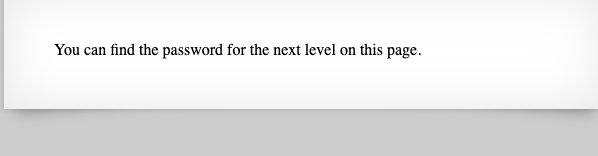
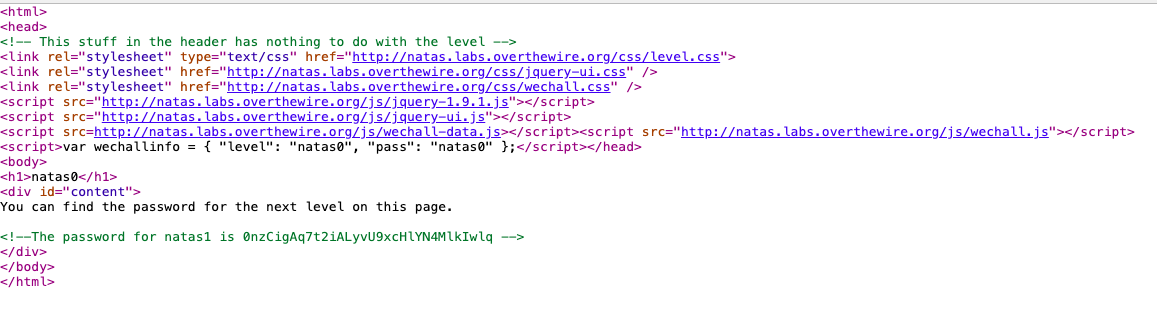
**OverTheWire : NATAS**

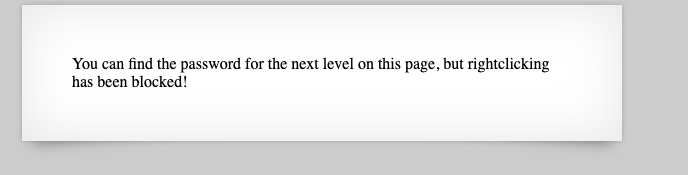
**Natas 0:** metemos natas0 de user y de contraseña tal y como se nos indica en la URL y nos sale un cartel



Le damos click derecho a la página y a inspeccionar y nos sale la contraseña del siguiente nivel : 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq



**Natas lvl 0-1:** Al meter el user Natas1 y la contraseña 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq nos sale un cartel:

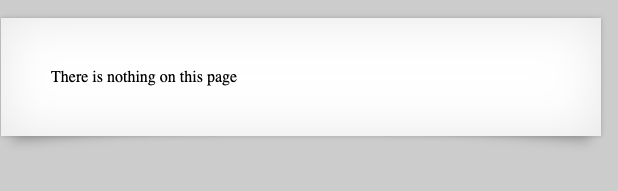


Usando cmd + option + U en el mac, se abre la pantalla del código de fuente y vemos la contraseña:

The password for natas2 is TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI



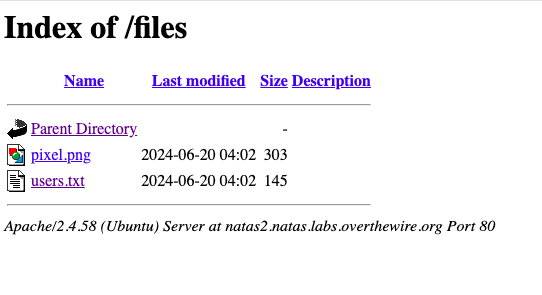
**Natas 1-2:** Usamos el user natas2 y la contraseña TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI y llegamos a la siguiente pantalla:



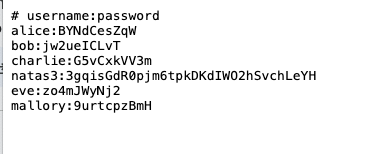
Abrimos inspeccionar pagina



a simple vista no hay ninguna contraseña pero si ponemos /files al final de la URL si nos sale algo

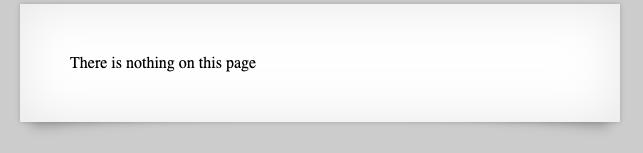


si entramos dentro de users.txt



la contraseña es : 3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH

**Natas 2-3:**

****

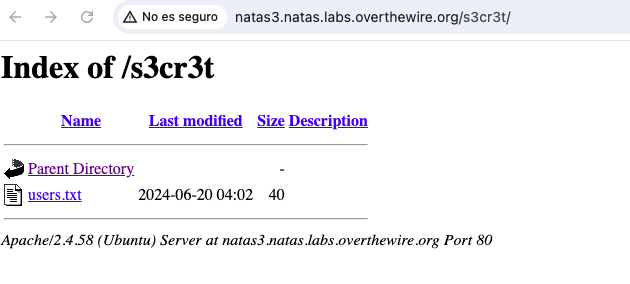
****

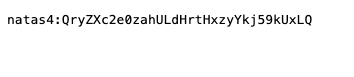
"Ni siquiera Google lo encontrará esta vez..." es nuestra pista aquí. Los archivos a los que se refiere son los de robots.txt.

Añadimos al final de la URL /robots.txt

****

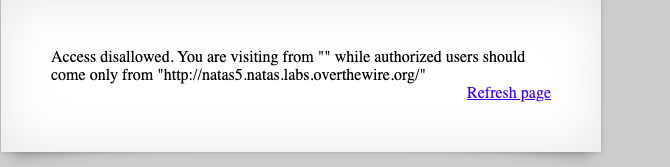
Parece que el archivo robots.txt está configurado para evitar que los rastreadores encuentren el directorio /s3cr3t/. Para acceder a este directorio, modificamos la URL de la siguiente manera:<http://natas3.natas.labs.overthewire.org/s3cr3t/>





La contraseña de natas4 es :QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

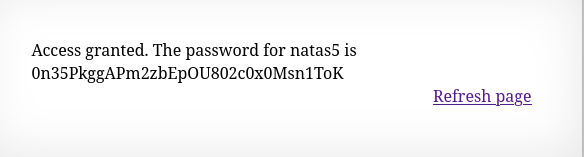
**Natas3-4:**

****

interceptamos con burpsuite

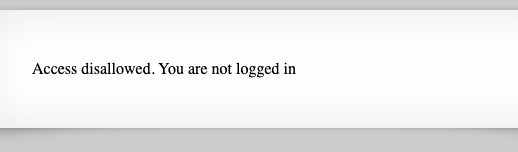


le damos a forward y refresh page entonces nos sale el apartado referer con el enlace web, cambiamos el natas4 por natas5 y forward otra vez.

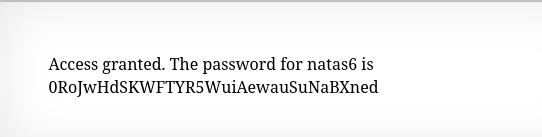


0n35PkggAPm2zbEpOU802c0x0Msn1ToK

**Natas4-5:**

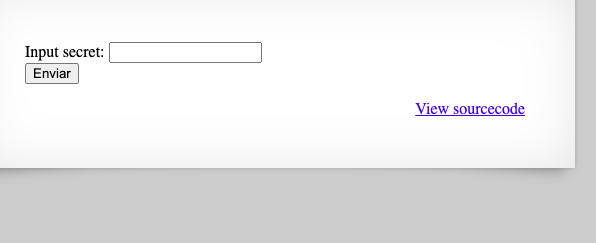


interceptamos con burpsuite y donde pone loggedin=0 lo cambiamos por loggedin=1 pulsamos forward y nos sale ya



0RoJwHdSKWFTYR5WuiAewauSuNaBXned

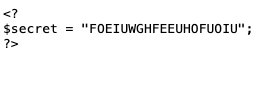
**Natas6-7:**

****

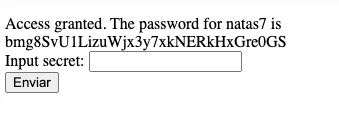
si pulsamos view sourcecode

****

Parece que PHP está incluyendo un enlace a un archivo almacenado en la página web /includes/secret.inc. Vamos a añadir eso al final de nuestra URL, así: <http://natas6.natas.labs.overthewire.org/includes/secret.inc>. Deberíamos llegar a una página en blanco, así que vamos a 'Ver el código fuente de la página.’



introducimos este código en la página donde te pide un codigo



bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

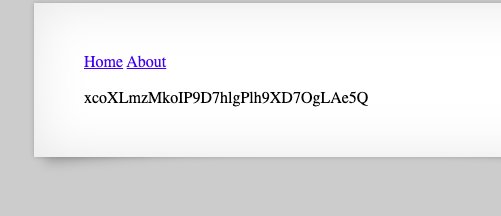
**Natas 6-7:**



En este nivel parece que se nos proporcionan 2 enlaces, "Home" y "About". Vamos a "Ver el código fuente de la página" y ver si podemos encontrar algo.



La URL debería lucir así: <http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas_webpass/natas8>



xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

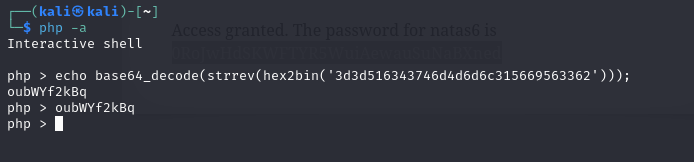
**Natas 7-8:**



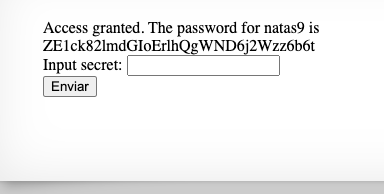


Parece que el código secreto que necesitamos está codificado. Revisando el código PHP, podemos ver que el 'secreto' ingresado se convierte de binario a hexadecimal, se invierte y luego se codifica en base64.

Para obtener el 'secreto', necesitamos ingeniería inversa. Comencemos abriendo la consola y ejecutando PHP con php -a. Podemos obtener la clave secreta desde la clave codificada decodificando en base64, invirtiendo la cadena y convirtiendo el hexadecimal de vuelta a binario.



meteremos ese código y veremos si sale o no la contraseña del siguiente natas



ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t

**Natas8-9:**



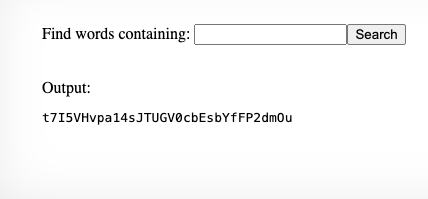


Por la forma en que se está utilizando 'key' en el script PHP, probablemente podamos insertar código arbitrario: si escribimos la palabra 'password', entonces el comando passthru en el script PHP se verá así: grep -i password dictionary.txt. Viendo cómo 'key' está encapsulado entre comillas y no hay filtro de entrada, podemos asumir que podemos ingresar caracteres especiales.

Podemos usar el separador de comandos “;” que nos permitirá ejecutar 2 comandos en una línea. También utilizaremos el comando de comentario “#”, que comentará el resto del texto después del símbolo.

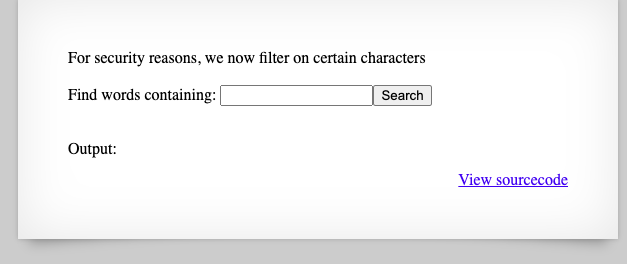
Así que, en el campo de entrada, escribiremos ; cat /etc/natas\_webpass/natas10 #, lo cual ejecutará el comando passthru de esta manera: grep -i ; cat /etc/natas\_webpass/natas10 #, comentando y omitiendo dictionary.txt.

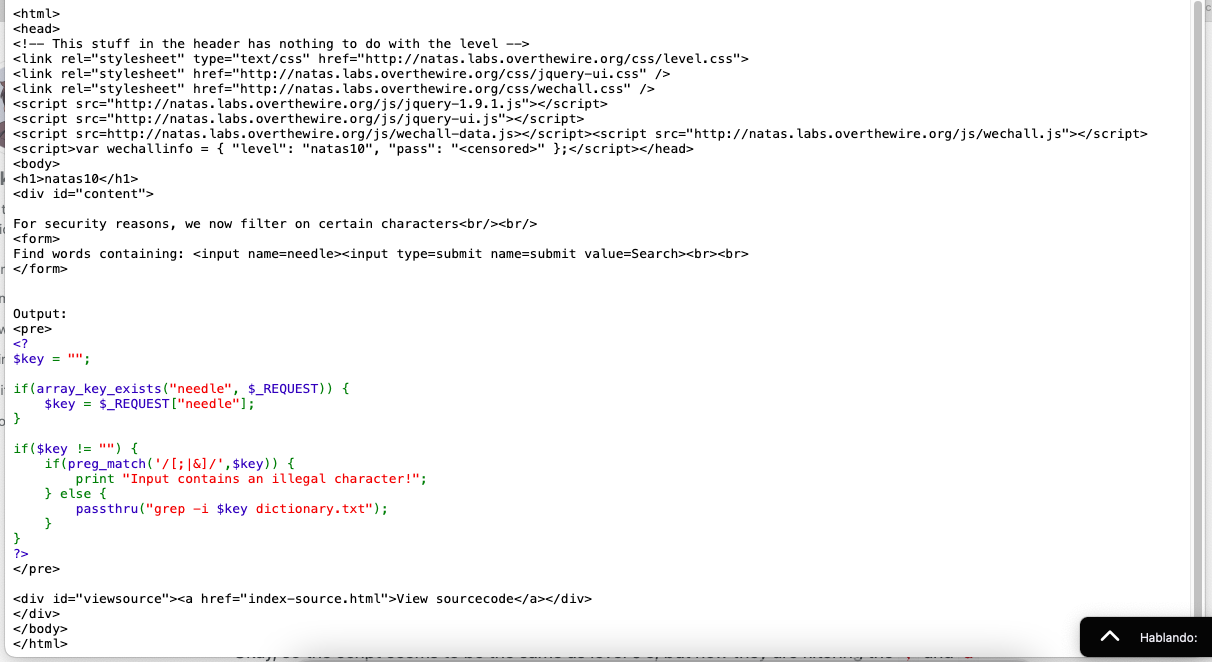




t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu

**Natas9-10**

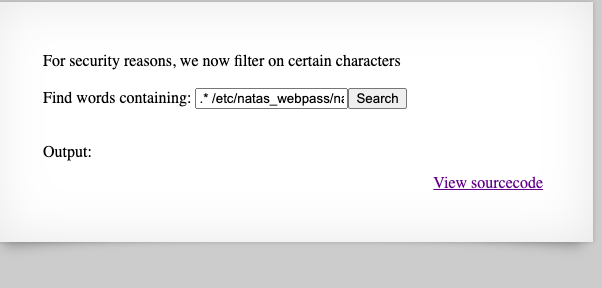
****

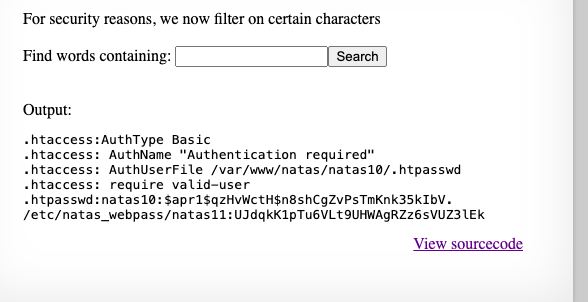
****

Vale, parece que el script es similar al de nivel 9, pero ahora están filtrando los comandos ; y &.

Parece que aún no han corregido la forma en que 'key' almacena la entrada. Así que podemos explotar esto de la misma manera que hicimos en el nivel 9, pero esta vez solo usando expresiones regulares.

Vamos a ingresar .\* /etc/natas\_webpass/natas11 # dentro de la consulta. Al ingresar .\* le decimos a grep que busque todo, ignorando mayúsculas y minúsculas, y que coincida con etc/natas\_webpass/natas11. El comando # comenta dictionary.txt, evitando que ocurran errores.





htpasswd:natas10:$apr1$qzHvWctH$n8shCgZvPsTmKnk35kIbV.

/etc/natas\_webpass/natas11:UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk