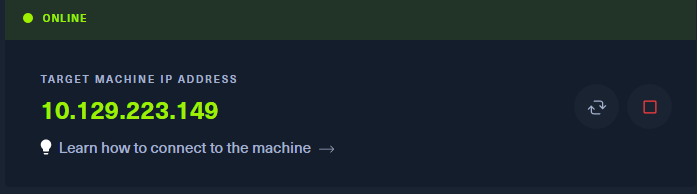
**ANALISIS MAQUINA VIRTUAL COCODRILE**

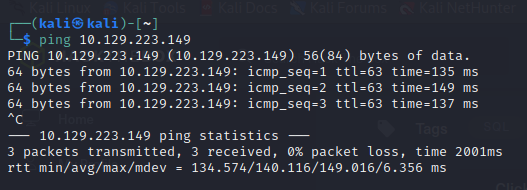
**Dificultad:** Facil

**Etiqueta:** PHP, Ftp

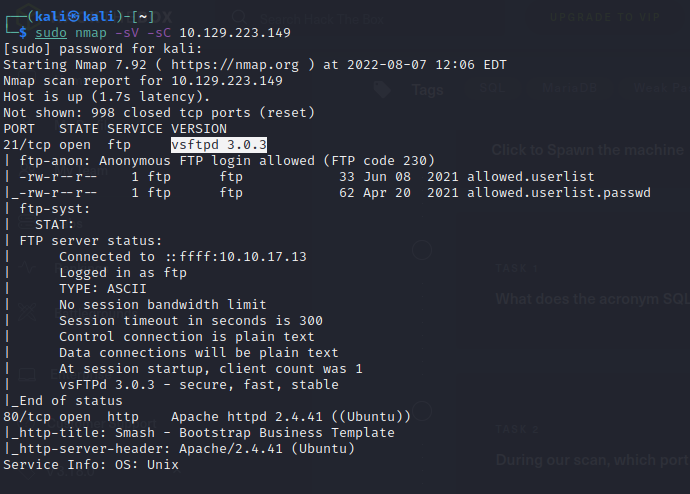
**IP Maquina**



Realizamos ping para ver si tenemos conexión

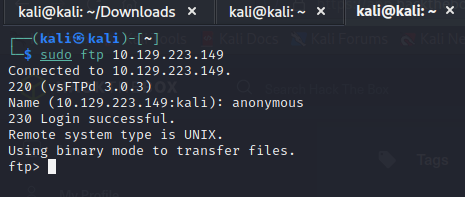


Escaneamos para ver los puertos y servicios

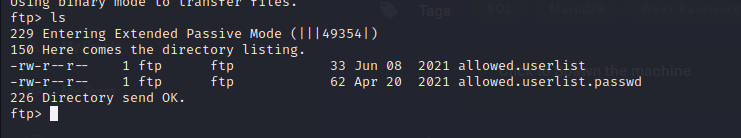


Tenemos el puerto 21 abierto que pertenece al servicio ftp conla versión vsftpd 3.0.3 y también tenemos el puerto 80 del servicio apache versión httpd 2.4.41

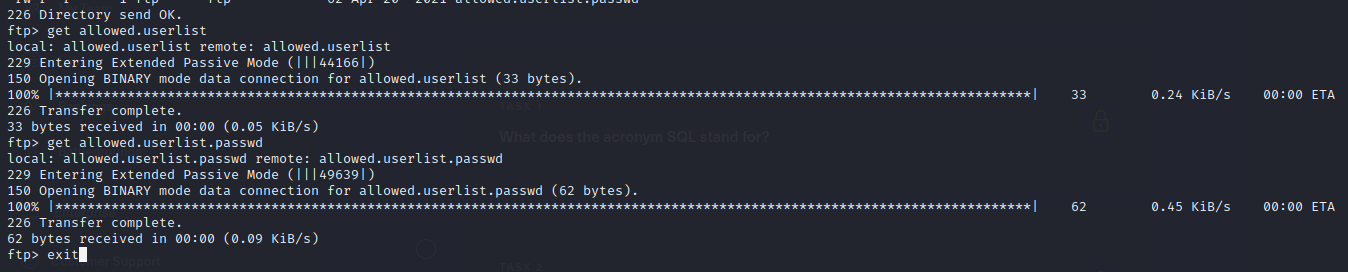
Volvemos a probar con el nombre de usuario Anonymous y contraseña en blanco para ver si tenemos suerte de poder ingresar



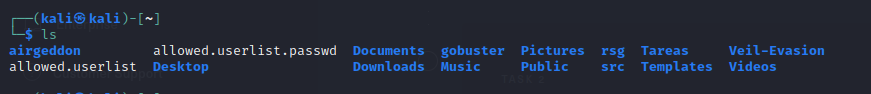
Ingresamos satisfactoriamente solo enlistamos con el comando ls o dir para ver que archivos encontramos

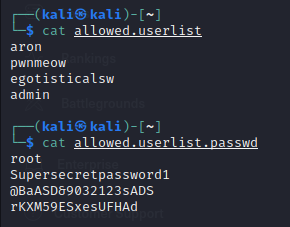


Podemos observar que hay dos archivos, allowed.userlist que probablemente es un listado de usuarios y allowed.userlist.passwd que será el listado correspondiente a las constraseñas de los usuarios, con esto podríamos relizar una fuerza bruta a una pagina web, que suponemos que habra una ya que tenemos abierto el puerto 80. Entonces procedemos a descargar los archivos

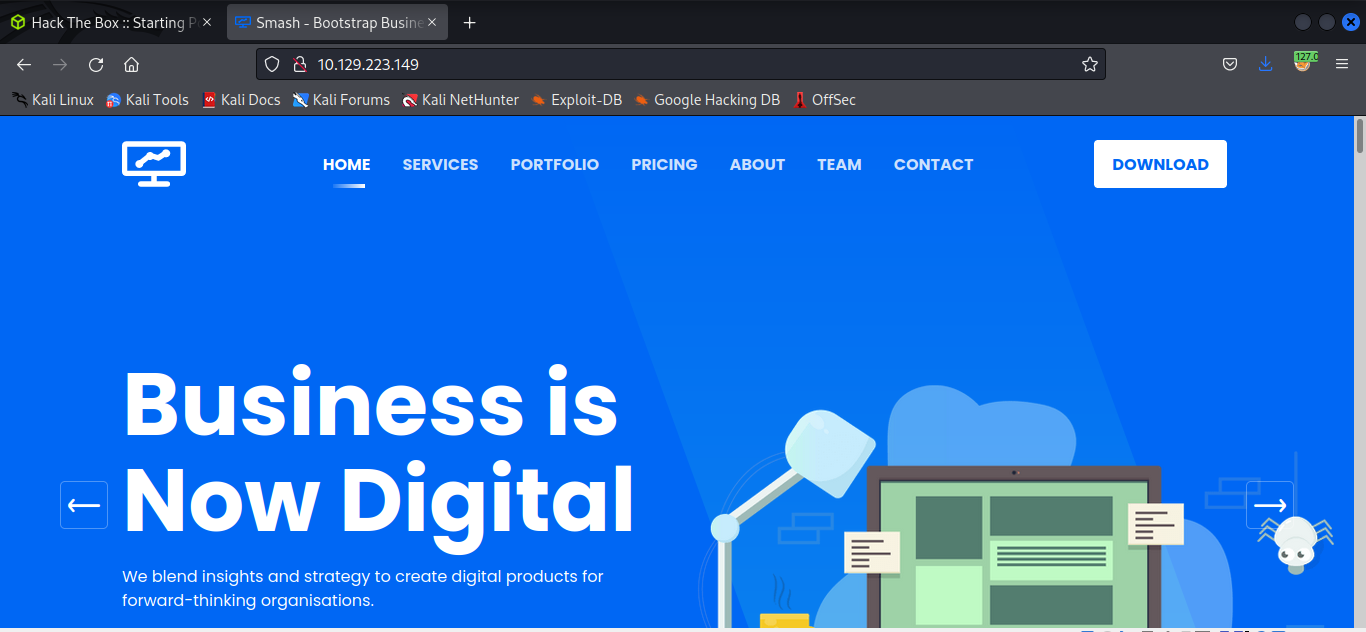


En la ubicación que estamos damos ls para ver archivos descargados y con el comando cat podemos verificar su contenido

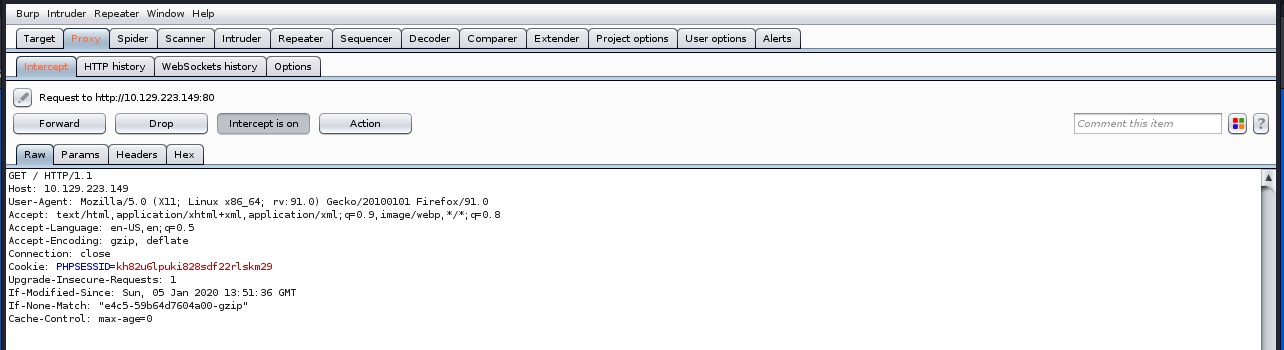




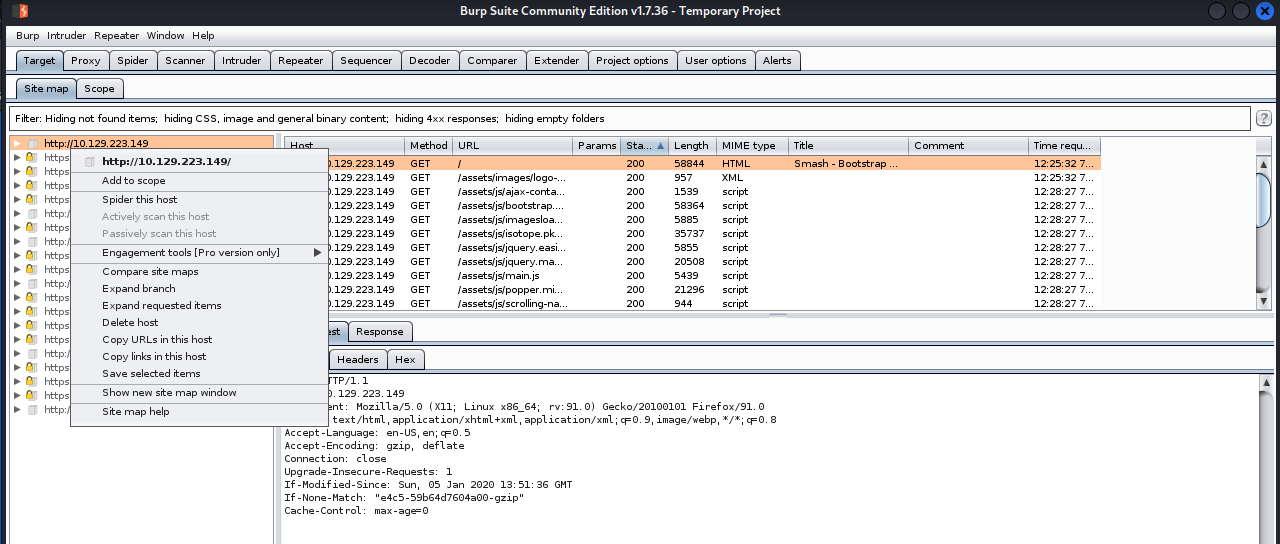
Verificamos la pagina web colocando en el navegador la dirección ip de la maquina vulnerable



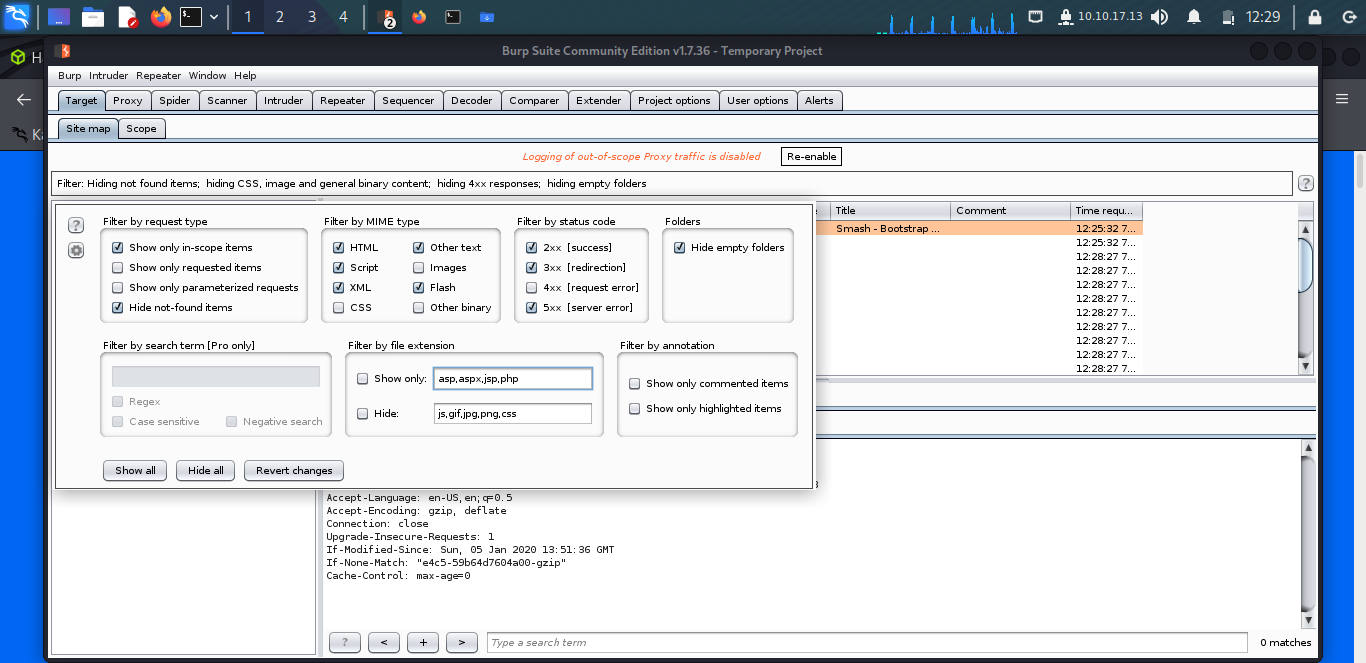
Ahora usaremos la herramienta burpsuite para analizar los directorios que contenga la pagina web, activaremos foxy proxy y encenderemos el burpsuite para leer el trafico damos forward y apagamos



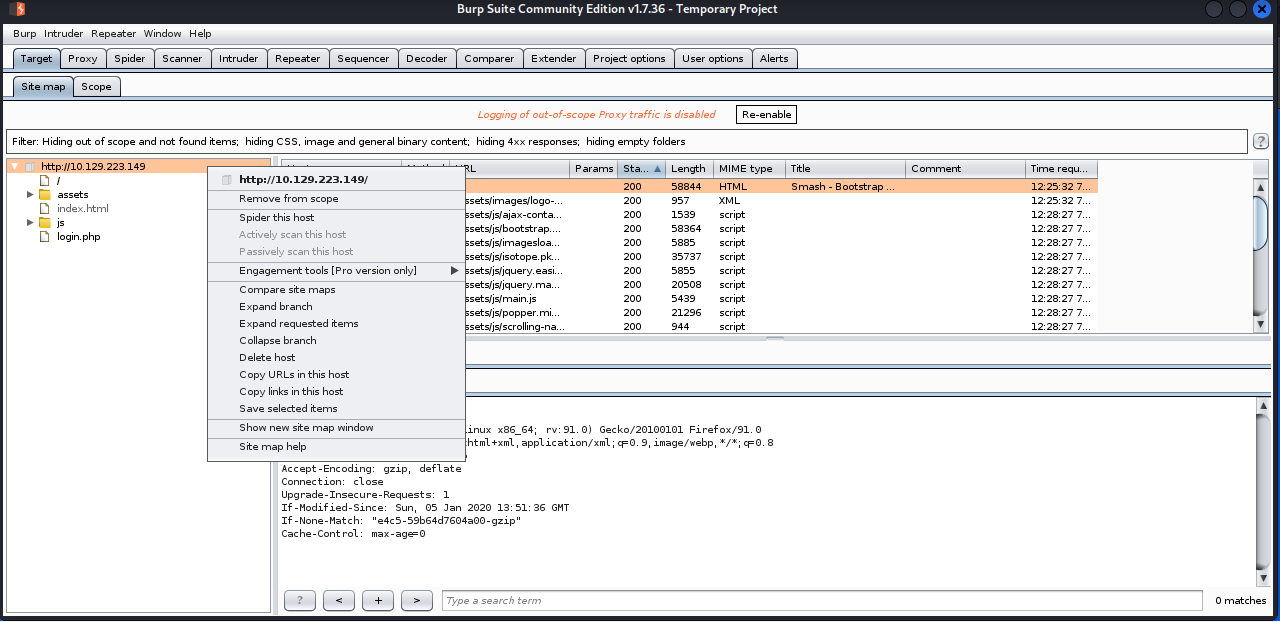
En la viñeta target damos clic derecho a la pagina y add scope



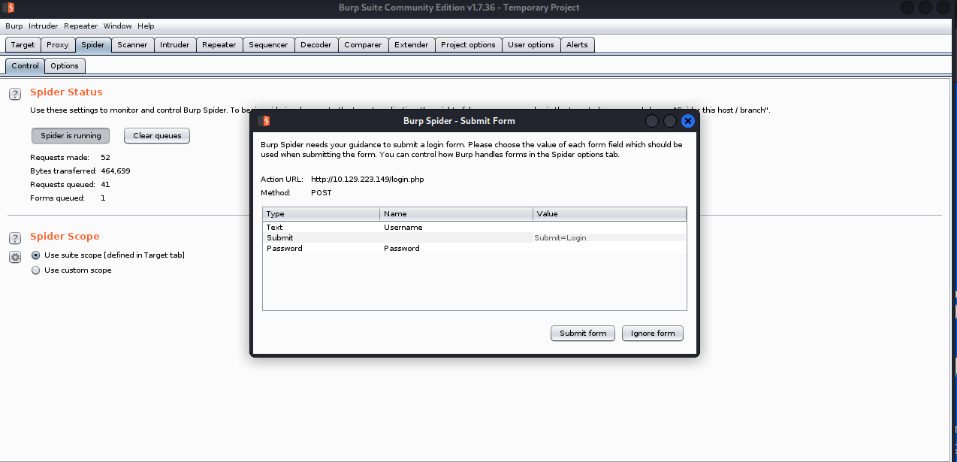
Filtramos para que solo se vea la pagina que estamos trabajando



Clic derecho nuevamente a la pagina y le damos spider

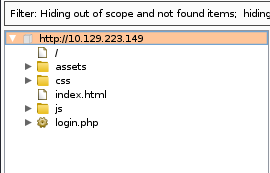


Verificamos en la viñeta spider si se esta analizando

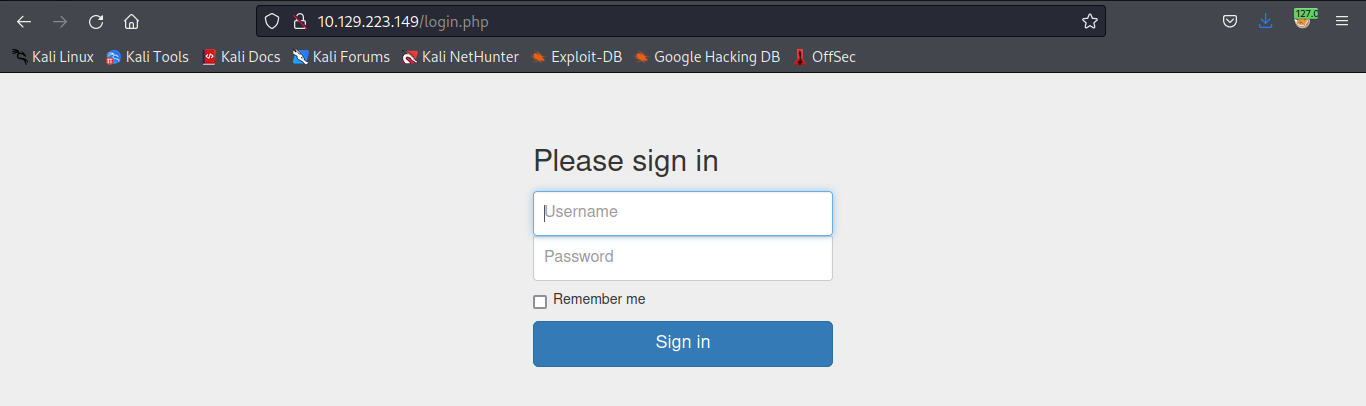


Si salen cuadros le damos submit form

Con este proceso tendremos todos los directorios listados y archivos de la pagina web

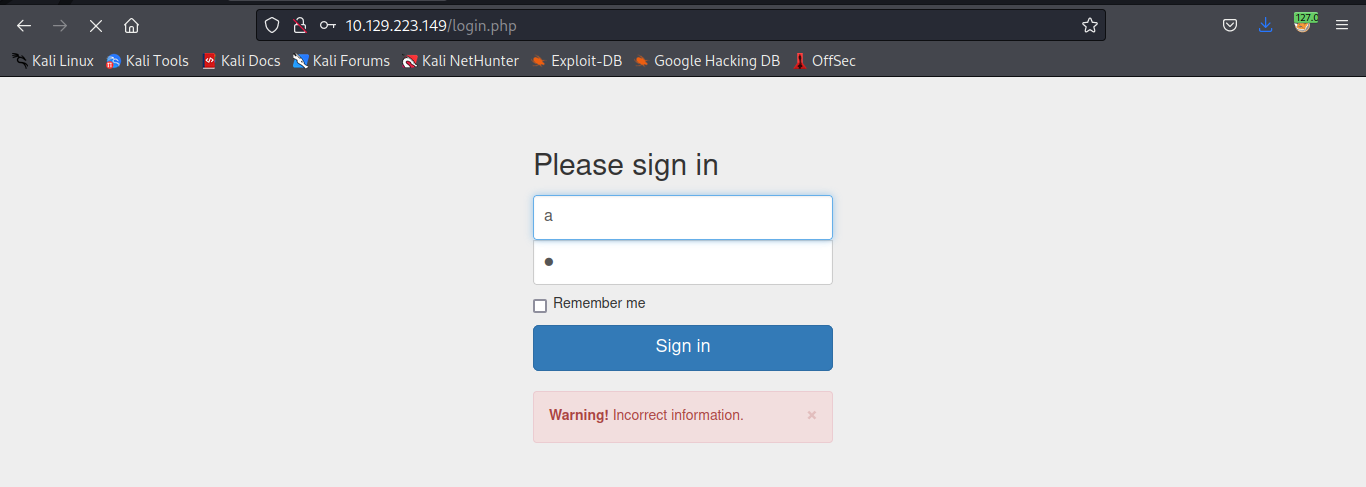


Podemos notar que la pagina tiene una sección login la cual colocaremos en el navegador



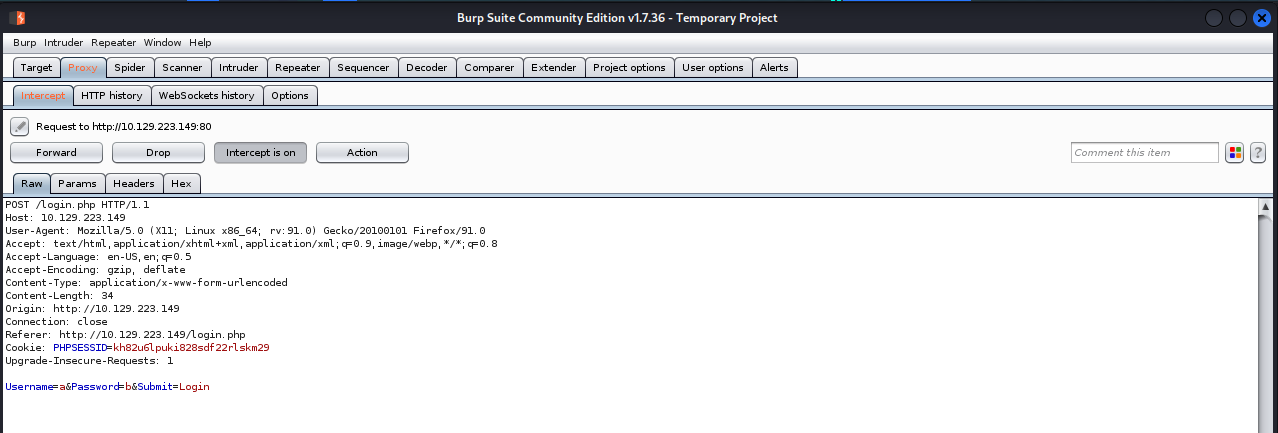
Ahora analizaremos con burpsuite para después realizar un ataque de fuerza bruta con los archivos que descargamos con ftp

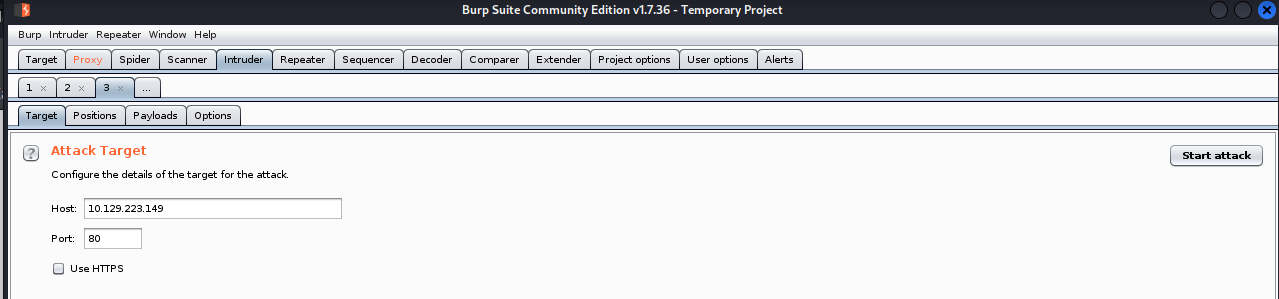
Probamos a ingresar aleatoriamente datos



Vemos cuando las credenciales son incorrectas nos sale **Incorrect Information** (info importante)

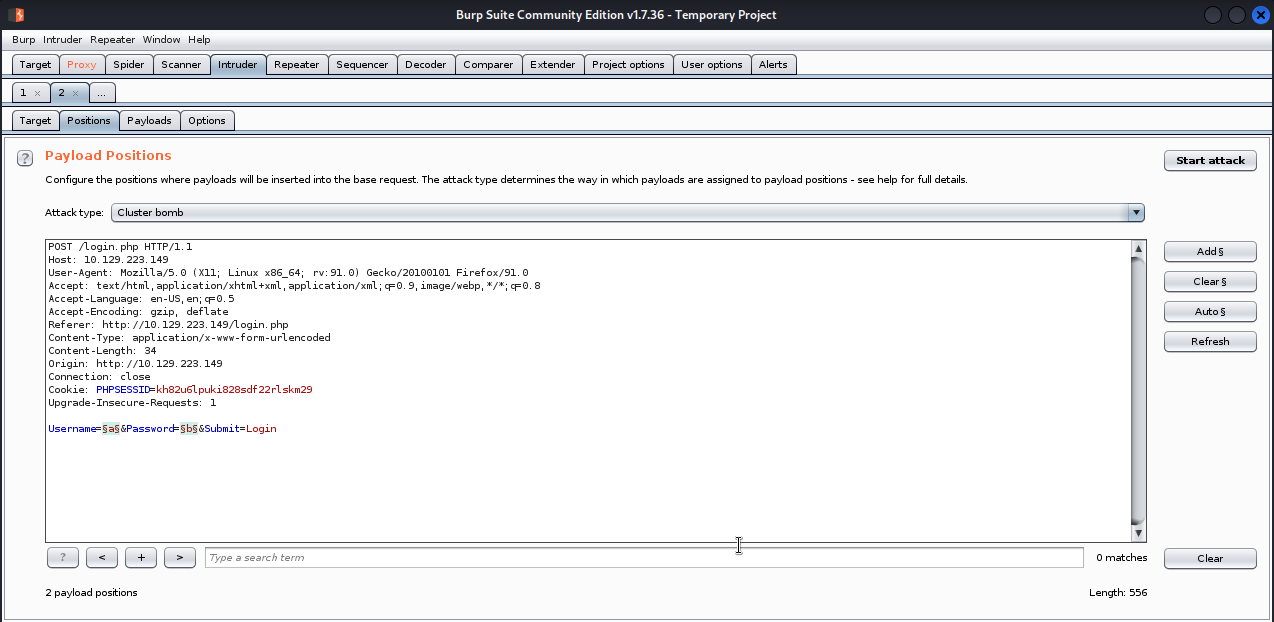
Capturado el trafico con burpsuite solo clic derecho y elegimos intruder





Tenemos que configurar las viñetas positions, paylodads y options.

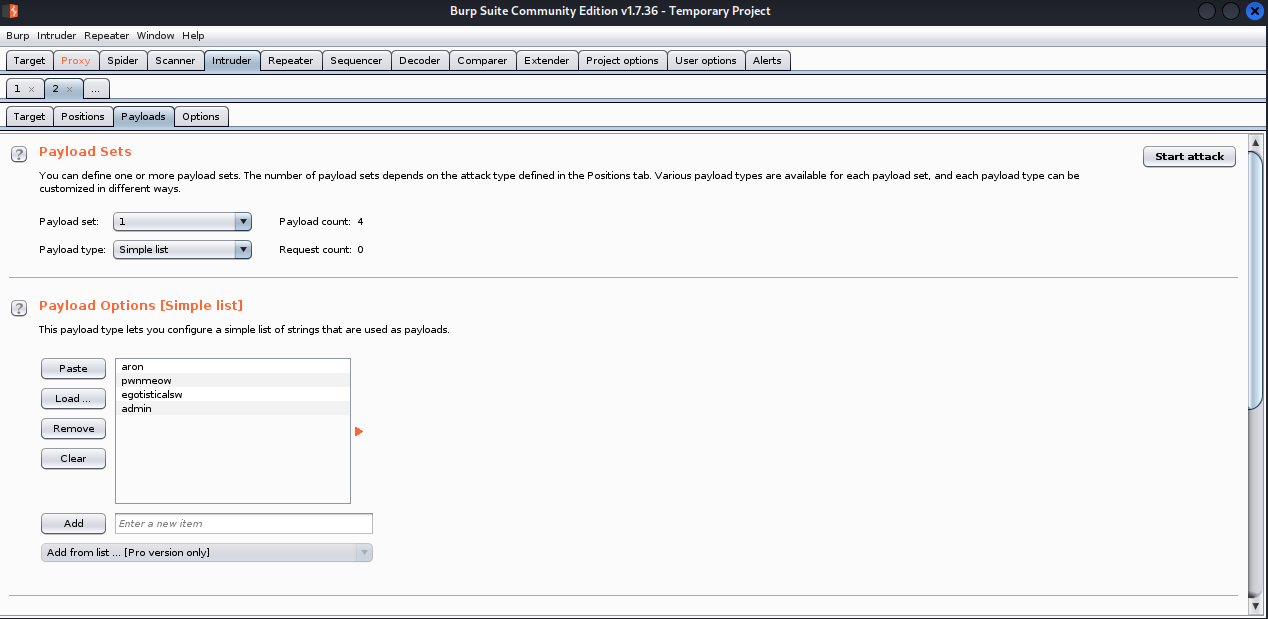
Positions:



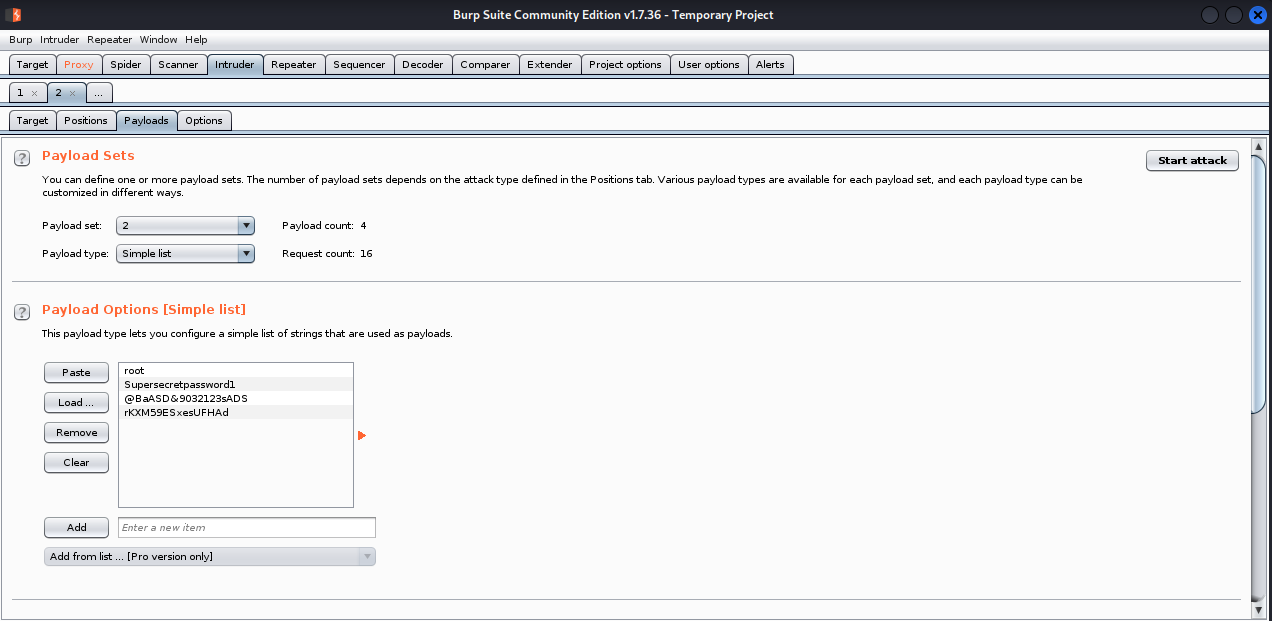
Elegimos el tipo de ataque cluster clumb podemos darle al botón clear para que nos limpie toda selección y agregamos add a las variables que escribimos en los textbox de la pagina que seria “a” en username y “b” en password al agregar add ambos lados de la palabra deben tener el símbolo $

Payloads:

En esta sección colocaremos las listas descargadas en pasos anteriores

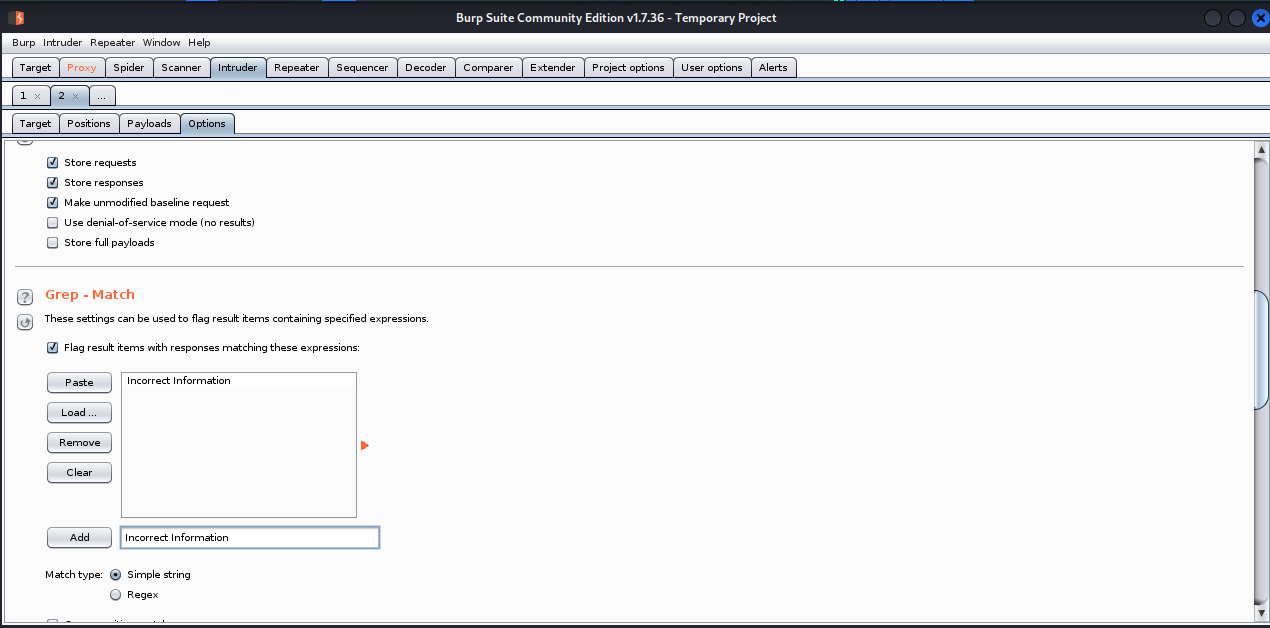


En payload 1 en load adjuntamos la lista de usuarios, en el payload 2 adjuntamos la lista de passwords



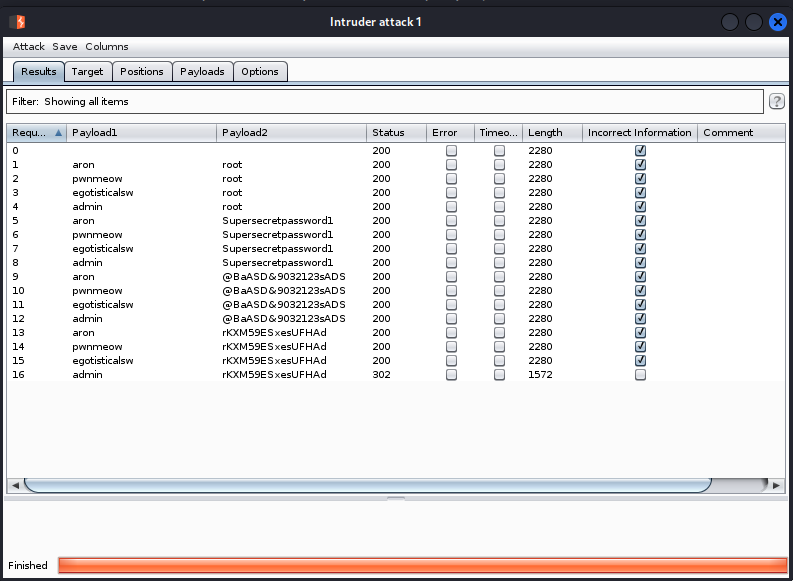
Options

Buscamos las opciones de grep Match y borramos toda la lista que sale por default y agregamos el texto que nos salia cuando colocamos mal las credenciales **Incorrect Information**



Damos en start Attack

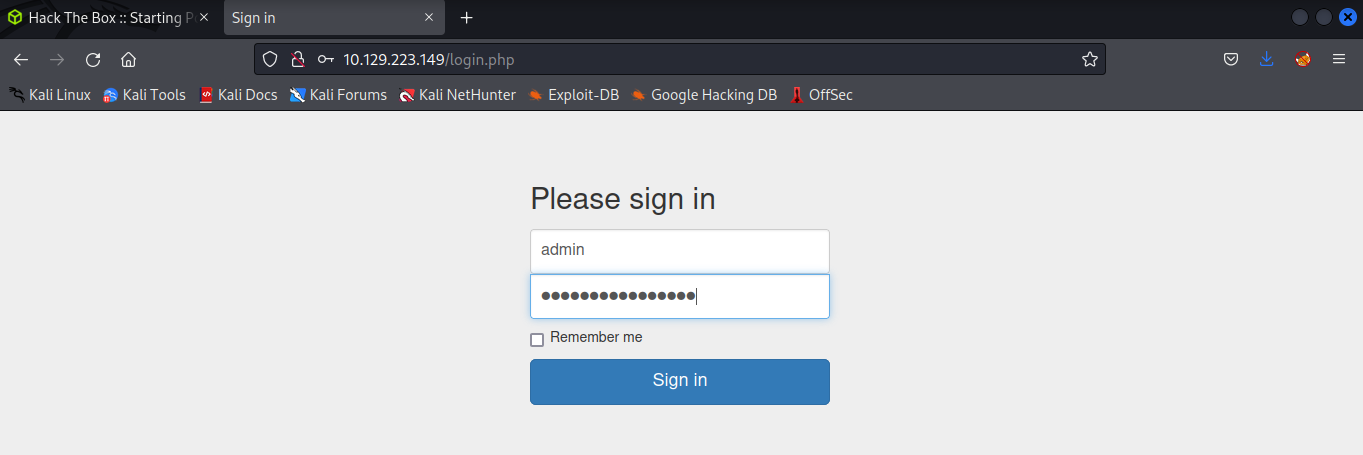
Nos saldra un cuadro con todas las posibles combinaciones y la combinación donde no salga con el checkbox activado de incorrect information esa serán las credenciales de la pagina, la cual tenemos que ir a probar al navegador

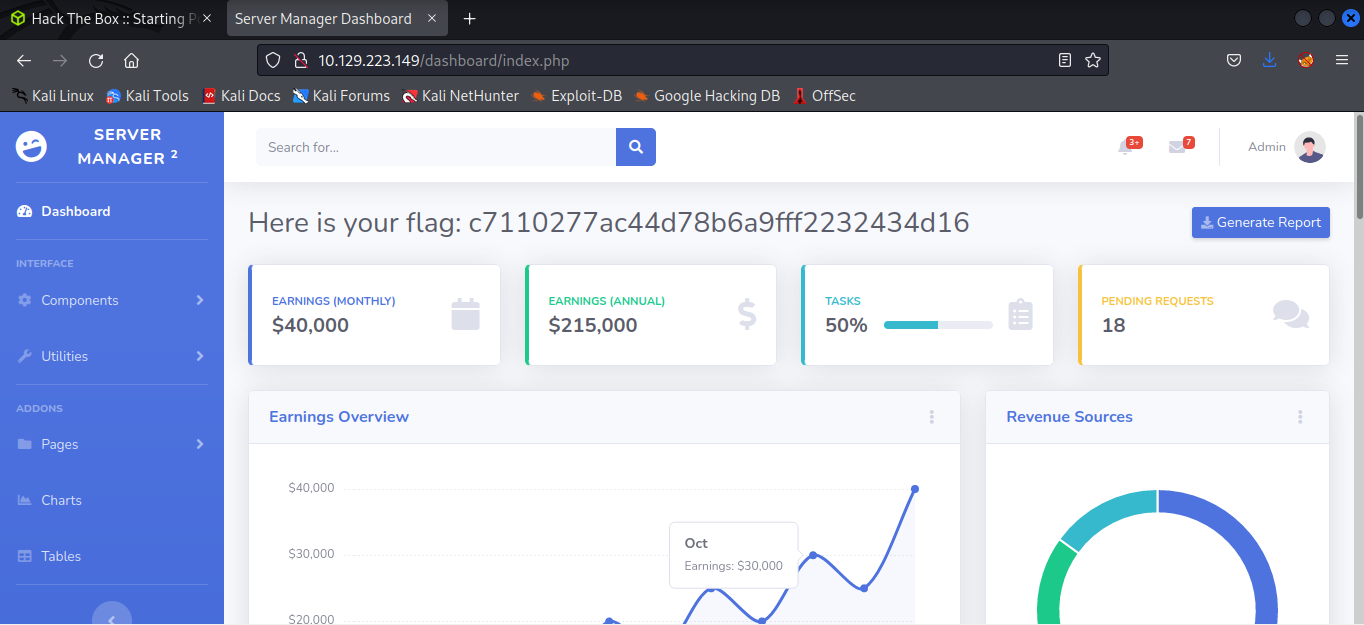


Username: admin

Password: rKXM59ESxesUFHAd

Desactivamos foxy proxy para trabajar normalmente





Bandera: c7110277ac44d78b6a9fff2232434d16