Universidad Autónoma de Chiapas

Facultad: Contaduría y Administración

Licenciatura: Ingeniería en Desarrollo y Tecnologías de Software

Análisis de Vulnerabilidades

"Actividad 2.3 - Realiza los siguientes ataques al DVWA"

Alumno: Nango Ponce Manuel de Jesus

Grupo: 7M

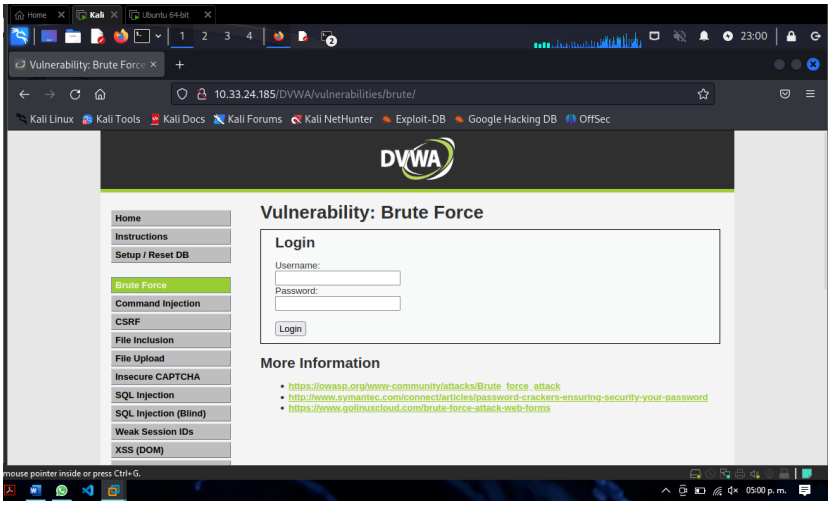
Matrícula: A200338

Docente: Luis Gutiérrez Alfaro

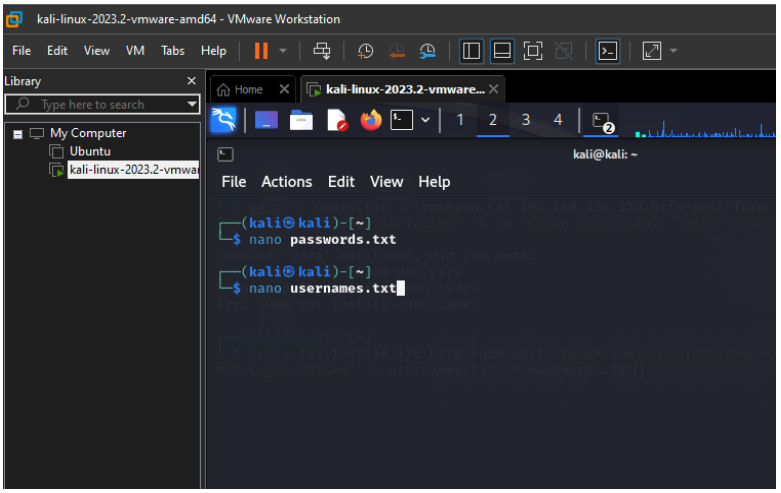
Tuxtla Gutiérrez, Chiapas
27/09/2023

I.- Realizar el ataque al DVWA haciendo un ataque de fuerza bruta

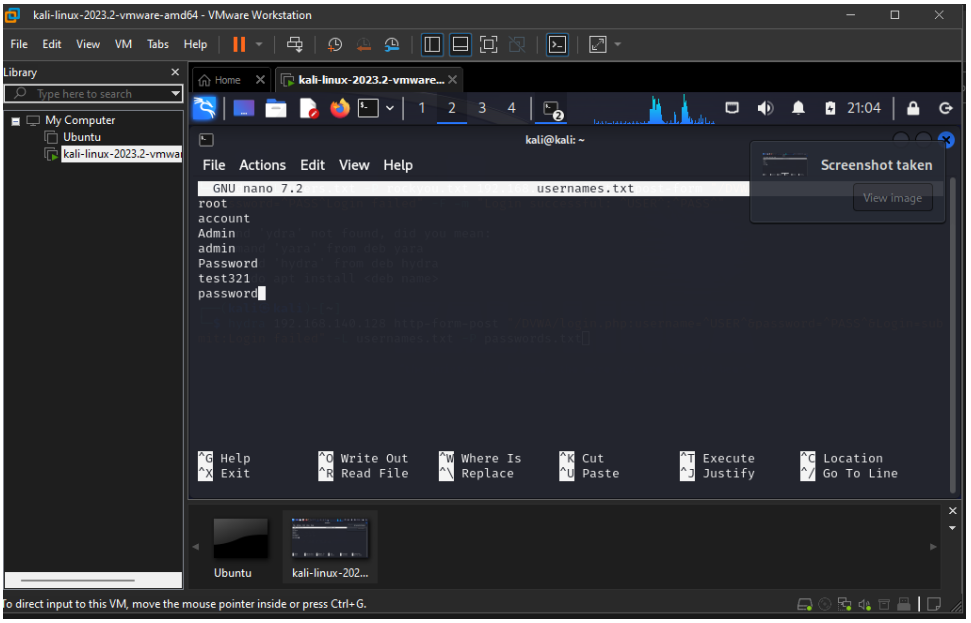
Abrimos nuestro DVWA, vamos a la sección Brute Force (Fuerza Bruta):



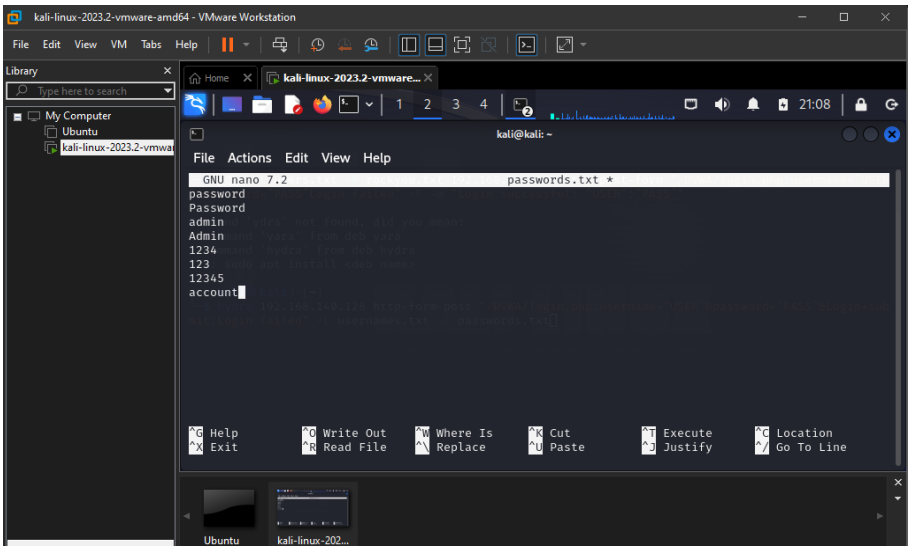
Comando para crear los archivos de texto:



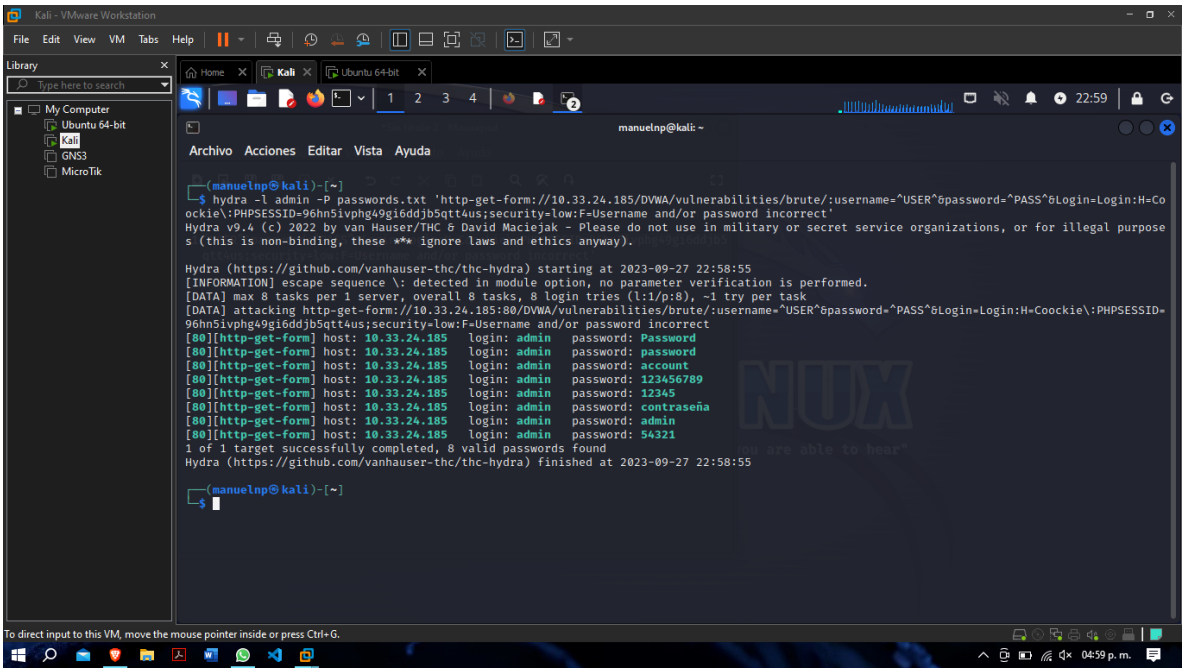
Archivo de Texto usernames.txt:



Archivo de Texto passwords.txt



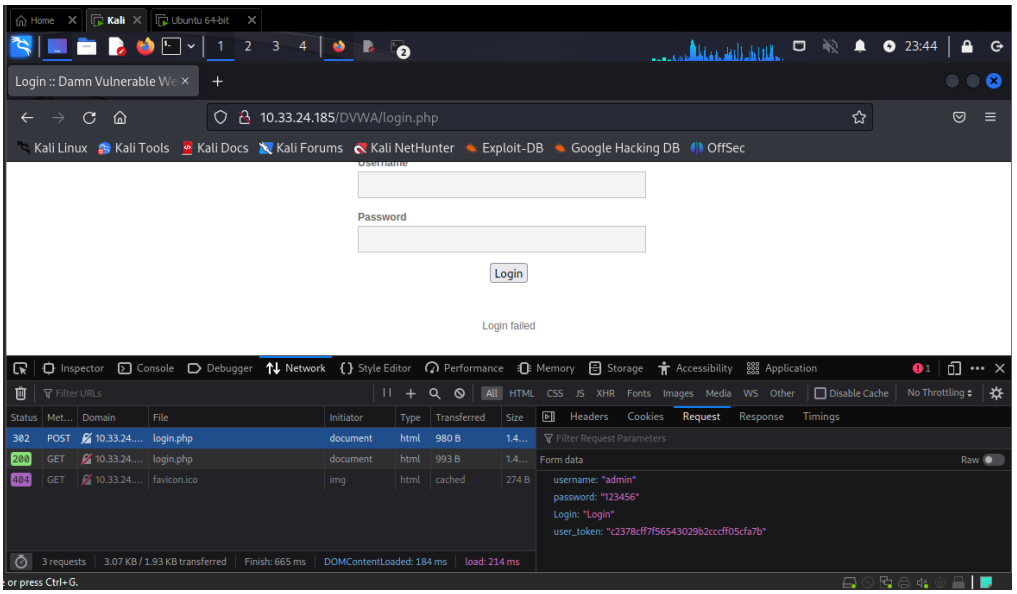
Una vez creados los archivos de texto, en Hydra ejecutamos el comando:



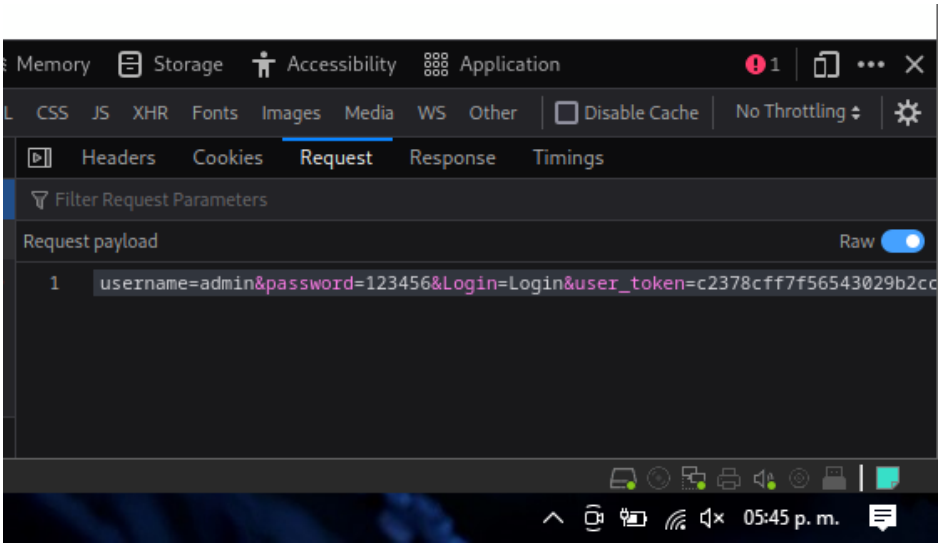
Comando: hydra -l admin -P rockyou.txt 'http-get-form://10.33.26.58/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=96hn5ivphg49gi6ddjb5qtt4us;security=low:F=Username and/or password incorrect'

2.- Ataque a un formulario web al DVWA Inicio de Sesión

En el login de DVWA escribimos un usuario y contraseña cualquiera, damos click derecho a la página e inspeccionar…
En la Pestaña **Network** buscamos la subpestaña **Request** y ahí nos mostrará los datos.

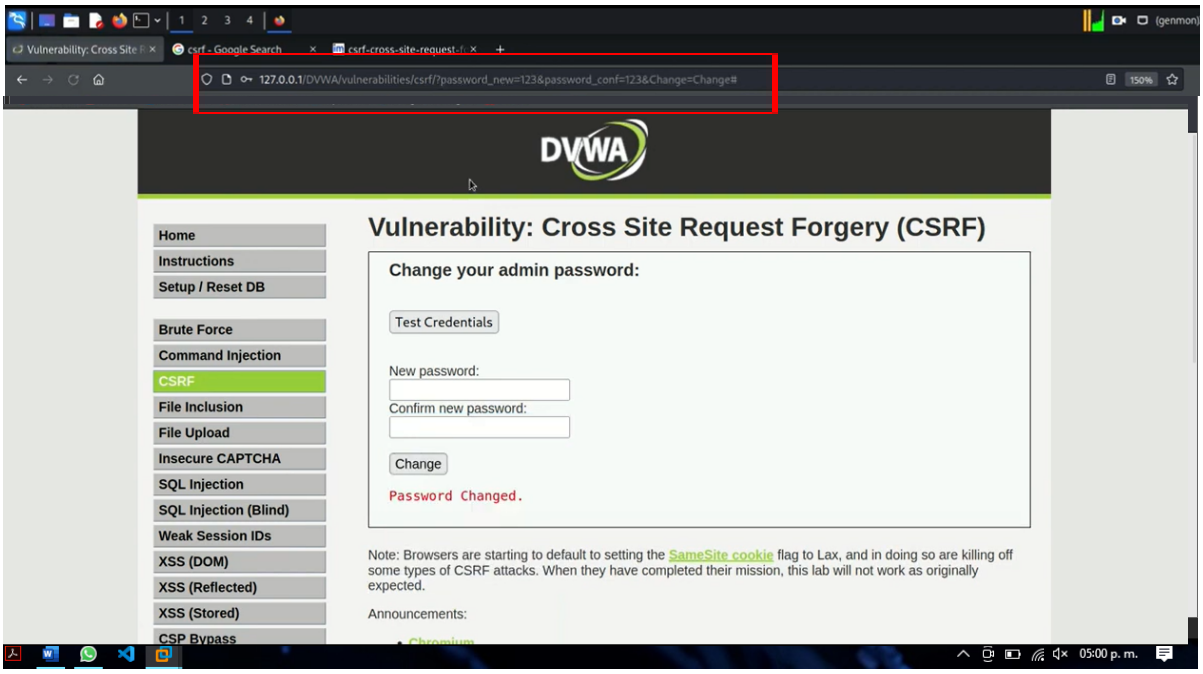


Activamos la opción **Raw** y ya lo tenemos:

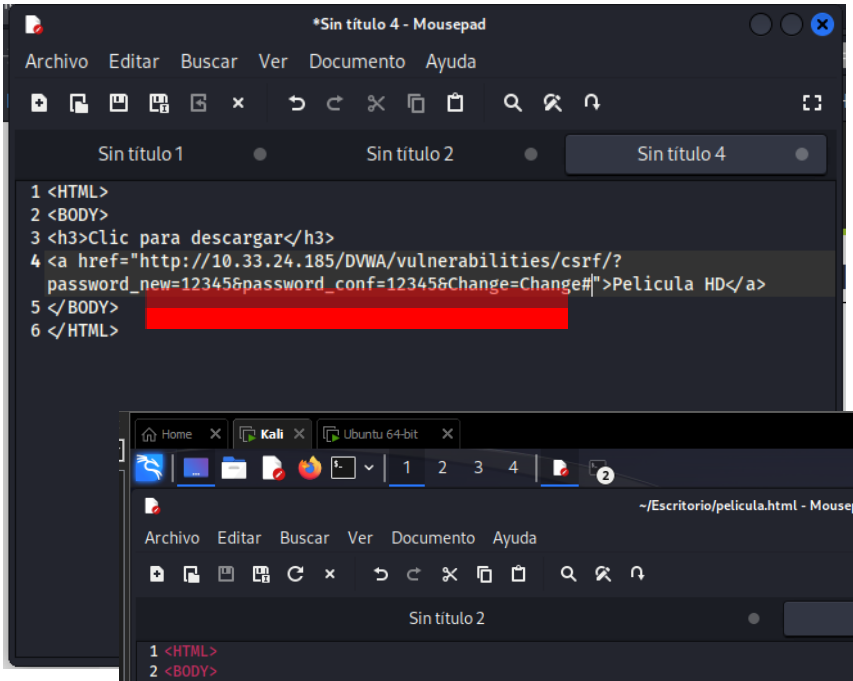


3.- Ataque Diferente (CSRF)

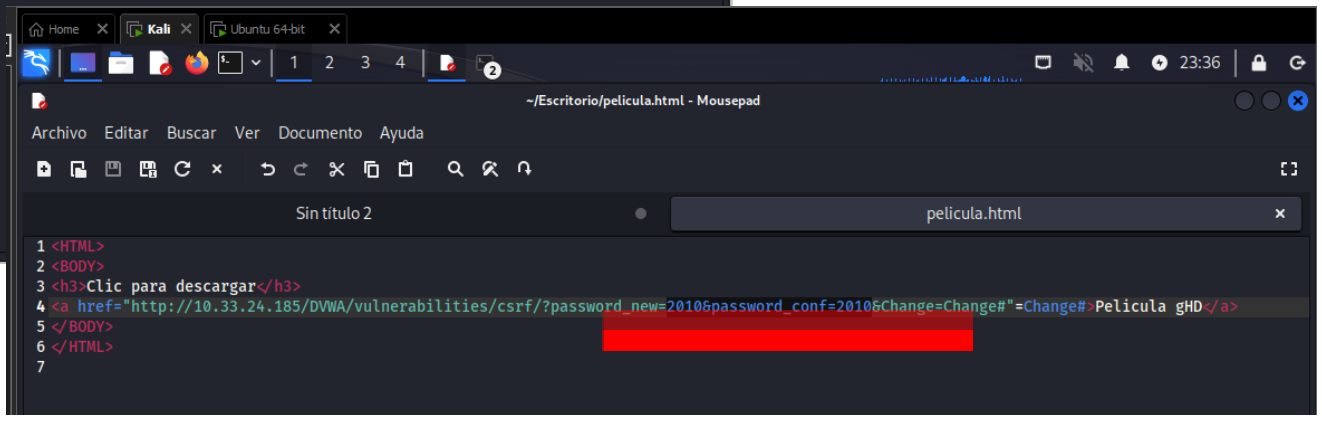
Si vamos al apartado **CSRF** notaremos que si cambiamos la contraseña, esta se muestra en la URL, (no guardé la captura correcta, pero cambié la **contraseña** a **12345**):



Copiamos la URL que nos da justo cuando cambiamos la contraseña, después, en un archivo **HTML** hacemos la siguiente página web, en donde pondremos la URL de DVWA:

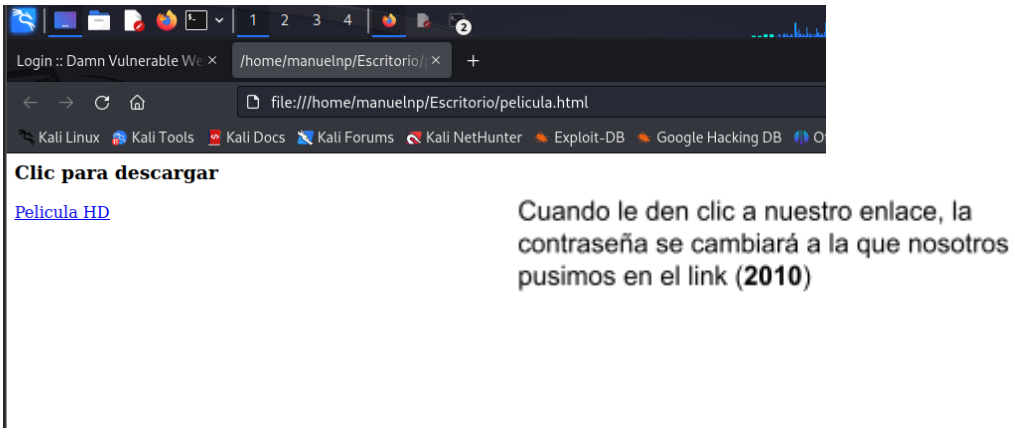


Dentro de un enlace (href) ponemos el link, y se puede notar que aparece la contraseña **12345**.

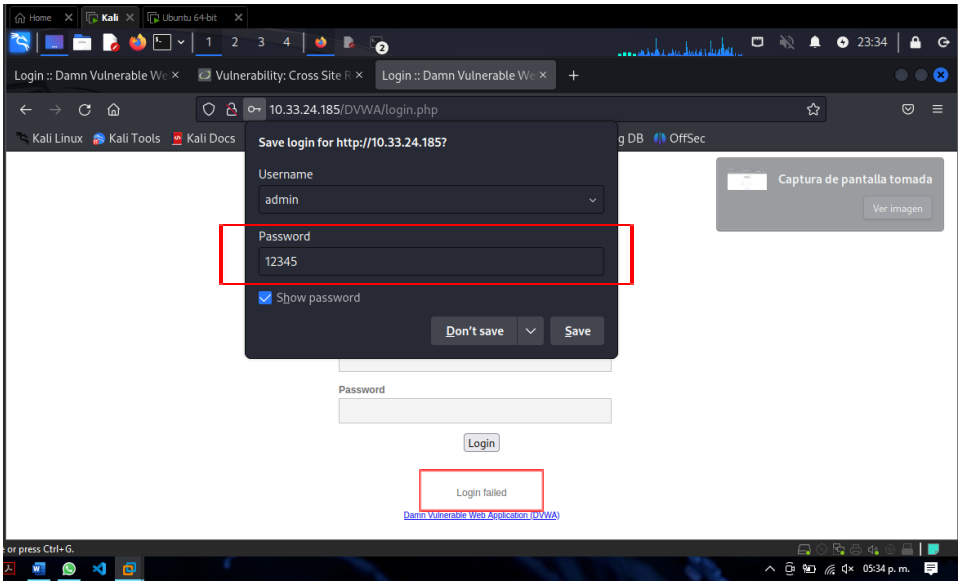


Cambiamos la contraseña por la que nosotros queramos, en este caso **2010**

El resultado de la página web es la siguiente:



Así que cuando queramos ingresar nuevamente al DVWA con la contraseña que habiamos cambiado (**12345**), no nos permitirá iniciar sesión:



Y cuando pongamos la contraseña que pusimos en el link de HTML, es decir **2010** ya nos dejará iniciar sesión.