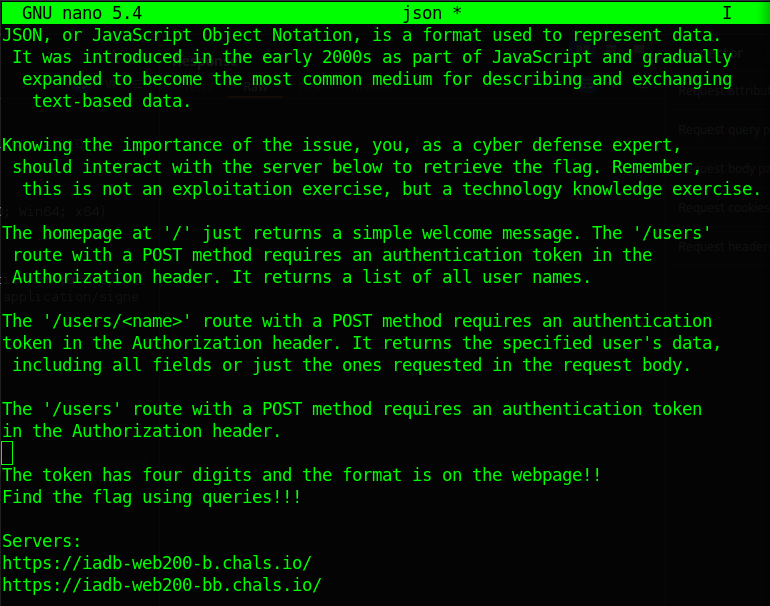
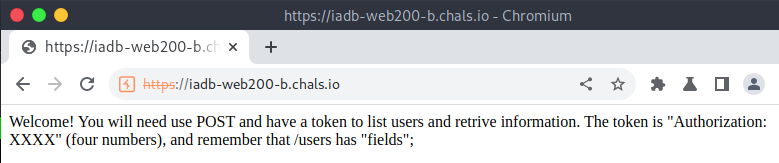
Inter-American Cyber Defense Challenge: JSON

Observamos el enunciado e ingresamos a la dirección mencionada.

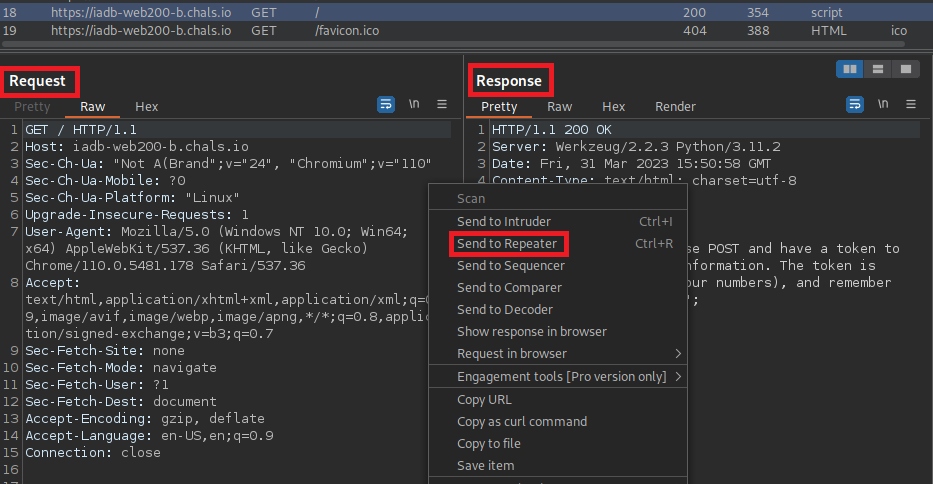


<https://iadb-web200-b.chals.io/>

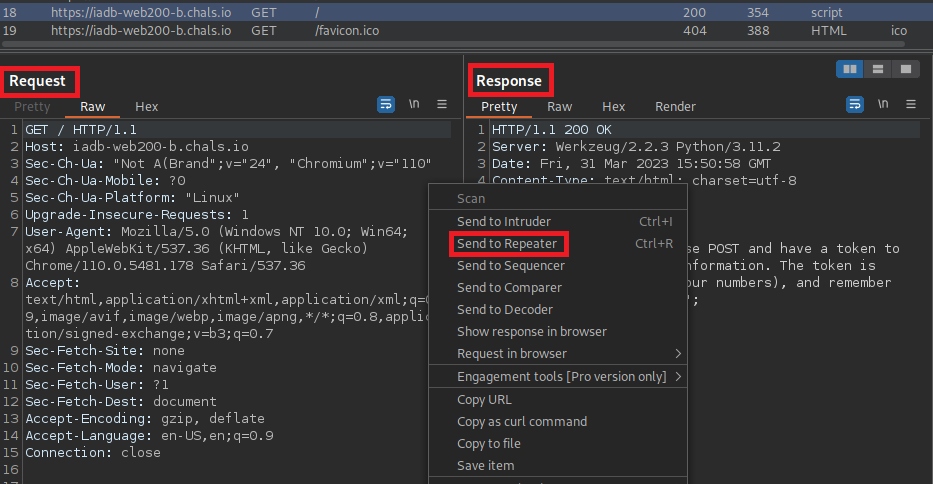


Obtenemos una respuesta del servidor que nos indica que usemos una petición POST, un token de 4 dígitos con una cabecera Authorization para poder observar el contenido del directorio /users

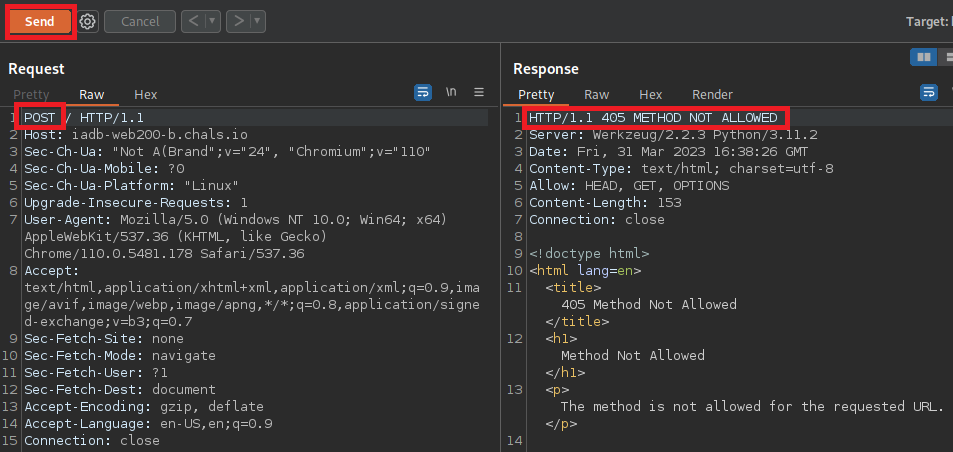
Llevamos esto a Burpsuit



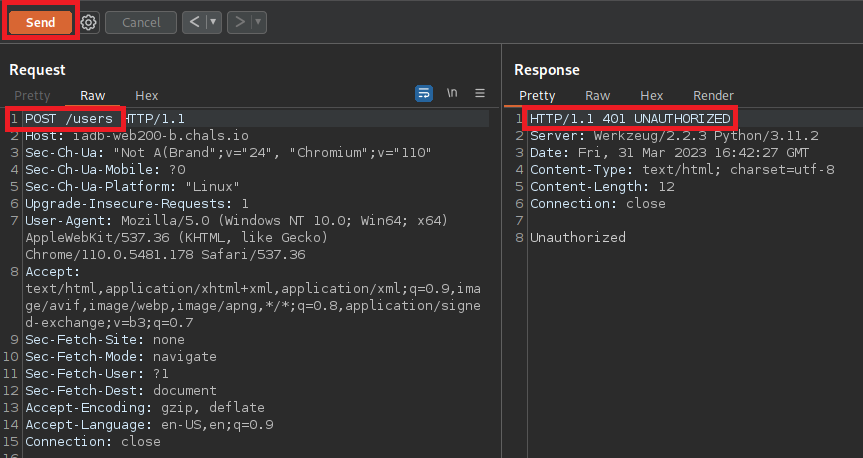
Capturamos la petición y la mandamos a repeater para poder modificarla antes de enviarla al servidor



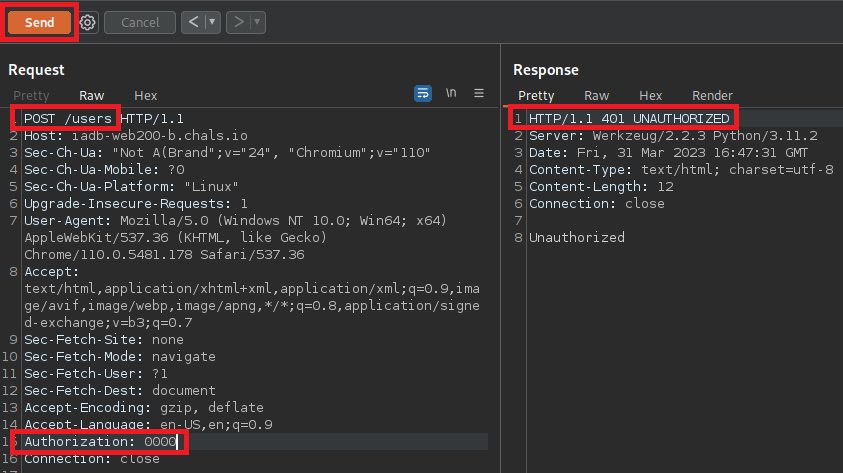
Una vez en repeater comenzaremos a agregar elementos para poder hacer querys y obtener información del servidor.



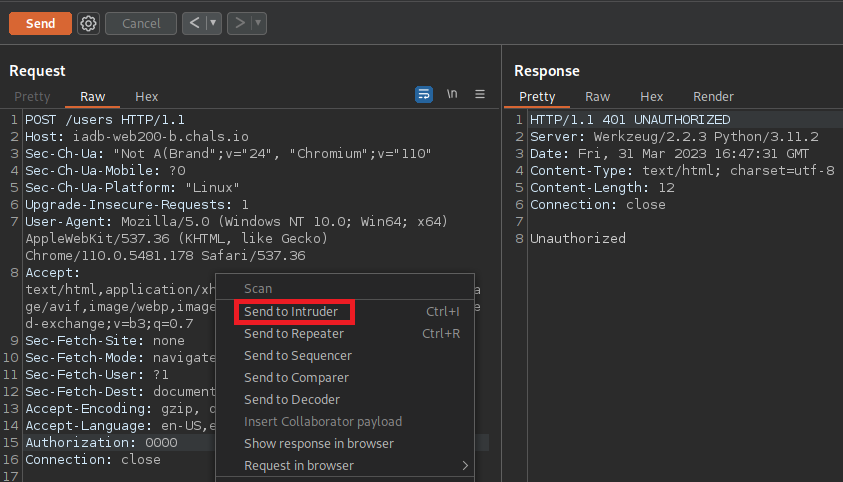
¨hacemos nuestro primer cambio a la petición y observamos como la respuesta del servidor es que el método POST no está permitido.

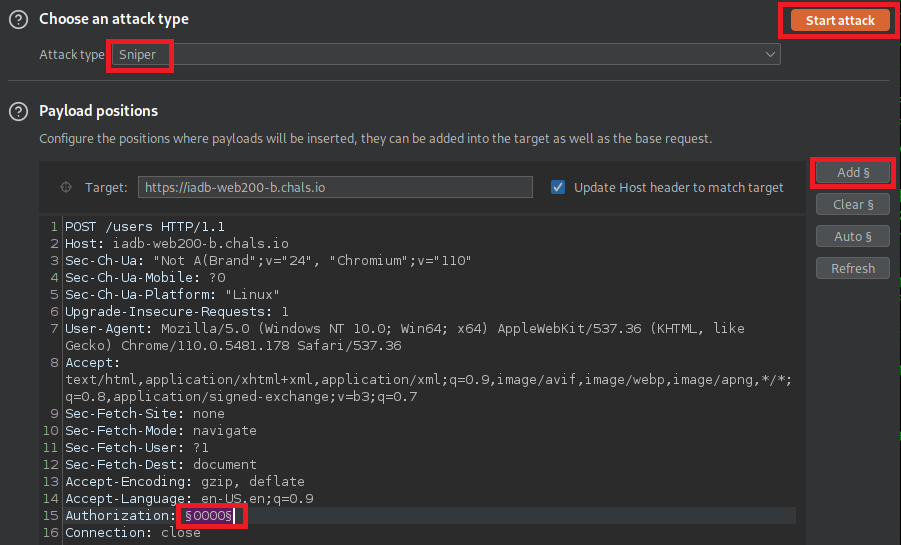


Agregamos el directorio users a nuestra petición y ahora la respuesta del servidor es que no tenemos autorización para ver el contenido del directorio.



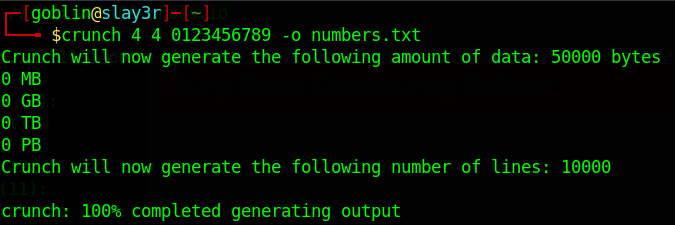
Agregamos la cabecera de autorización y la respuesta es obviamente la misma pero usaremos esto para aprovechar otra bondad de burpsuit enviando esta petición a intruder.

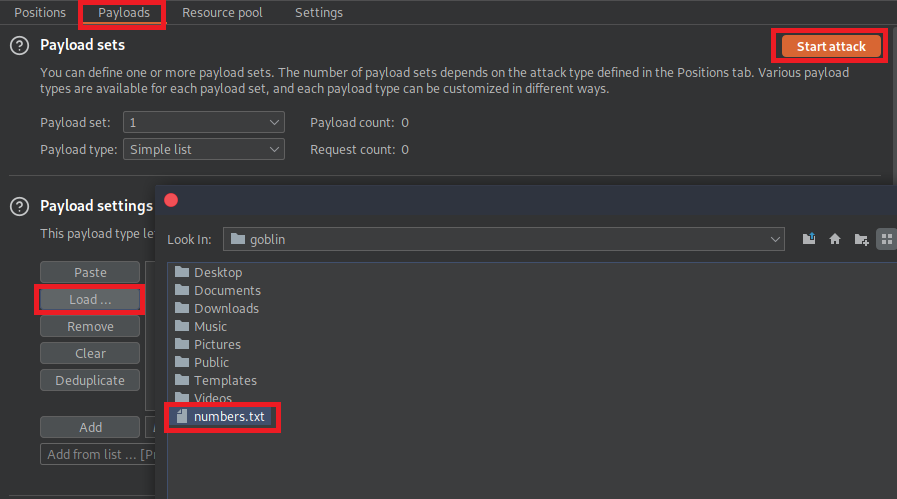




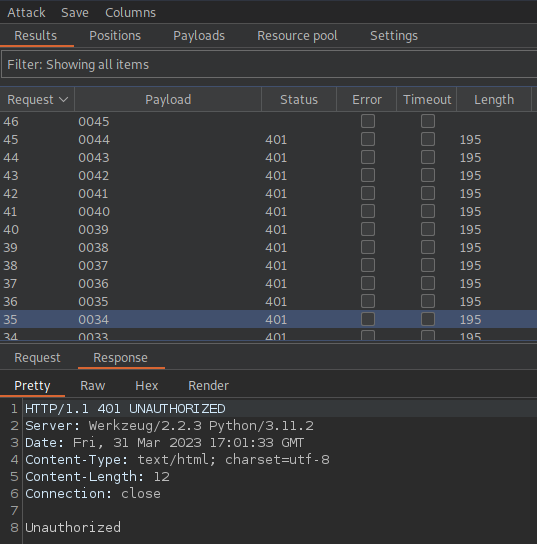
Una vez en el modulo intruder agregamos el valor que queremos atacar con fuerza bruta y como se trata solo de un valor lo dejaremos en el tipo de ataque Sniper.

Como sabemos que tenemos que probar 9999 posibilidades crearemos un diccionario con Crunch de 4 dígitos con números de 0 al 9 y le diremos que se guarde con el nombre number.txt

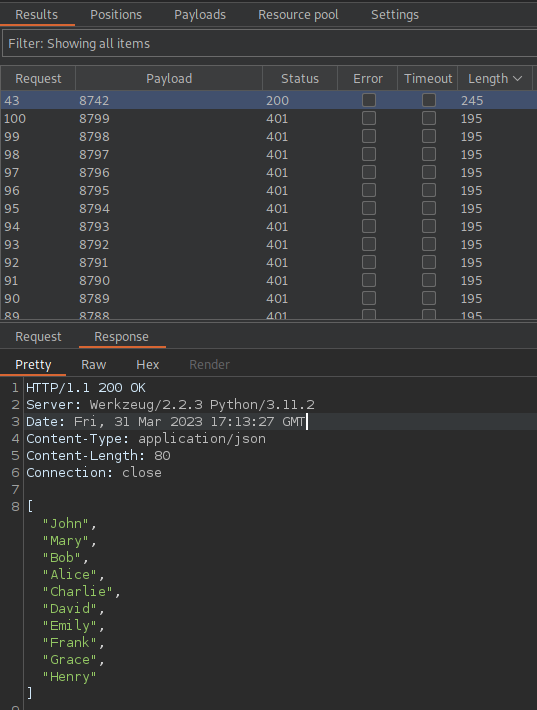




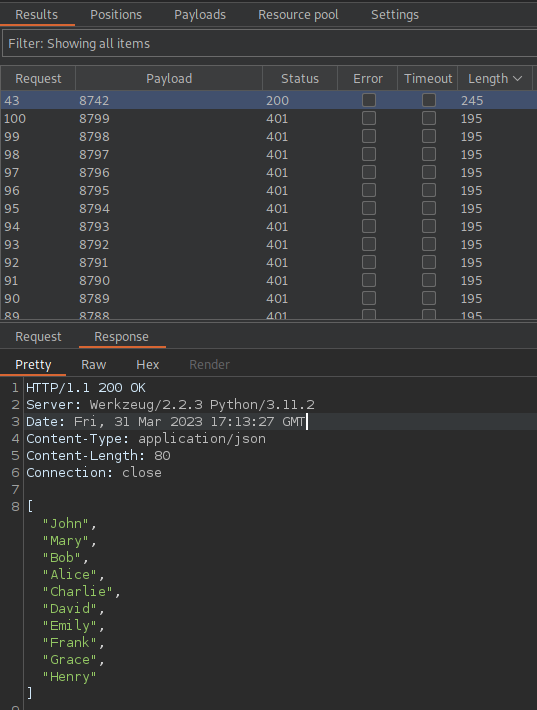
Vamos al sub modulo Payloads y cargamos nuestro diccionario una vez cargado presionamos el botón Start attack para comenzar.



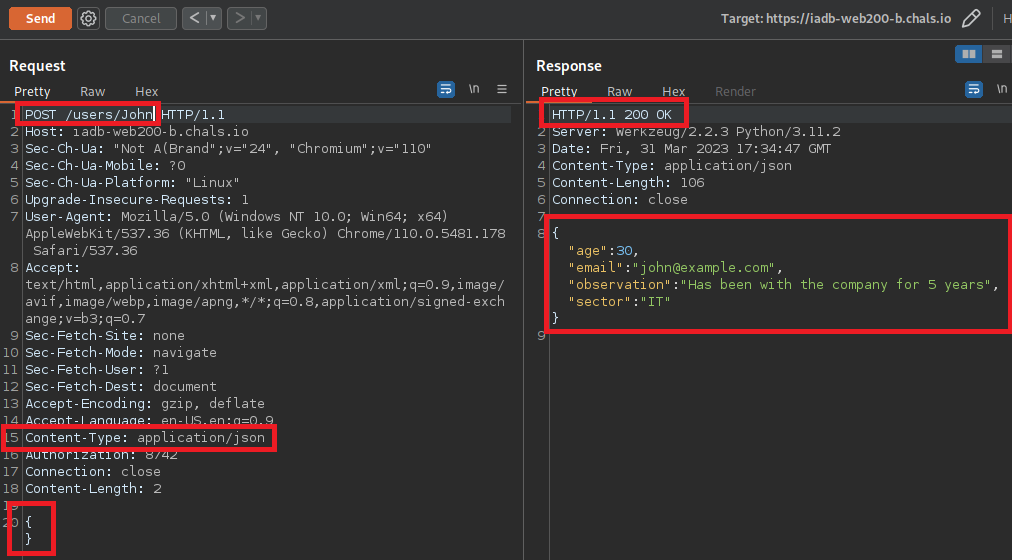
Podemos observar como las respuestas son inautorizadas, pero con paciencia lograremos dar con el número de token correcto.



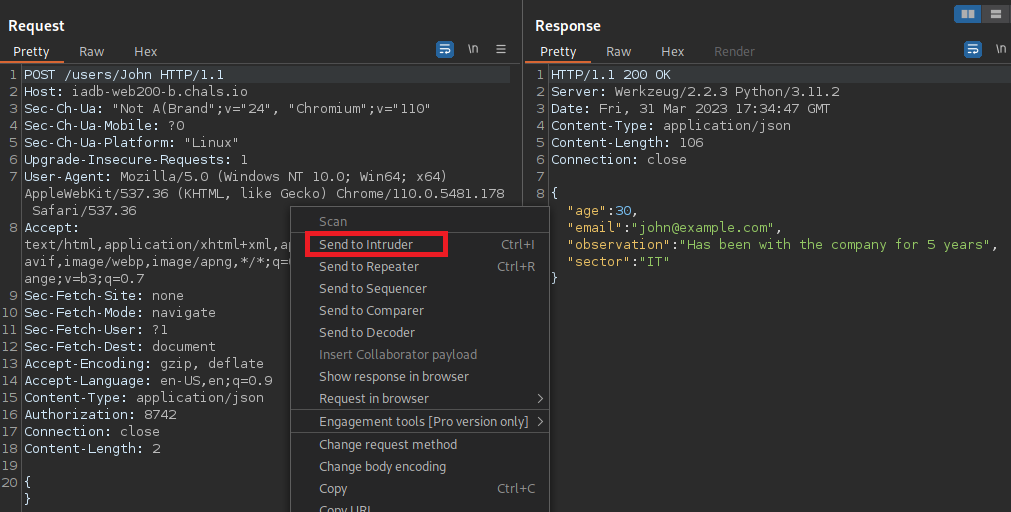
Para poder encontrar la petición aceptada ordenamos por el tamaño de la respuesta y nos damos cuenta que es la que buscamos por el código 200 que obtuvimos.

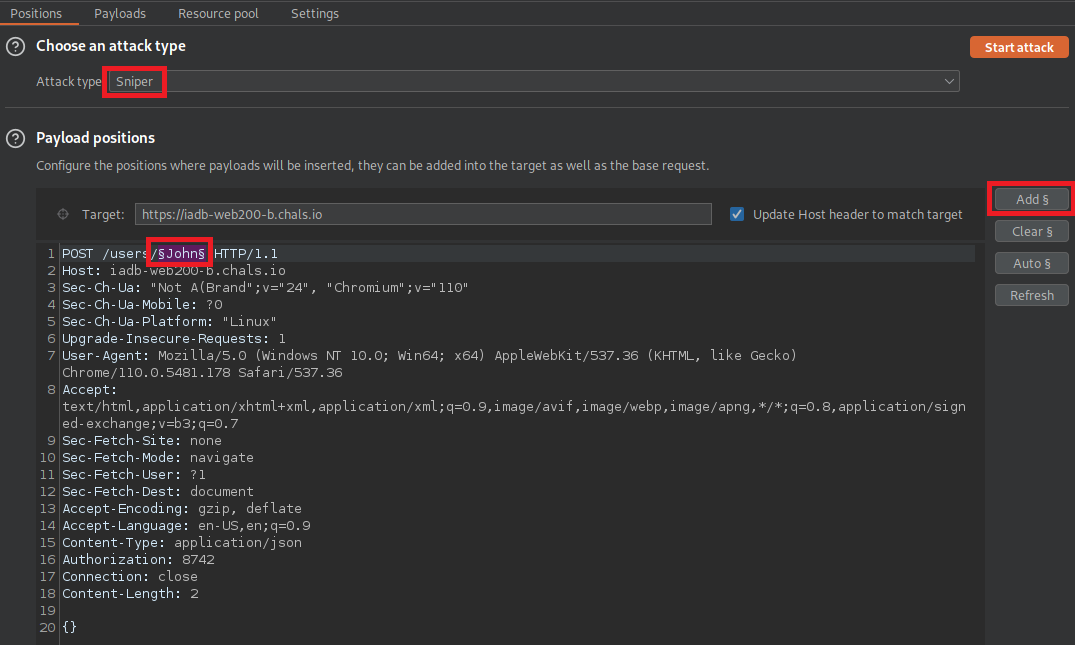


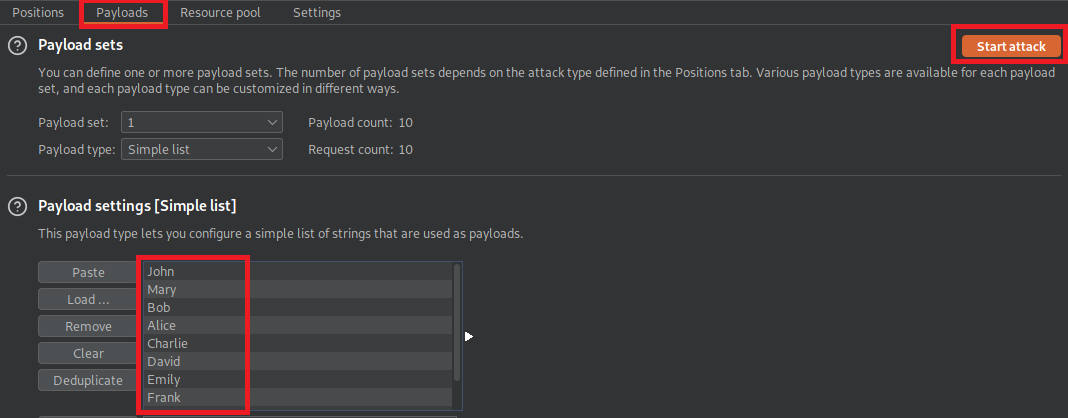
Observamos la respuesta y nos damos cuenta de que obtuvimos nombres de usuarios en un formato XML o JSON, cosa que no es necesario analizar demasiada por el nombre del reto.

Esta vez agregaremos el header Content-type con el valor application/json y al final pondremos dos llaves para invocar la informacion dentro de su propio formato.

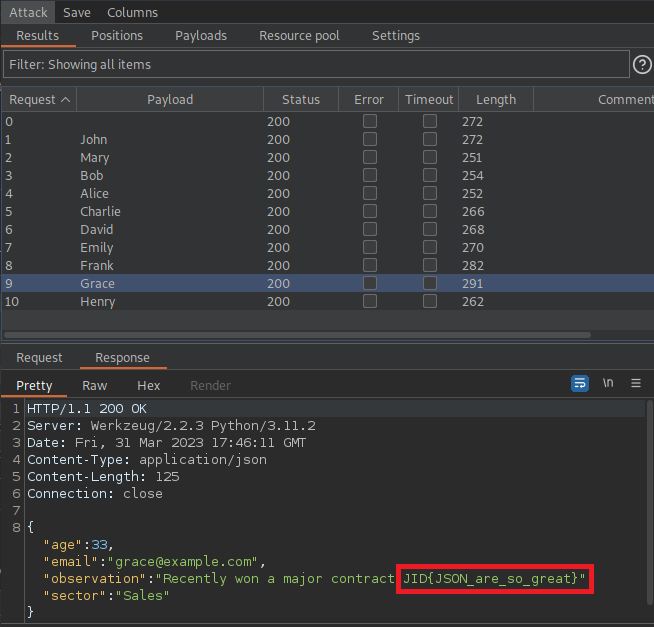
Obtenemos como respuesta del servidor con el usuario john, pero tenemos una lista de usuarios asi que otra vez aprovecharemos el modulo intruder.





Usaremos el campo donde está el usuario john para remplazar con el diccionario.

Usamos la lista de usuario que encontramos en la respuesta del servidor y dejamos al burpsuit hacer su trabajo.



Como todas las respuestas serán 200 hacemos la búsqueda manual y dentro de la data del usuario Grace observamos que se encuentra incrustada la flag.