Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Hacking Ético

UD05. Hacking de aplicativos web.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

Una vez Pedro ha completado el curso, ha adquirido los conocimientos necesarios para poder realizar tareas propias de una auditoría de hacking ético sobre un aplicativo web.

Al igual que hicieron sus compañeros Luis y Paloma, Pedro ha de realizar unas sesiones formativas con la finalidad de compartir estos conceptos con sus compañeros de trabajo. De esta manera, todos podrán tener, al menos, unas nociones básicas de ciertas técnicas de hacking ético en aplicativos web que ha podido aprender Pedro en el curso.

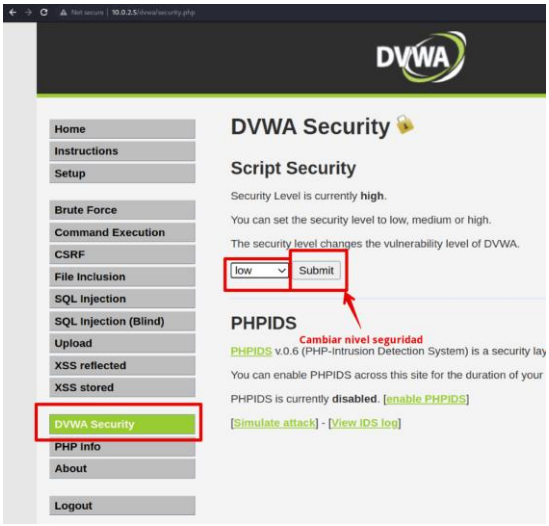
Pedro tiene pensado seguir el mismo enfoque práctico que sus compañeros han dado a este tipo de sesiones formativas dado que todos tienen claro que es el mejor sistema para poder afianzar los conceptos. De modo que configura un laboratorio de pruebas específico para esta temática y resolver de manera práctica algunas de las vulnerabilidades en aplicativos web aprendidas durante el curso.

¿Qué te pedimos que hagas?

Todos los apartados de esta práctica se realizarán sobre el portal vulnerable DVWA que se encuentra instalado en la máquina metasploitable bajo el protocolo HTTP.

Sergio Romero Redondo. *Portales Vulnerables* (CC0)

Tendréis que configurar el nivel de seguridad en "low" para poder realizar la práctica. Para ello, una vez accedáis al portal tendréis que configurar el nivel de seguridad en el apartado "DVWA Security"



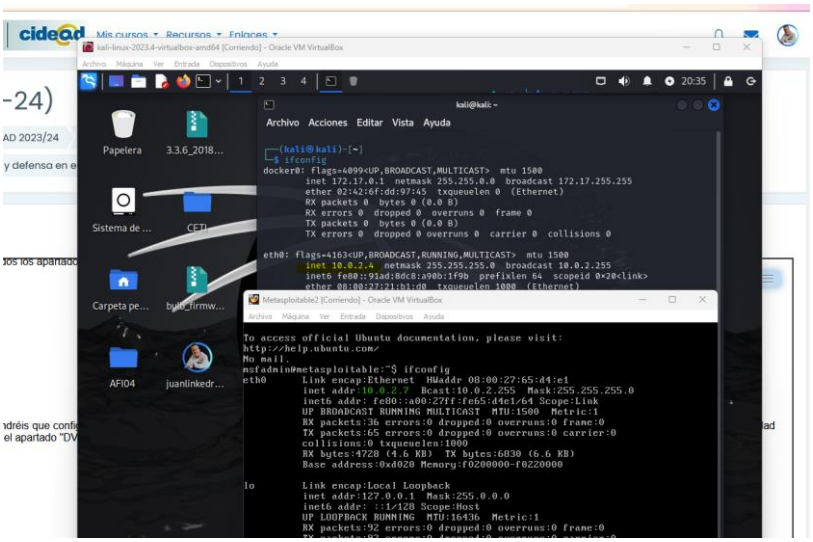
Sergio Romero Redondo. *Nivel de seguridad* (CC0)

✓ Apartado 1: Fuerza Bruta con BurpSuite

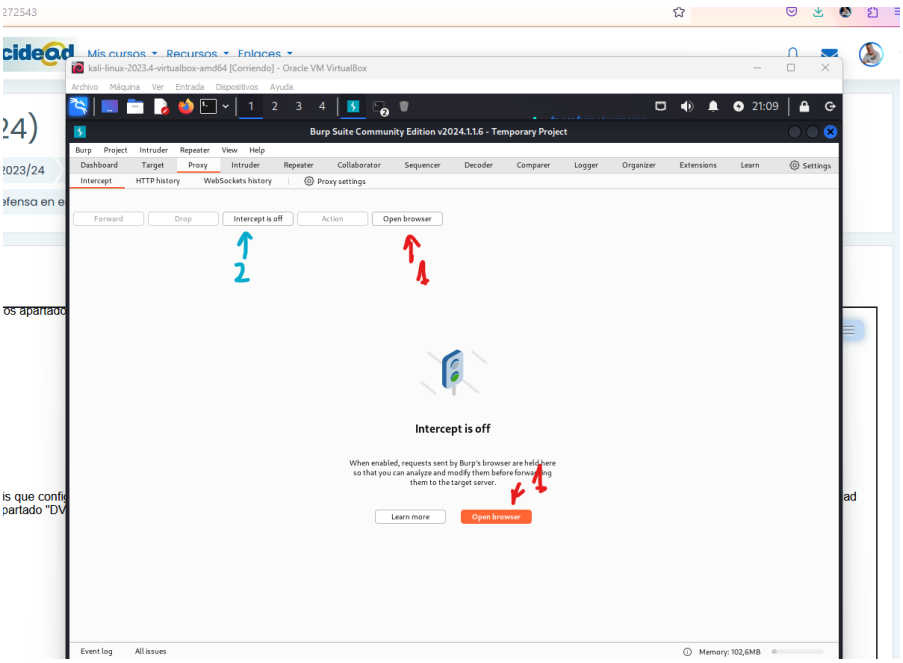
Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de fuerza bruta sobre la funcionalidad "Brute Force" de Damn Vulnerable Web Application.

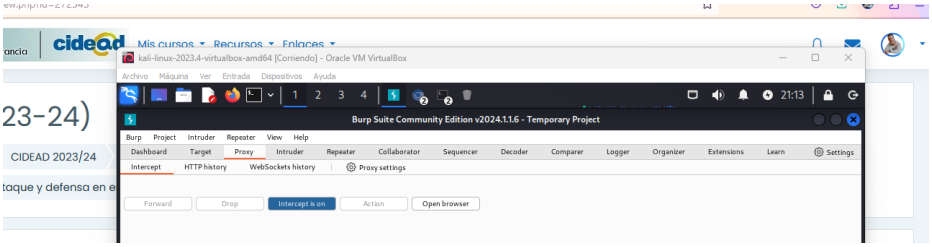
Arranco las máquinas **`Kali`** y **`Metasplotable2`** utilizadas en tareas anteriores.

Confirmamos las IP: **`Kali 10.0.2.4`** y **`Metasplotable2 10.0.2.7`**



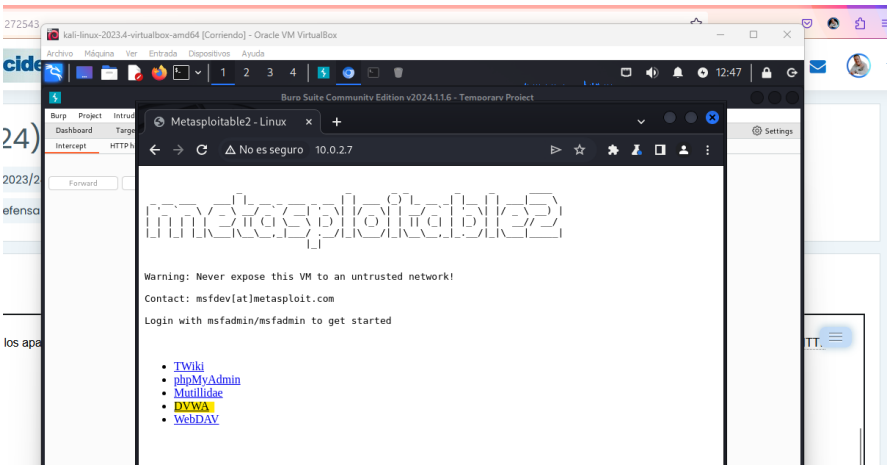
Iniciamos **`BurpSuite`**, y abrimos el navegador que trae integrado desde la pestaña **`proxy`**. Desde este punto también podemos activar la interceptación.



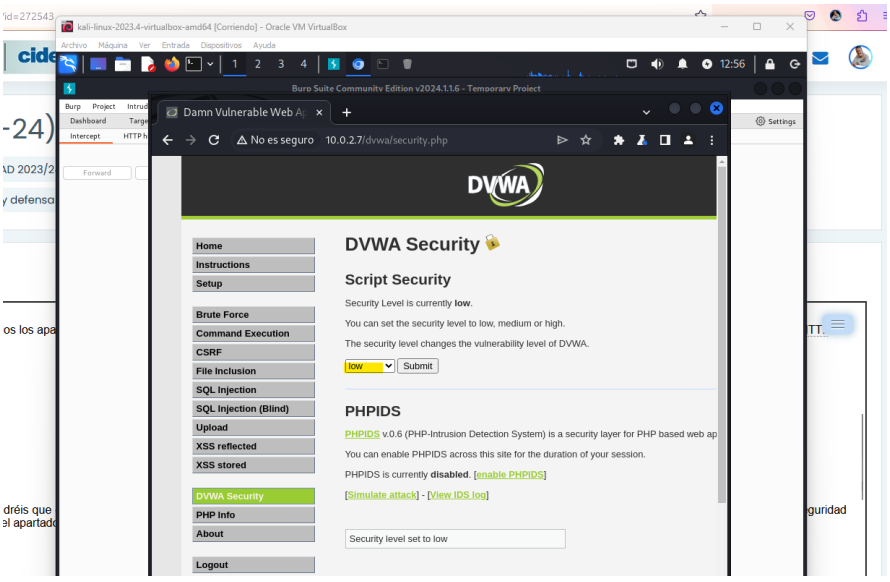


Desactivamos por el momento y accedemos a la máquina de **metasploitable2** desde el navegador.

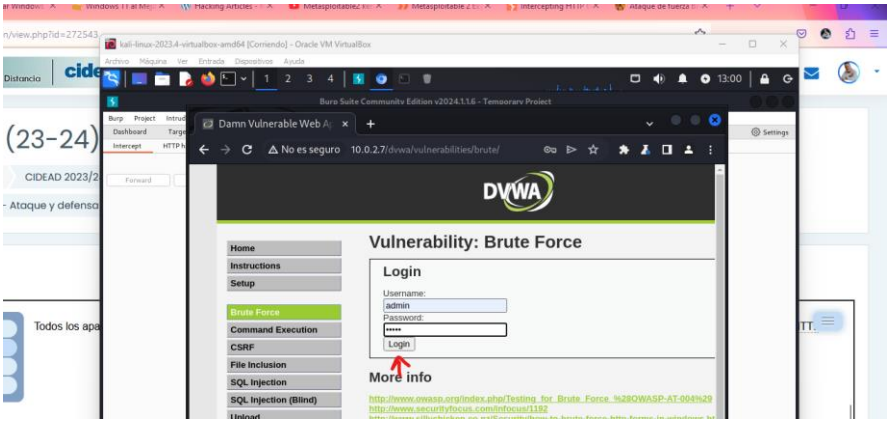
Aquí, nos muestra las herramientas disponibles y podemos entrar a **Damn Vulnerable Web Application**.



Tras loguearnos y siguiendo las pautas del enunciado, seleccionamos el nivel de seguridad **low**.

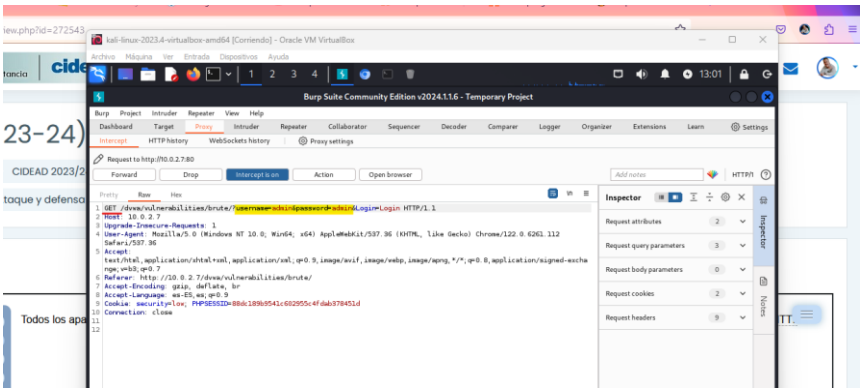


Comenzamos con el ejercicio activando la interceptación y, tras pulsar en la pestaña **Brute Force**, intentamos loguearnos.

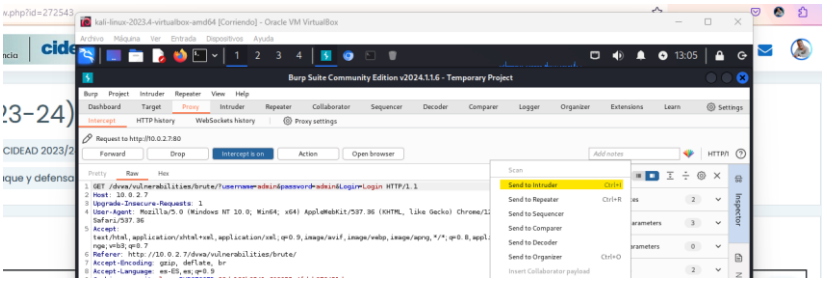


Inmediatamente, nos abre una nueva ventana **BurpSuite** con la petición enviada.

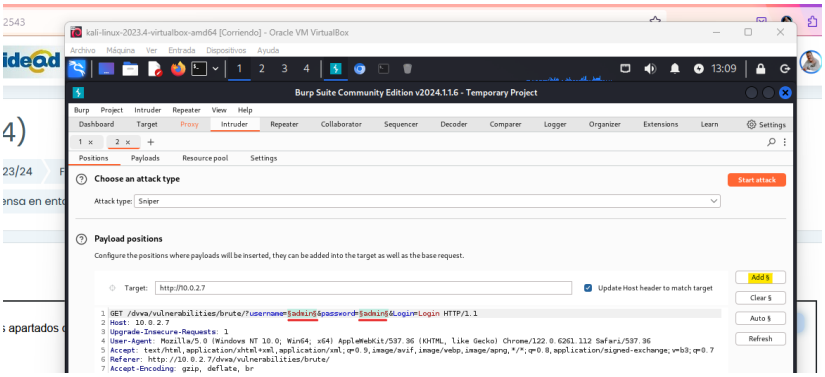
Podemos observar que llega por el método **GET**, inseguro, pero que nos permitirá poder probar con los parámetros.



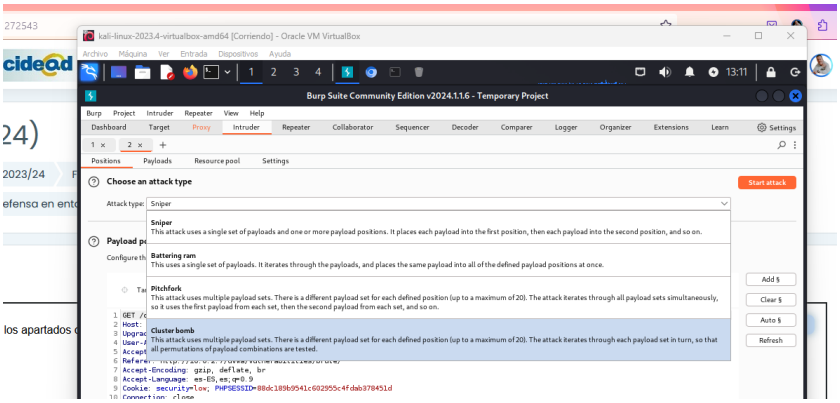
Desde el menú contextual, seleccionamos **Send to Intruder**.



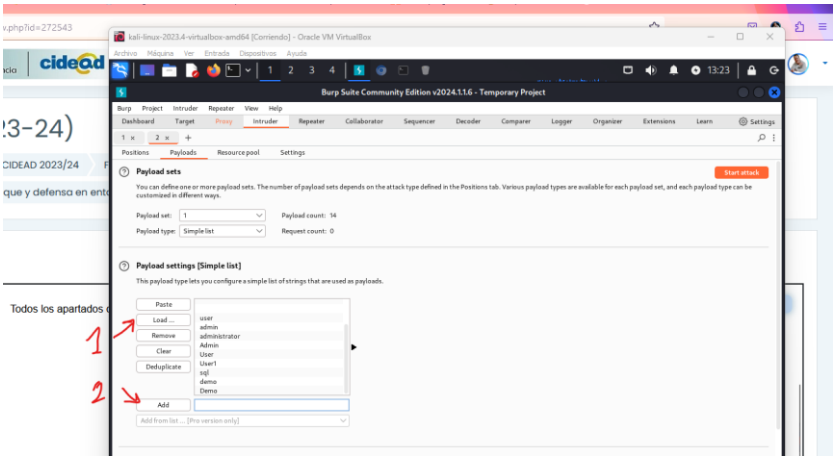
Nos lleva a la pestaña **intruder**, donde podremos añadir los parámetros que necesitamos (**admin/admin**) mediante **Add**.



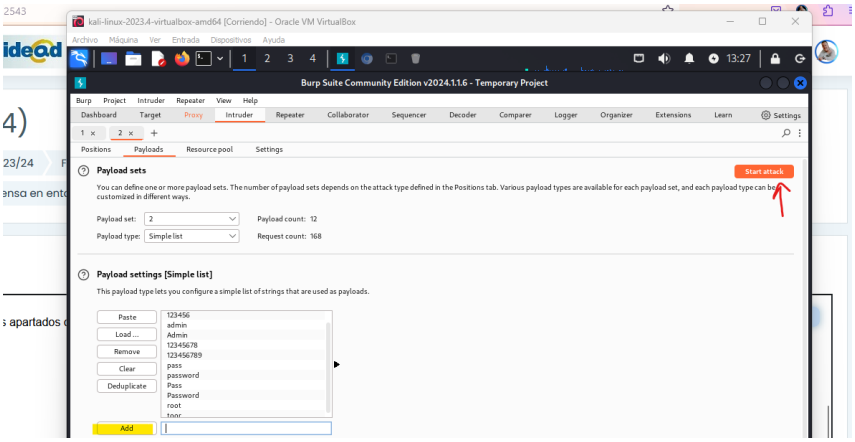
También cambiaremos el tipo de ataque de **sniper** a **Cluster bomb**, para poder jugar con los parámetros y distintos diccionarios si es necesario.



Configuraremos los **payloads** para el usuario y la contraseña. Podemos añadir un diccionario desde **Load** o insertar los nombres a nuestro antojo desde **Add**.



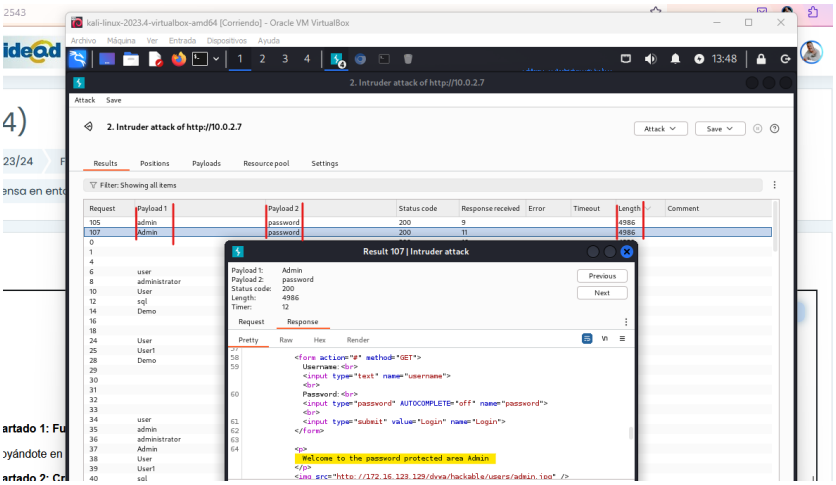
Igual que con el usuario, que está en la posición 1, configuramos la contraseña y tras ello, pulsamos sobre **`Start attack`** para que comience.



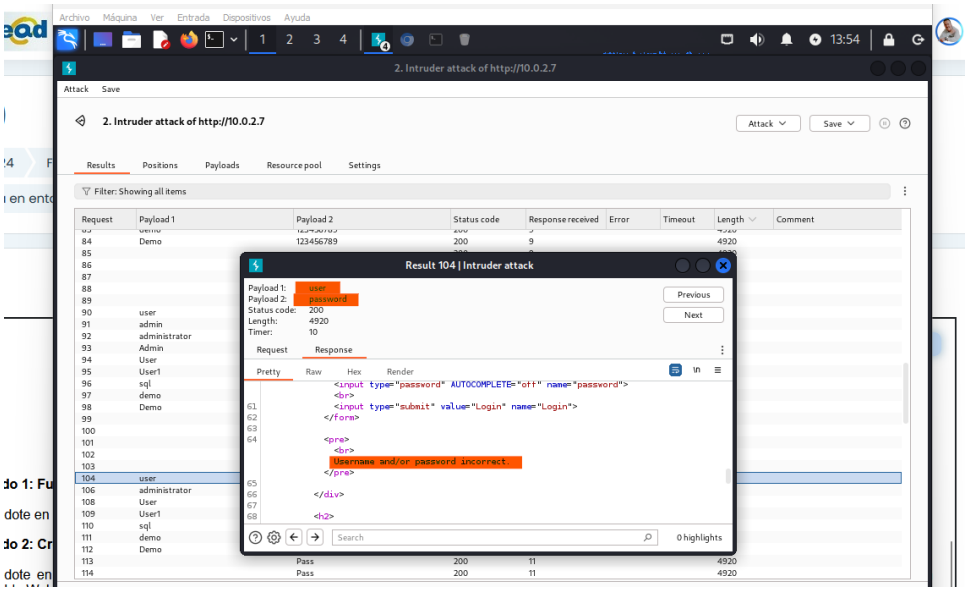
Al terminar, hacemos una revisión visual y podemos observar cómo dos de las peticiones mantienen un tamaño mayor.

Accediendo a una de ellas, comprobamos cómo nos muestra una frase de bienvenida, lo que se traduce en un acceso correcto.

Tras esto, podemos asegurar que los usuarios **`admin`** y **`Admin`**, pueden acceder con la contraseña **`password`**.



Podemos seleccionar otra opción común como **user/password**, y comprobar que el intento es infructuoso.

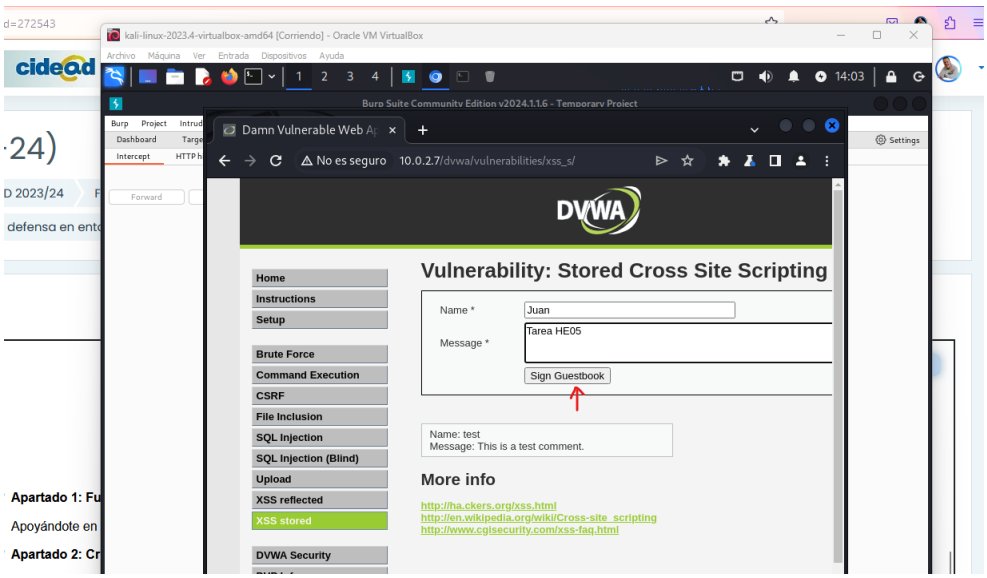


✓ Apartado 2: Cross Site Scripting Almacenado con BurpSuite

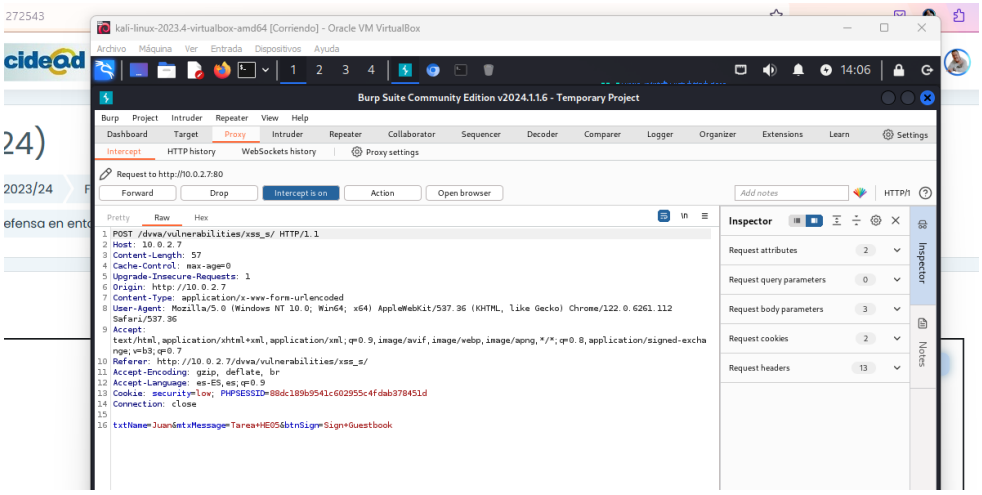
Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de Cross Site Scripting Almacenado sobre la funcionalidad "XSS stored" de Damn Vulnerable Web Application.

El funcionamiento inicial es similar al punto anterior, pero en este caso entramos en **XSS Stored**.

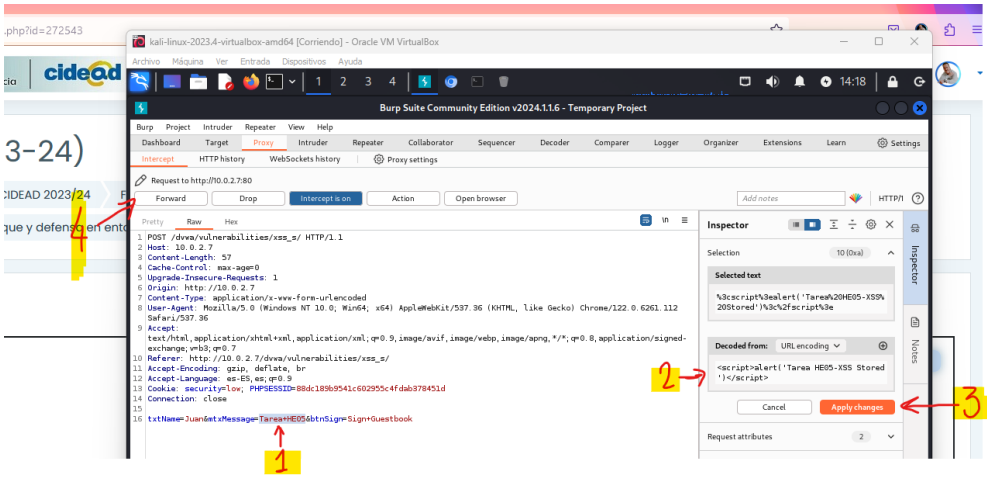
Aquí, rellenamos el formulario y tras activar la interceptación, pulsamos sobre **Sign Guestbook**.



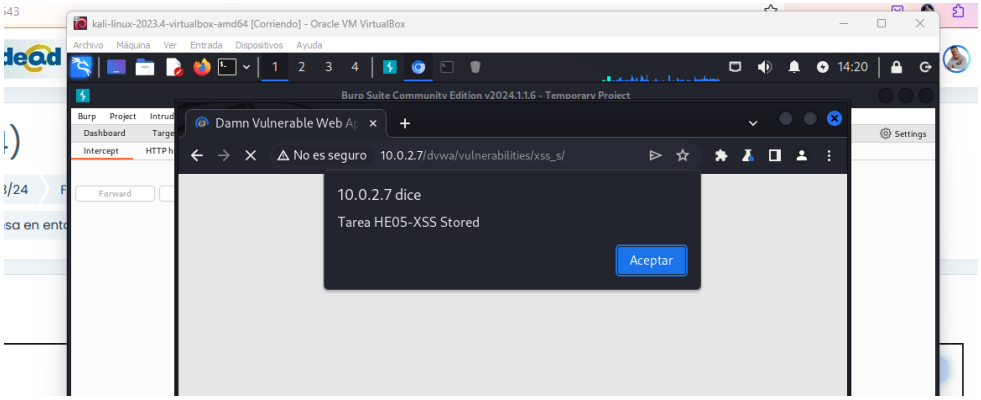
Como antes, nos lleva a otra ventana para mostrarnos la petición. En este caso utiliza el método **POST**, pero podemos aprovechar esta vulnerabilidad **XSS** desde el cuerpo del mensaje.



Seleccionamos el mensaje y lo editamos con un script (utilizaremos el clásico **`alert`** para estos ejemplos). Tras ello, aplicamos los cambios y pulsamos sobre **`forward`**.



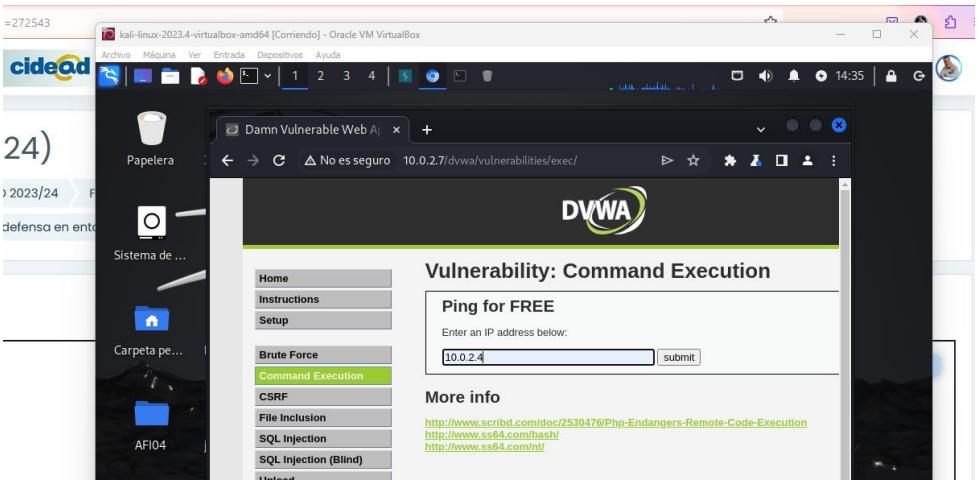
Eso nos mostrará el mensaje que guardamos, con el intento de envío.



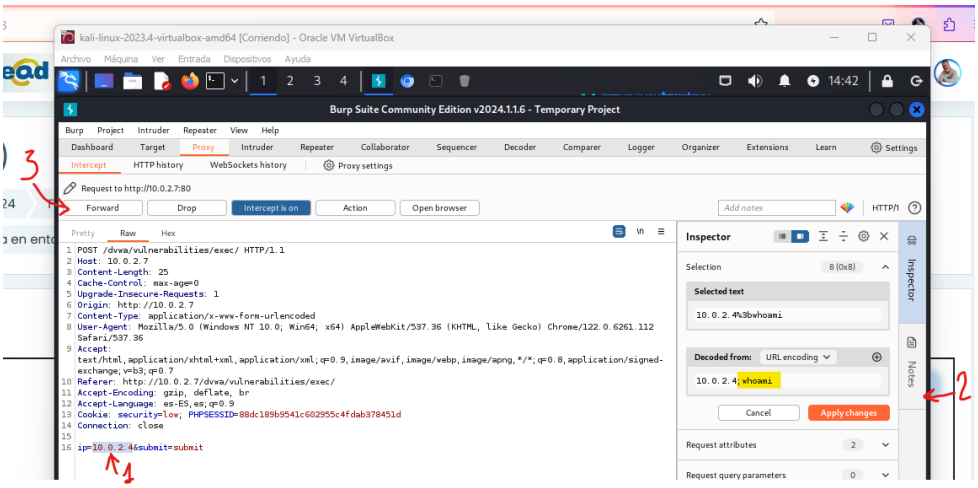
✓ Apartado 3: Ejecución remota de código con BurpSuite

Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de ejecución remota de código sobre la funcionalidad "Command Execution" de Damn Vulnerable Web Application.

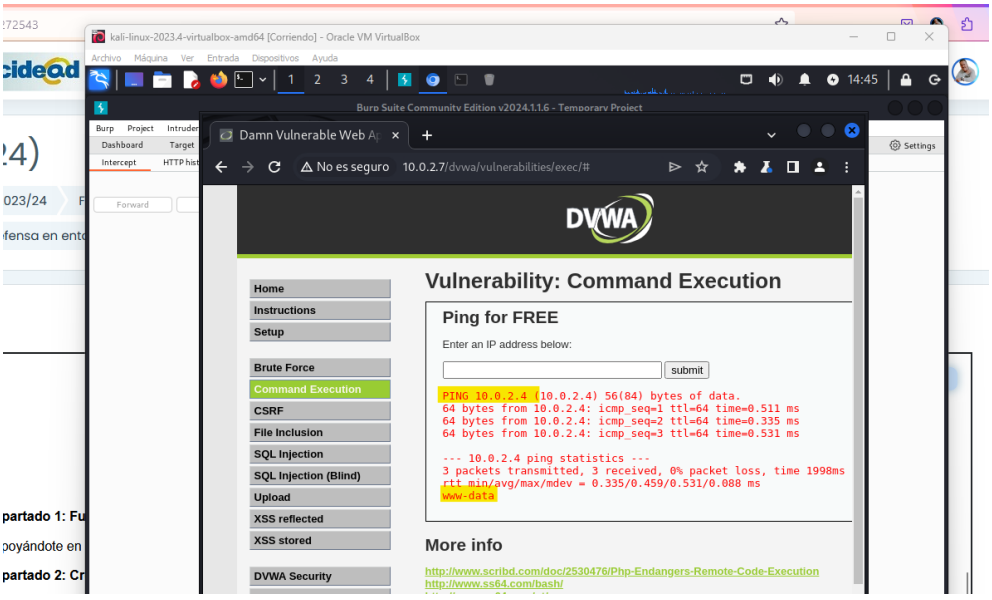
Como en puntos anteriores, accederemos en este caso a **`Command Execution`** y pondremos una **`IP`** cualquiera (en este caso, la de la máquina **`Kali`**) sobre la que hacer un **`ping`**.



Como en el ejercicio anterior, lo que hacemos es modificar el campo que es de nuestro interés. En este punto es la **IP**, tras la cual le añadiremos un comando clásico para ver si lo ejecuta. Tras guardar los cambios, pulsamos sobre **forward**.



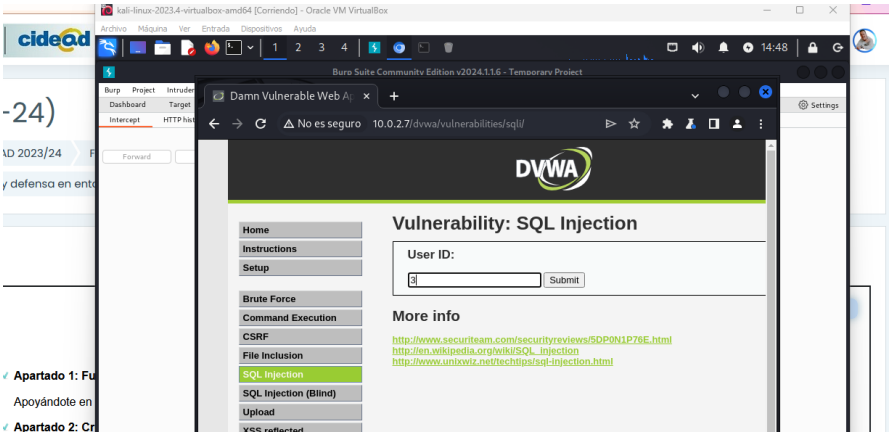
Al volver a la vista, nos muestra los pings realizados correctamente, al igual que la ejecución del comando.



✓ Apartado 4: Ejecución de inyección SQL con BurpSuite

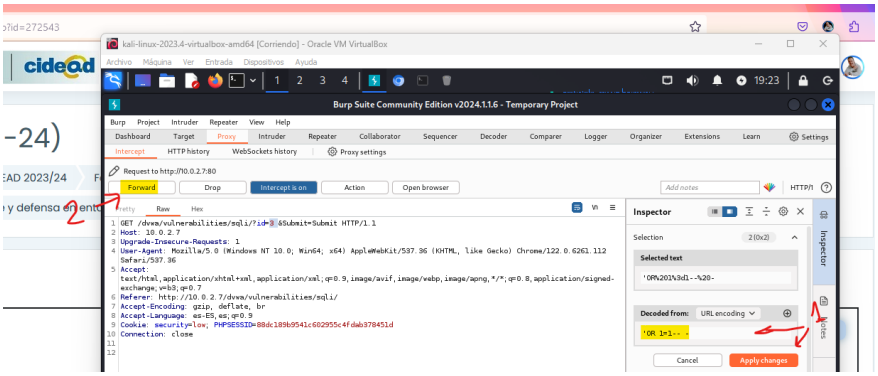
Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de inyección SQL sobre la funcionalidad "SQL injection" de Damn Vulnerable Web Application.

Comenzamos el ejercicio como los anteriores, pero aquí añadimos un **`id`** al azar e iniciamos la interceptación.

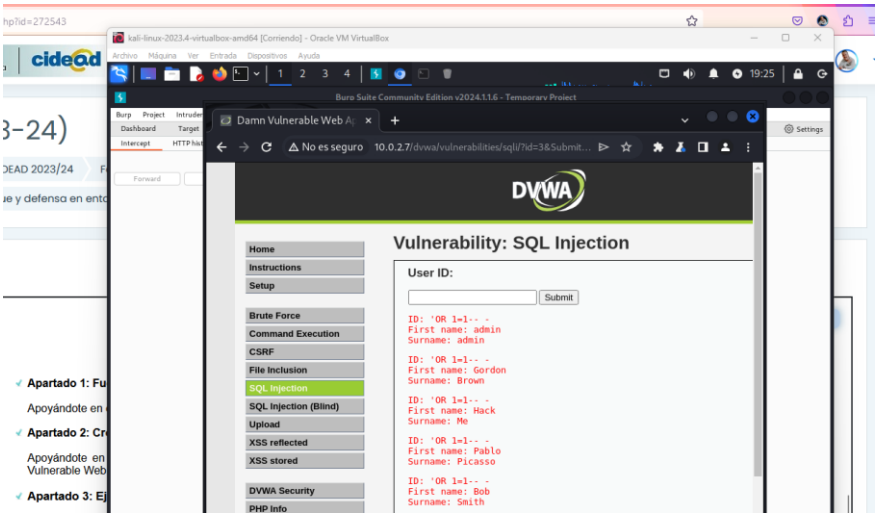


`BurpSuite` nos enseña la petición **`GET`** con la ruta, donde podemos identificar claramente el **`id`** enviado y que podemos manipular como en los casos anteriores.

En este caso, romperemos la sentencia con un **`OR`**. Guardamos cambios y pulsamos sobre **`forward`**.



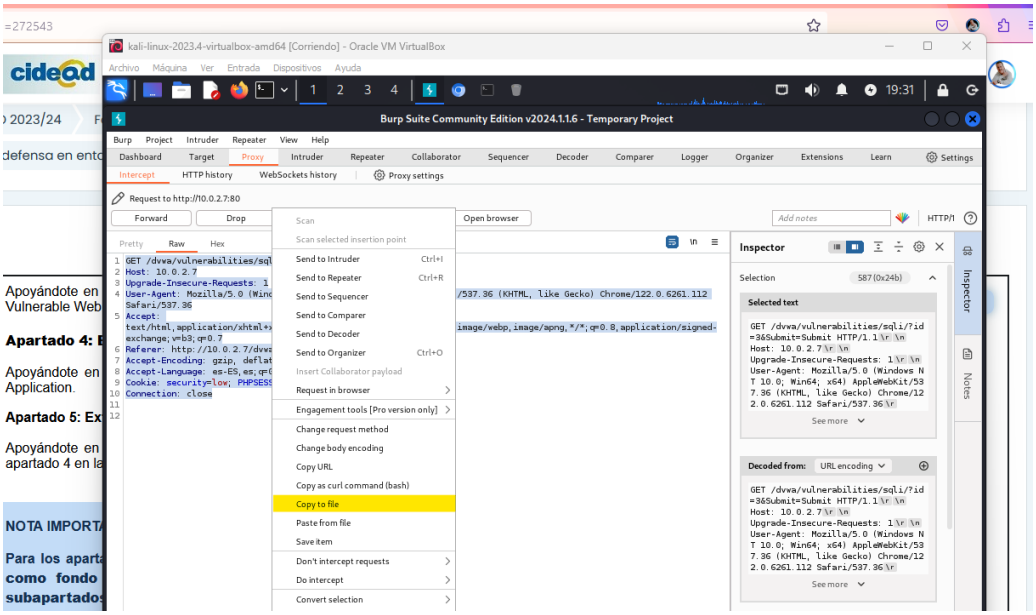
Podemos ver como el **`OR`** ha funcionado y al devolver siempre true la consulta, nos muestra todos los usuarios.



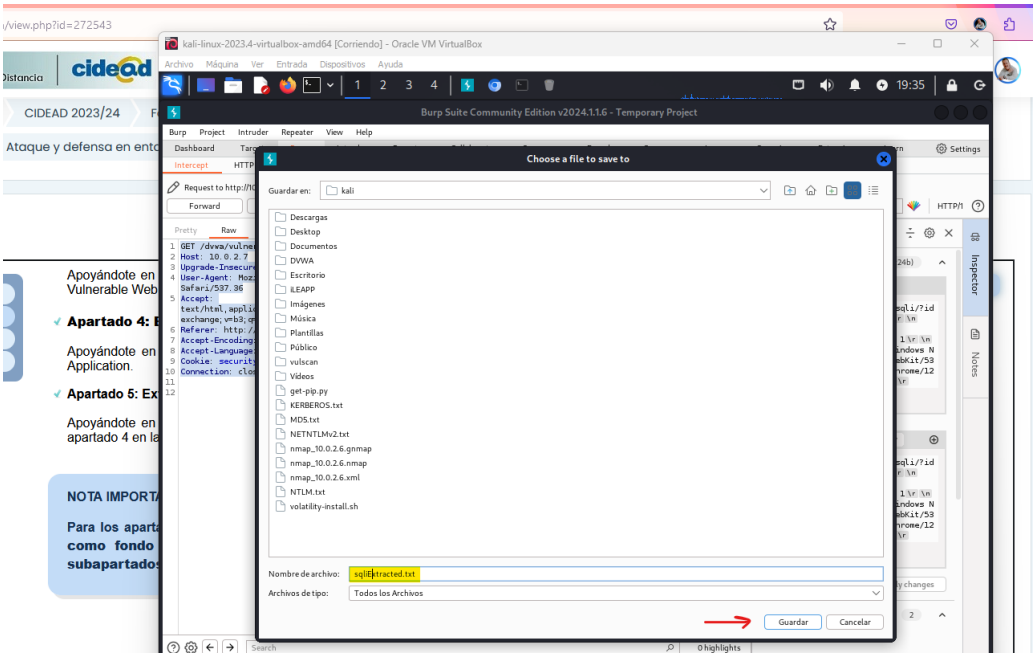
✓ Apartado 5: Extraer datos con sqlmap

Apoyándote en la herramienta sqlmap extrae información de el "Banner de la Base de Datos" utilizando la vulnerabilidad de inyección SQL localizada en el apartado 4 en la funcionalidad "SQL injection" de Damn Vulnerable Web Application.

Desde la petición anterior, capturamos su contenido en un archivo con el menú contextual y la opción **`Copy to file`**.

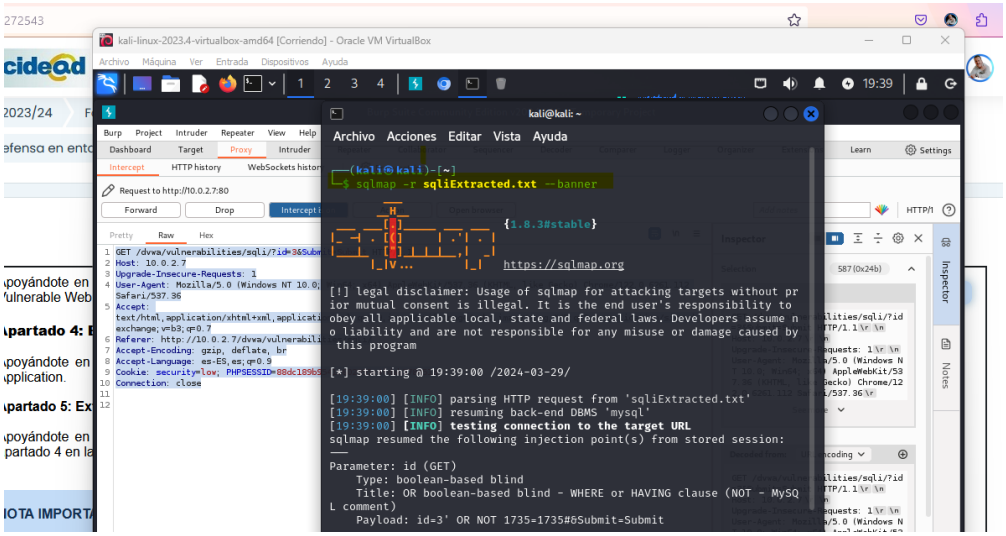


Tras darle un nombre, guardamos.

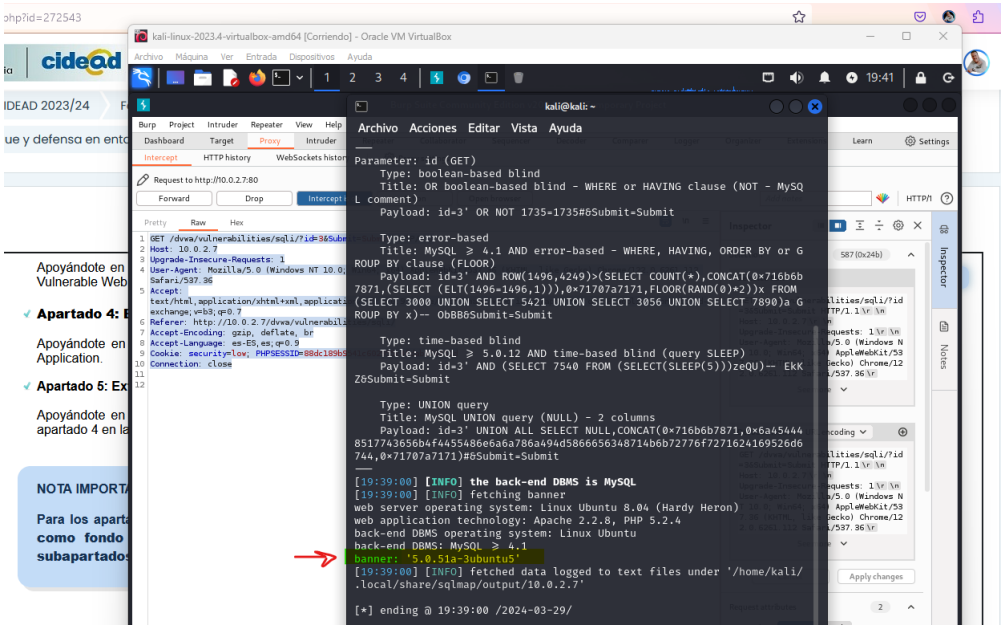


A continuación, y aprovechando las cookies de sesión, abrimos una consola y desde **SQLMap** le pasamos el archivo y le indicamos que queremos el banner.

`sqlmap -r sqliExtracted.txt --banner`



Nos muestra **`5.0.51a-3ubuntu5`**



Webgrafía.

https://www.mecd.es/cidead/aulavirtual/course/view.php?id=2369#section-6

https://keepcoding.io/blog/ataque-de-fuerza-bruta-con-burp-suite/

https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/#dvwa

https://www.youtube.com/watch?v=67T6Q2cj2-U