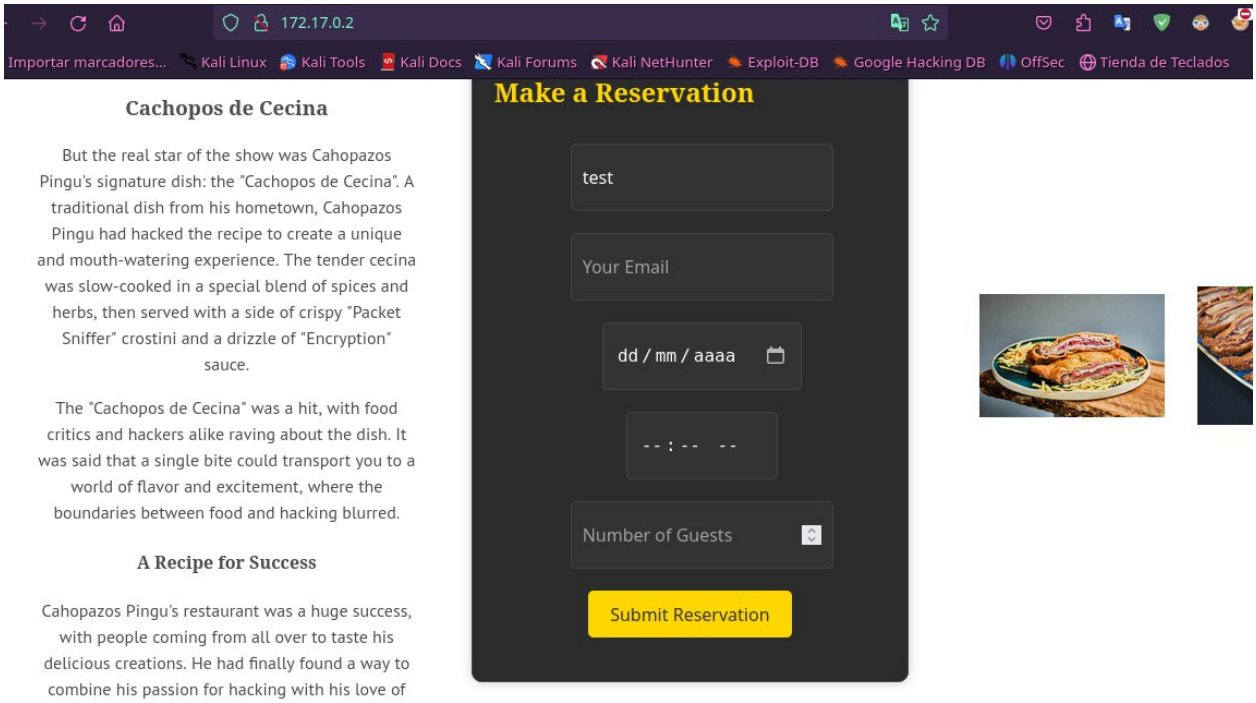
Máquina “Cachopo” de la plataforma de aprendizaje gratuito DockerLabs de dificultad media.

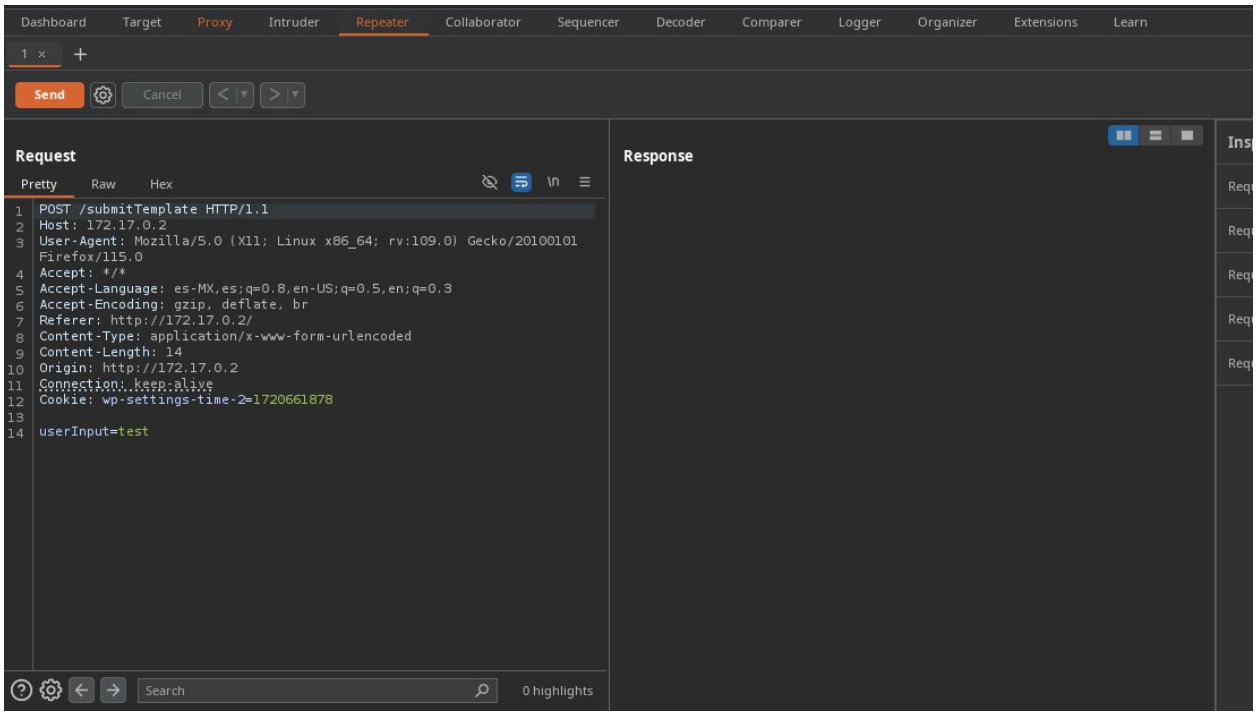
```
# Nmap 7.94SVN scan initiated Thu Aug  1 06:15:28 2024 as: nmap -p22,80,3000 -sCV -oN targeted 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000056s latency).

PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 7b:98:d4:e7:ec:50:0b:b2:3a:21:76:2c:45:95:23:61 (ECDSA)
|_  256 5d:15:2b:28:ec:67:7e:78:3c:16:12:65:2f:59:d4:88 (ED25519)
80/tcp   open   http    Werkzeug/3.0.3 Python/3.12.3
|_http-title: Cahopos4-4ll
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.3 Python/3.12.3
|     Date: Thu, 01 Aug 2024 11:15:36 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 9332
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width initial-scale=1.0">
|     <link rel="stylesheet" href="/static/css/style.css">
|     <title>Cahopos4-4ll</title>
|     </head>
|     <header>
|     <nav>
|     <h2><a href="/" id="logo">DockerLabs</a></h2>
|     <button class="nav-button fa fa-bars"></button>
|     <div>
|     <!-- <ul> -->
|     <ul>
```

Se realizó un escaneo de puertos y detectamos que los puertos 22 y 80 están habilitados. Esto sugiere que un servidor web está activo y que el servicio SSH (Secure Shell) está habilitado.



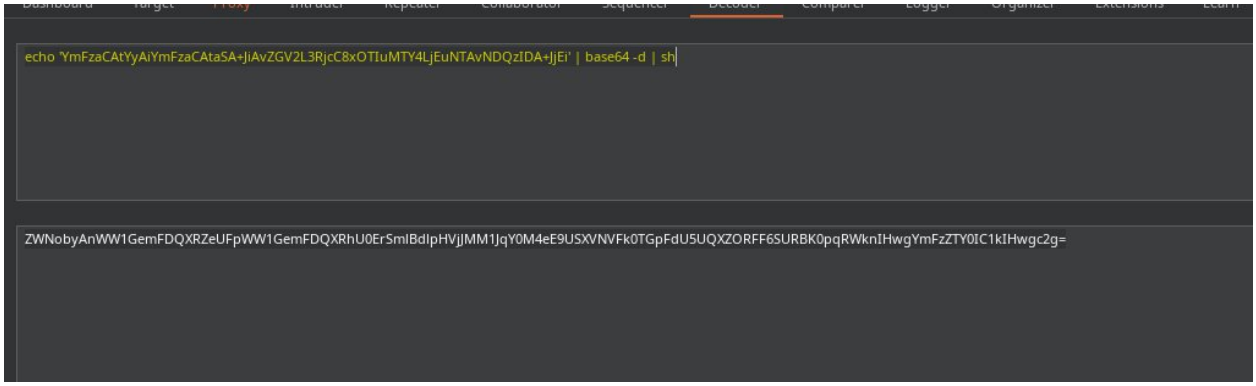

Hay un formulario para realizar la reservación, pero al analizarlo hemos observado que el único texto que se procesa es el del primer campo de texto a través de un método POST. Por lo tanto, vamos a interceptar la petición en Burp Suite para averiguar lo que está sucediendo dentro de la página.



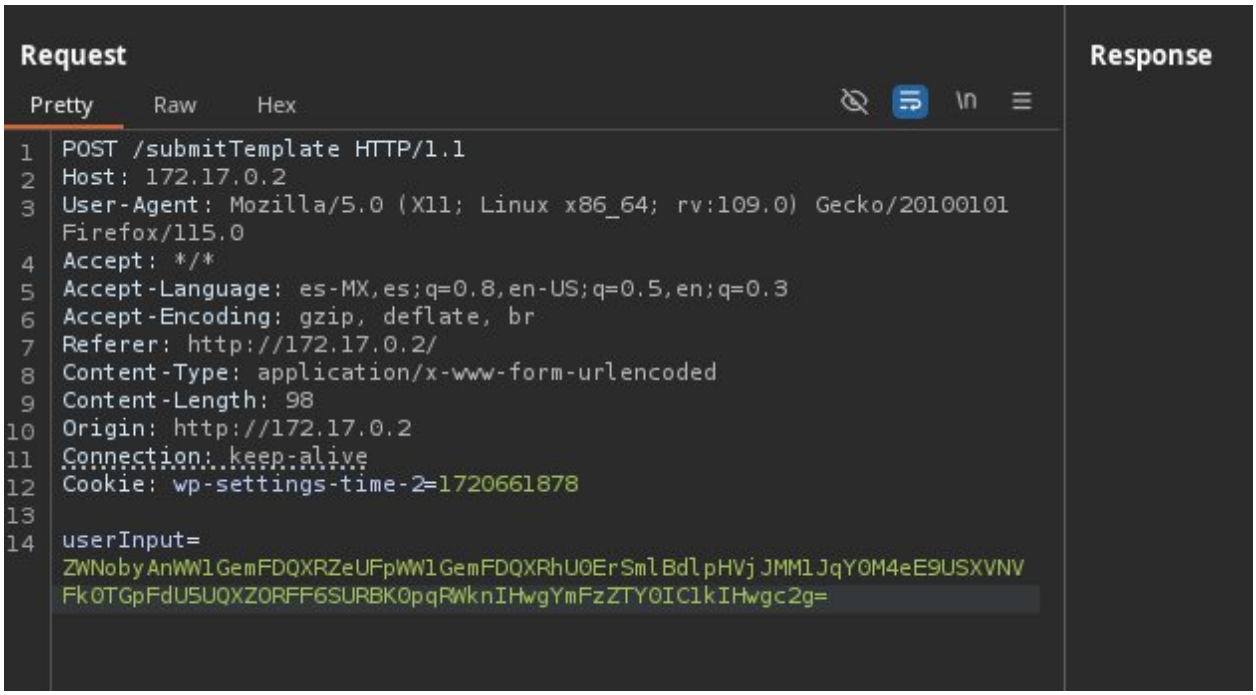

Mandamos la petición web al Repeater para modificar el UserInput y verificar si manipulando las variables encontramos alguna reacción que nos comunique con la máquina donde está alojada la página web.


Encapsulamos la reverse shell con bash -c y la almacenamos dentro de comillas dobles. Luego, en el decoder, la decodificamos con base64. Este procedimiento se siguió porque, según el análisis, esta máquina solo procesa información en base64.

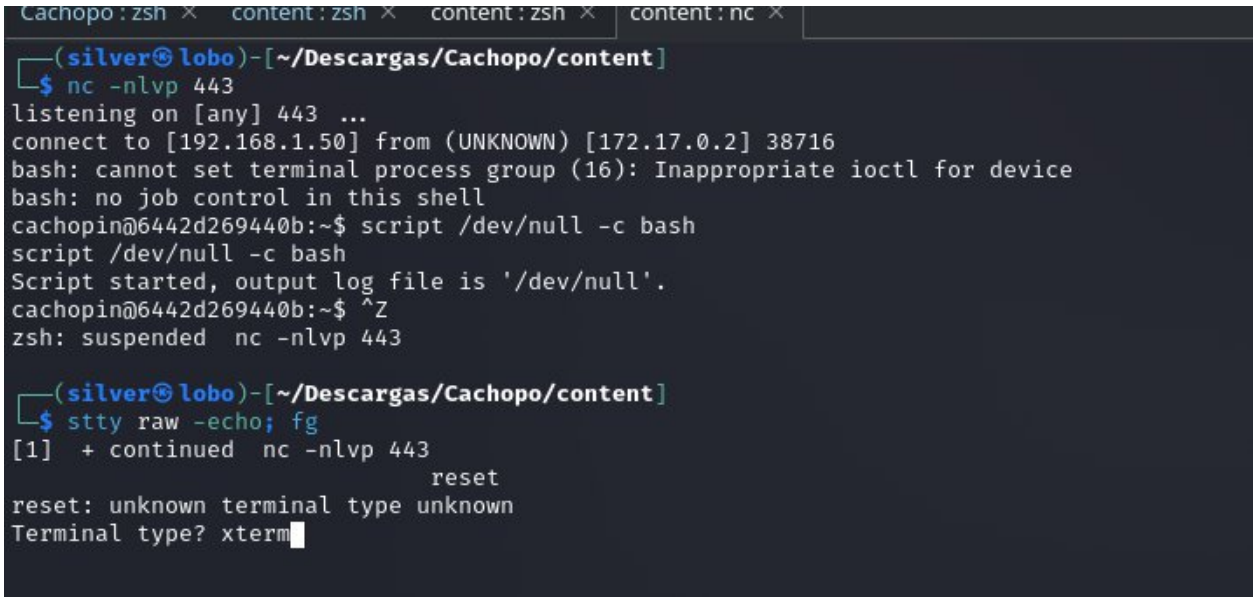

Preparamos el decoder para realizar la petición puesto que solo lee en base 64



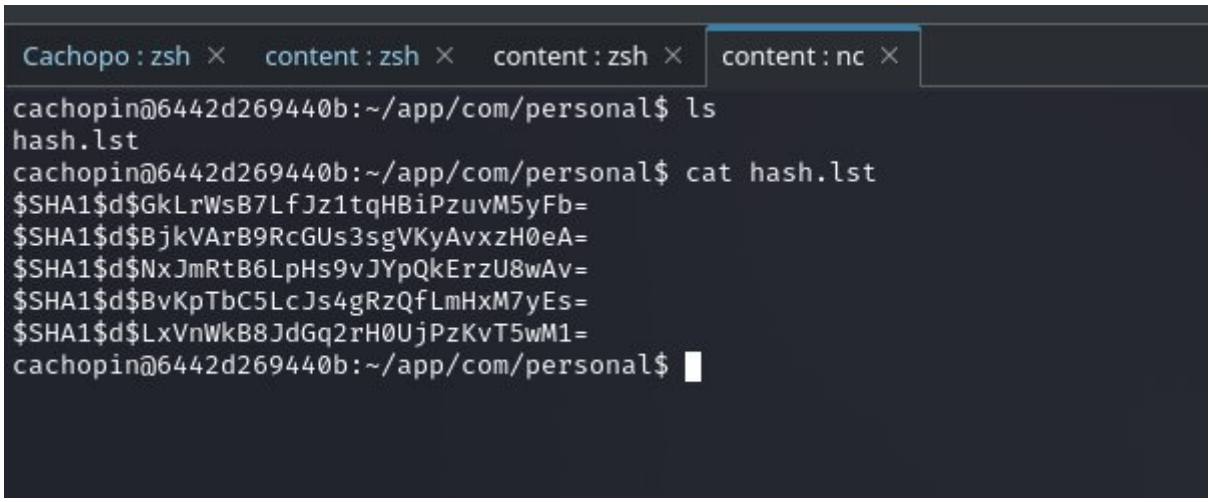

Recogemos toda la cadena y la pasamos en su totalidad todo en base64



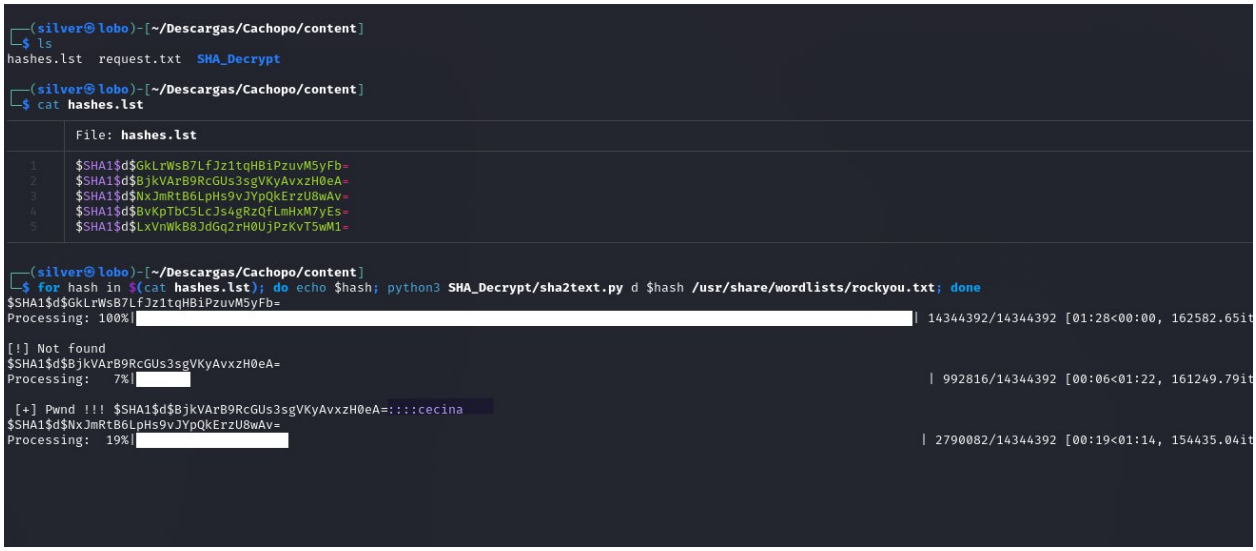

Realizamos la petición.



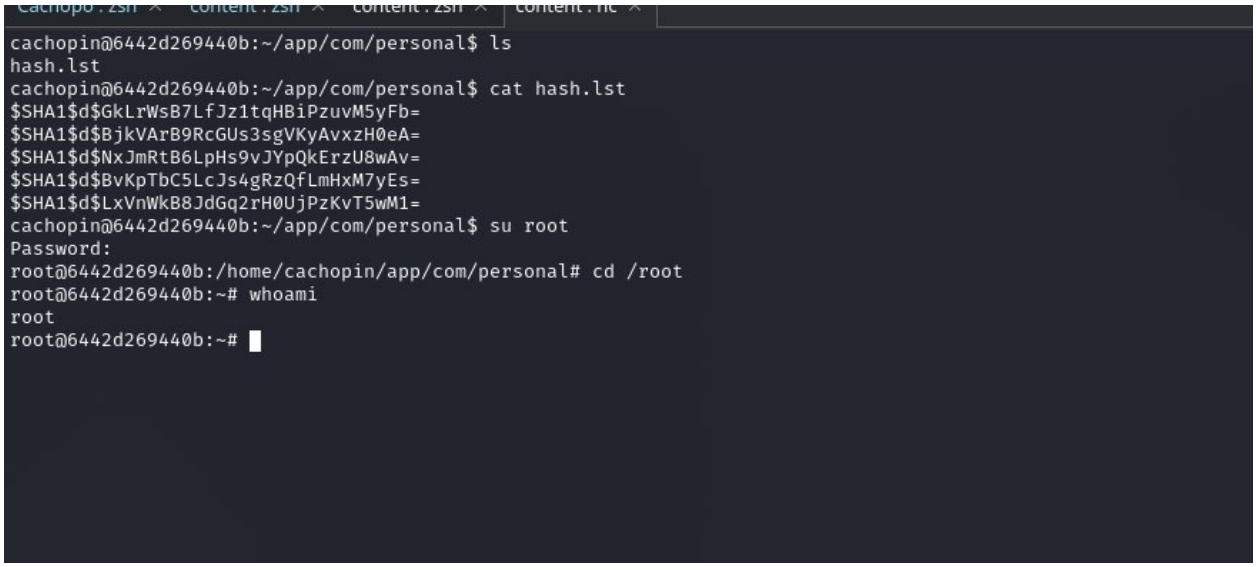

Tenemos contacto con la máquina, a lo que hacemos un tratamiento de la tty.




Encontramos esta lista de posibles contraseñas futuras, por lo que es necesario realizar un ataque de fuerza bruta para descifrar su contenido.



Utilizamos un script disponible en GitHub, cuyo propietario es PatxaSec, para obtener la contraseña, que en este caso es "cecina".




Entramos ahora como usuario root.