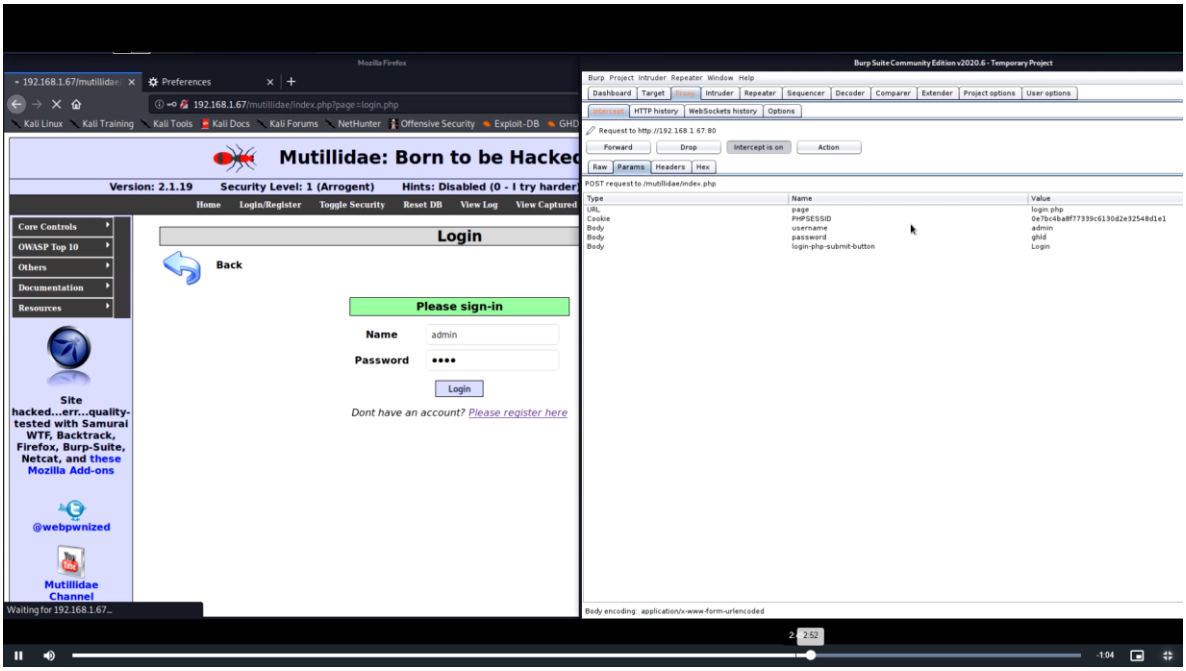


Figura 4.10.4 iSQL seguridad alta

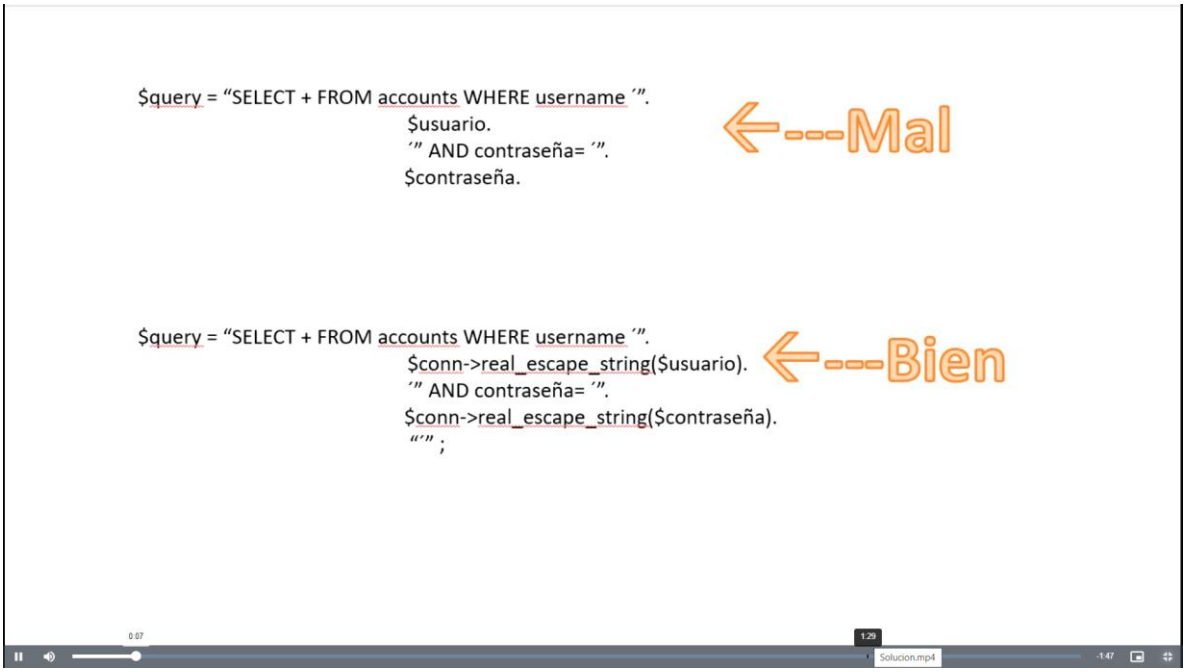


Figura 4.10.5 iSQL Prevención

4.1.2.5 Glosario

Como se apreciar en la siguiente figura, también cuenta con un amplio glosario de casi 100 definiciones (figura 4.12) que lleva de la mano al usuario final.

Figura 4.12 Glosario

Capítulo V

Pruebas

5.1 Elaboración del plan de Pruebas

El lugar donde podemos observar las actividades de los futuros usuarios del sistema que vamos a desarrollar puede ser una escuela, un lugar donde se imparten cursos, desde casa o desde cualquier lugar en donde se tenga internet y la persona requiera aprender sobre hacking ético.

5.2 Definición y justificación de las pruebas que se harán en el sistema

Las pruebas que vamos a ocupar son heurísticas de usabilidad basado en las heurísticas proporcionadas por Jakob Nielsen (Nielsen, 2020), dicho método consiste en comparar un conjunto predefinido de principios de usabilidad de una aplicación (en este caso una plataforma en la web) al intentar completar ciertas tareas del sistema ya que
principalmente el proyecto a diseñado se refiere específicamente a un sistema que sea fácil de entender, que sea llamativo, amigable y que tenga una interfaz muy comprensible para poder utilizar la herramienta de aprendizaje de hacking ético de manera adecuada, ya que existen en la red varios sistemas para este fin pero sin mucha facilidad de comprensión, además de que el diseño de las páginas no tienen buena estructura y no son para cualquier persona, sino requiere conocimientos avanzados para su funcionamiento.

Además, todas las páginas existentes están en idioma inglés, haciendo aún más difícil la comprensión, con lo cual se pretende tener una interfaz demasiado amigable para lograr este fin.

5.3 Instrumentos utilizados para validar las pruebas de usuario

Ya que una evaluación Heurística es un método de inspección de la usabilidad sin usuarios, yo considero que esta prueba es la mejor manera de evaluar mi proyecto debido al alcance y al uso final del mismo, una herramienta de entrenamiento para hacking ético requiere 100% de un sistema que sea comprensible, estructurado y usable.

Se examinará la calidad de uso de una interfaz, a partir del cumplimiento de unos principios reconocidos de usabilidad: los heurísticos

5.4 Plan de pruebas

Realizaremos la evaluación heurística de la usabilidad. A continuación, presento las 14 preguntas que he considerado para evaluar principios genéricos de navegación y claridad arquitectónica.

1. ¿Presentan todas las páginas un título identificativo?
2. ¿El enlace a la página principal (home Page) se identifica claramente?
3. ¿Los apartados más importantes del sitio son accesibles desde la página principal?
4. ¿Evita el sitio el paso forzoso por una página de bienvenida siempre que se visita?
5. ¿La tarea que se está llevando a cabo en cada momento se identifica claramente?
6. ¿Aparece la imagen del sitio en todas las páginas?
7. ¿Es clara la ruta a seguir del curso?
8. ¿El sistema responde con mensajes claros si se comete un error p/e en el login?
9. ¿A simple vista es llamativa la herramienta?
10. ¿El sitio cumple con la expectativa del estudiante?
11. ¿El diseño y la disposición de los contenidos es concisa y clara (se ha evitado la sobrecarga informativa)?
12. ¿La organización de la página se consigue con títulos, listas y una estructura constante?
13. ¿Todos los enlaces pueden reconocerse fácilmente e indican claramente su estado?
14. ¿Las herramientas más necesarias están siempre visibles?

Con el fin de lograr un análisis heurístico completo y con parámetros uniformes cada una de estas variables se apuntará en una plantilla en la que se asignará una de estas tres opciones: «sí, siempre», «no, nunca» o «a veces».
Responder «sí, siempre» supondrá presencia de usabilidad en el sistema y responder «no, nunca» supondrá ausencia de usabilidad (figura 1)

Pregunta	***Si, siempre***	***No, nunca***	***A veces***

1	***X***		
2			***X***
3		***X***	
.....			

Figura 5.1 Usabilidad

5.5 Eficiencia

Por medio de la observación directa basada en pruebas con usuarios, se podrá determinar si los usuarios conseguirán completar las tareas encomendadas para verificar si el sistema está cumpliendo con el objetivo en concreto, se considerará que el sistema resulte
efectivo si se consigue localizar la información terminológica solicitada en las tareas.

5.6 Eficacia

La eficacia se evaluará a través del siguiente cuestionario de respuestas cerradas («sí», «no» y «a veces»):
1. ¿Ha costado mucho tiempo dar con la respuesta o la has encontrado rápidamente?
2. ¿Te parece eficaz la búsqueda?
3. ¿Te ha parecido fácil de usar la página de inicio?
4. ¿Has realizado la búsqueda con rapidez y agilidad?

5.7 Satisfacción

El grado de satisfacción del usuario se evaluará mediante una entrevista cuyas repuestas se habían categorizado como
«sí», «no» y «a veces».
1. ¿Te ha parecido fácil de usar la aplicación?
2. ¿Te ha resultado fácil interpretar los iconos, los textos de los menús y la estructura de las páginas?
3. ¿Resulta fácil la búsqueda en este sitio web?

5.8 Resultados:

Una vez que se concluyó la fase de desarrollo de una primera versión de la herramienta de hacking ético, se procedió a poner la plataforma en un modo de prueba dominio local de manera controlada por ciertos usuarios para sus correspondientes pruebas y medición de rendimiento en un ambiente controlado.
Para efectos de estudio probamos la aplicación con algunos estudiantes y no estudiantes de computación.

Para la evaluación de la herramienta de hacking ético se utilizaron heurísticas que se centra en las funcionalidades básicas: iniciar sesión, curso, modulo, lección.
El objetivo de esta evaluación fue identificar los principales defectos de usabilidad en la interfaz a través de la aplicación de estas heurísticas:

1. Visibilidad del estado del sistema
2. Lógica de la información.
3. Control y libertad para el usuario
4. Prevenir errores
5. Reconocimiento
6. Flexibilidad y eficiencia
7. Estética y diseño
8. Recuperación de errores

Con respecto a las preguntas realizadas después de revisar el sistema encontramos lo siguiente:

- Problemas de diseño.

    - Links a primera vista difíciles de encontrar.

    - Diseño

    - Recuperación de contraseña no funcional

Los resultados y opiniones obtenidas fueron buenas y del gusto de los usuarios en general, sin embargo, aún existen detalles a corregir (detalles estéticos).
Posteriormente se pidió retroalimentación de los usuarios, donde expusieron dudas, sugerencias, pensamientos e ideas que tuvieron durante y después de la

prueba de usabilidad.

5.9 Resumen

La herramienta hacking ético obtuvo calificaciones aceptables, tanto en el estudio heurístico como el de usabilidad. Aunque hubo comentarios y opiniones diversas, en general se cree que la plataforma tiene un gran potencial. Es cierto que existen algunos errores que se señalaron, sin embargo, casi todos los problemas residen en la parte de diseño y son cambios que en su mayoría se pueden realizar sin mayor problema.

Conclusiones

En el pasado, escuelas y academias tradicionales dominaban todo el medio de aprendizaje. Con la llegada de internet, comenzaron a destacar modelos de enseñanza y aprendizaje online como el e-learning, y más recientemente, el blended education, que combina un enfoque de la educación en línea y la metodología tradicional del aula, después de la pandemia además pudimos ser testigos que la educación en línea cobro mucha fuerza como no se veía antes.

Así como el mundo digital cambió nuestro acercamiento con, por ejemplo, servicios, (UBER; Spotify; Netflix; el e-commerce) nosotros también como seres humanos, ajustamos nuestras prioridades a la nueva economía; hoy además de un buen ingreso, buscamos tener más tiempo libre, autonomía y un crecimiento constante.

Las siguientes razones son en demasía importantes para saber que una herramienta como la desarrollada podría tener éxito:

1. Es rápido y sencillo

Un curso corto es una excelente manera de estudiar y adquirir nuevas habilidades. Es rápido, fácil y accesible en la mayoría de los casos. Además, se puede hacer a tiempo parcial sin ningún inconveniente y tiene una de esas grandes ventajas que describimos unas líneas arriba, se puede cursar a distancia.

2. Estudia a tu tiempo en el lugar que requieras

Una de las mejores cosas de estudiar cursos es que puedes inscribirte en cualquier momento del año y completarlo a tu ritmo. Puedes estudiar, si así lo decides, desde tu casa o bien desde cualquier otro lugar que te plazca. Éstos se adaptan a ti y no al revés.

3. Aprovecha tu tiempo

Estudiar un curso relativamente corto nos permitirá conseguir en breve un nuevo conocimiento y a la par, ahorrar tiempo.

4. El curso es gratuito.

5. El conocimiento impartido no es común

   El curso que se desarrolla en la herramienta es accesible no para cualquiera pues no todos tienen conocimiento de este tema por lo cual las pocas personas que se preparan en él pueden obtener más ingresos pues hay poca competencia en ese sentido. De las cosas increíbles que tienen los cursos es que son vanguardistas, adelantados, que enseñan cosas que las escuelas tradicionales no contemplan. Por ello, estas nuevas habilidades tienen demanda en el mercado, y por consecuencia, son bien pagadas.

6. Mantente actualizado
   También puede ser que estés en la cúspide de tu carrera profesional y en una posición de liderazgo, para mantenerte allí, deberás continuar con tu constante preparación, actualizándote en tendencias e innovación tecnológica. Aquí es donde nuevamente un modelo corto y rápido de aprendizaje será tu pasaporte…

Todas estas razones nos hacen concluir que la herramienta es por demás una excelente idea para mejorar e incrementar el interés a que las personas se preparen en esta área que requiere inmediata atención.

GLOSARIO

Hacker

Experto de las tecnologías de comunicación e información que utiliza sus conocimientos técnicos en computación y programación para superar un problema, normalmente asociado a la seguridad.

Hacker ético

Que utiliza sus conocimientos de informática y seguridad para encontrar vulnerabilidades o fallas de seguridad en el sistema, con el objetivo de reportarlas en la organización para que se tomen todas las medidas necesarias que posibilite prevenir una catástrofe cibernética

Cracker

Se utiliza para referirse a las personas que rompen o vulneran algún sistema de seguridad

Seguridad Informática

Disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático

Pentesting

Consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos. Todas las empresas se enfrentan a riesgos, cada vez más frecuentes, que pueden afectar a su sistema

Bibliografía.

Armenta, M. H. (septiembre de 2019). *Forbes México.* Recuperado el 08 de febrero de 2020, de En América Latina se registran 45 ataques cibernéticos por segundo: https://www.forbes.com.mx/en-america-latina-se-registran-45-ataques-ciberneticos-por-segundo/

Condusef. (septiembre de 2019). *Condusef.* Recuperado el 09 de diciembre de febrero de 2020, de https://www.condusef.gob.mx/gbmx/?p=estadisticas

Kaspersky. (enero de 2020). *Kaspersky.* Recuperado el 09 de febrero de 2020, de https://latam.kaspersky.com/about/press-releases/2019_kaspersky-ofrece-pronostico-de-ciberseguridad-2020-para-america-latina

Onofre, J. S. (06 de junio de 2017). *El economista.* Recuperado el 08 de febrero de 2020, de México, el segundo país más ciber atacado de AL: Symantec: https://www.eleconomista.com.mx/tecnologia/Mexico-el-segundo-pais-mas-ciberatacado-de-AL-Symantec-20170606-0023.html

Soriano, A. G. (07 de junio de 2012). *Seguridad Cultura de Prevención para ti.* Recuperado el 08 de febrero de 2020, de https://revista.seguridad.unam.mx/print/2120

Beta, G. D. (2020). *Guia digitla Beta.* Obtenido de http://www.guiadigital.gob.cl/articulo/que-es-la-usabilidad.html

CLUF, M. (1995). Paint. Estados Unidos.

Cortés, M. (24 de julio de 2020). Obtenido de Cio.com.mx: http://cio.com.mx/dell-emc-powerflex-nueva-apuesta-de-almacenamiento/

Daltabuit, E. e. (2007). *Seguridad de la información.* Noriega, Mexico: Limusa.

ElevenPaths. (s.f.). *Blogthinkbig.* Obtenido de Algunos ejemplos y defensas contra el clickjacking: https://empresas.blogthinkbig.com/algunos-ejemplos-y-defensas-contra-e/

GmBH, M. t. (2017). *Maltego*. Recuperado el 12 de Febrero de 2020, de https://www.maltego.com/

Hacksplaning. (2020). *Hacksplaining*. Recuperado el 12 de Febrero de 2020, de www.hacksplaining.com/

Harris, S. e. (2005). *Hacking ético.* Anaya Multimedia.

HQ, C. (2020). *Cybrary*. Recuperado el 12 de Febrero de 2020, de https://www.cybrary.it/

Inc, C. (2020). *Hack.me*. Recuperado el 12 de Febrero de 2020, de https://hack.me/

Ku, K. (2019). ¿Donde encontrar un hacker? *Innovadores*.

Moore, H. (2003). *Metasploitable*. Recuperado el 12 de Febrero de 2020, de https://www.metasploit.com/
Paradigm, V. (s.f.). *https://online.visual-paradigm.com/es/diagrams/solutions/free-use-case-diagram-tool/*.
Picouto, F. e. (2004). *hacking práctico.* Anaya Multimedia.
Reyes, D. A. (2016). *Congreso en Seguridad en Cómputo* .
Soriano, A. G. (s.f.). Obtenido de Revista seguridad Unam: https://revista.seguridad.unam.mx/numero-13
Soriano, A. G. (2017). Haking Ético, mitos y realidades. *Seguridad Cultura de prevencion para ti*.
SQL, T. s. (s.f.). *Akamai*. Obtenido de https://www.akamai.com/es/es/resources/sql-injection-tutorial.jsp
Tori, C. (2016). *Hacking Etico.* Argentina: Mastroiani Impresiones.
Villa, V. (s.f.). CEO de Fluid Attacks.
Welivesecurity. (Abril de 2015). Obtenido de Comprendiendo la vulnerabilidad XSS: https://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/
wikipedia. (s.f.). *wikipedia*. Obtenido de Pentesting.

Beta, G. D. (2020). *Guia digitla Beta.* Obtenido de http://www.guiadigital.gob.cl/articulo/que-es-la-usabilidad.html
CLUF, M. (1995). Paint. Estados Unidos.
Cortés, M. (24 de julio de 2020). Obtenido de Cio.com.mx: http://cio.com.mx/dell-emc-powerflex-nueva-apuesta-de-almacenamiento/
Daltabuit, E. e. (2007). *Seguridad de la información.* Noriega, Mexico: Limusa.
ElevenPaths. (s.f.). *Blogthinkbig.* Obtenido de Algunos ejemplos y defensas contra el clickjacking: https://empresas.blogthinkbig.com/algunos-ejemplos-y-defensas-contra-e/
GmBH, M. t. (2017). *Maltego*. Recuperado el 12 de Febrero de 2020, de https://www.maltego.com/
Hacksplaning. (2020). *Hacksplaining*. Recuperado el 12 de Febrero de 2020, de www.hacksplaining.com/
Harris, S. e. (2005). *Hacking ético.* Anaya Multimedia.
HQ, C. (2020). *Cybrary*. Recuperado el 12 de Febrero de 2020, de https://www.cybrary.it/
Inc, C. (2020). *Hack.me*. Recuperado el 12 de Febrero de 2020, de https://hack.me/
Ku, K. (2019). ¿Donde encontrar un hacker? *Innovadores*.
Moore, H. (2003). *Metasploitable*. Recuperado el 12 de Febrero de 2020, de https://www.metasploit.com/
Paradigm, V. (s.f.). *https://online.visual-paradigm.com/es/diagrams/solutions/free-use-case-diagram-tool/*.
Picouto, F. e. (2004). *hacking práctico.* Anaya Multimedia.
Reyes, D. A. (2016). *Congreso en Seguridad en Cómputo* .
Soriano, A. G. (s.f.). Obtenido de Revista seguridad Unam: https://revista.seguridad.unam.mx/numero-13

Soriano, A. G. (2017). Haking Ético, mitos y realidades. *Seguridad Cultura de prevencion para ti*.
SQL, T. s. (s.f.). *Akamai*. Obtenido de https://www.akamai.com/es/es/resources/sql-injection-tutorial.jsp
Tori, C. (2016). *Hacking Etico*. Argentina: Mastroiani Impresiones.
Villa, V. (s.f.). CEO de Fluid Attacks.
Welivesecurity. (Abril de 2015). Obtenido de Comprendiendo la vulnerabilidad XSS: https://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/
wikipedia. (s.f.). *wikipedia*. Obtenido de Pentesting.

Mesografía

https://derechodelared.com/hack-me/
https://nogaradevcode.com/entrenamiento-en-seguridad-informatica-dale-una-checada-a-cybrary
https://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/

https://www.dragonjar.org/metasploitable-3-instalacion-en-gnulinux-windows-y-mac-os.xhtml
https://es.wikipedia.org/wiki/Metasploit
https://www.solvetic.com/tutoriales/article/4017-como-virtualizar-instalar-metasploitable-virtualbox/
https://www.monografias.com/trabajos12/hacking/hacking.shtml historia hack
https://www.iniseg.es/blog/ciberseguridad/que-es-el-hacking-etico/ def hacking ético
https://es.wikipedia.org/wiki/Cracker
https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/