**Explotación de desbordamiento de buffer**

Primero verificar que las VB estén conectadas

Ping a la VM Bee Box

A screenshot of a computer

Description automatically generated

Ping a la VM Kali

A computer code with numbers and letters

Description automatically generated

**Verificar la Vulnerabilidad de desbordamiento de búfer**

Ejecuta el siguiente comando para ver el contenido del archivo bof\_1.php:

A computer screen shot of a white screen

Description automatically generated

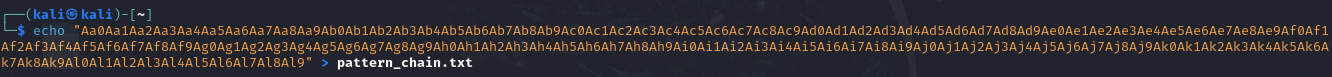
**Generar y usar la Cadena de Explotación**

1. Generar la cadena de explotación ejecutando el siguiente comando en Kali para generar una cadena que te ayudará a identificar el desbordamiento de búfer:

A screenshot of a computer

Description automatically generated

1. Guarde la cadena generada en un archivo llamado pattern\_chain.txt:



1. Inicia un servidor HTTP en Kali para transferir el archivo:



1. Descarga el archivo pattern\_chain.txten BeeBox usando wget:

A computer screen shot of a pattern

Description automatically generated

1. Lee el contenido del archivo descargado en BeeBox:

A black text on a white background

Description automatically generated

**Inyectar la cadena de explotación y el payload**

1. Usa la cadena generada con pattern\_create.rben el campo o parámetro que pueda causar el desbordamiento de búfer en bWAPP.

A screenshot of a computer

Description automatically generatedEjecuta un oyente en Kali para recibir la shell remota:

A screenshot of a computer code

Description automatically generated

1. Para obtener una shell remota, inyecta la siguiente carga útil en el campo que causa el desbordamiento:

A close-up of a number

Description automatically generated

1. Confirmar la conexión en Kali. Si el exploit es exitoso, deberías ver una conexión en el oyente de Kali y recibir un aviso de Bash.

A black background with white text

Description automatically generated

**Verificar los Registros del Servidor**

1. Revise los logs del servidor web en BeeBox para cualquier mensaje relacionado con el desbordamiento de búfer:

A screenshot of a computer

Description automatically generated