Que hemos necesitado para hacer un ataque de proxy

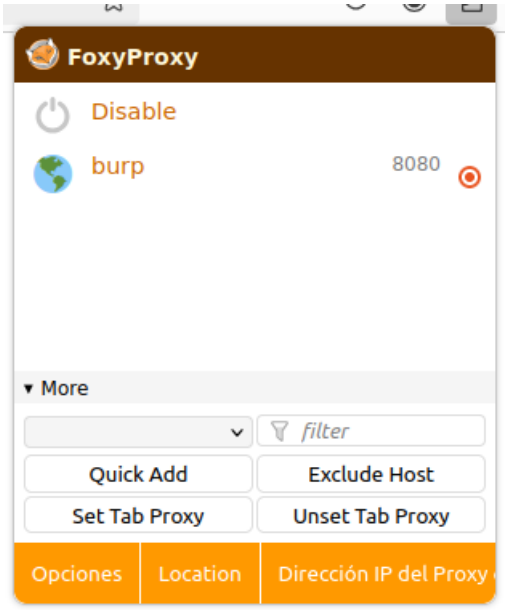
Burpsite

Foxyproxy

1º Configuramos foxyproxy con para que funciones con burp site

Extensiones → Opction

Después la encendemos



2. Pasamos a la aplicación de burtsite

Proxy→ encendemos la intercepccion

3. Analizados un paquete que sea relevante e importante y lo pasamos a intruder

4. Una vez en intruder podemos ver por ejemplo en este caso como se envia el usuario y la contraseña con un post

Request

Pretty Raw Hex

```
POST /login HTTP/1.1
Host: 10.0.1.51:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: http://10.0.1.51:3000/login.html
Content-Type: application/json
Content-Length: 47
Origin: http://10.0.1.51:3000
Connection: keep-alive
Priority: u=0

{
  "username":"usuario",
  "password":"contraseña"
}
```

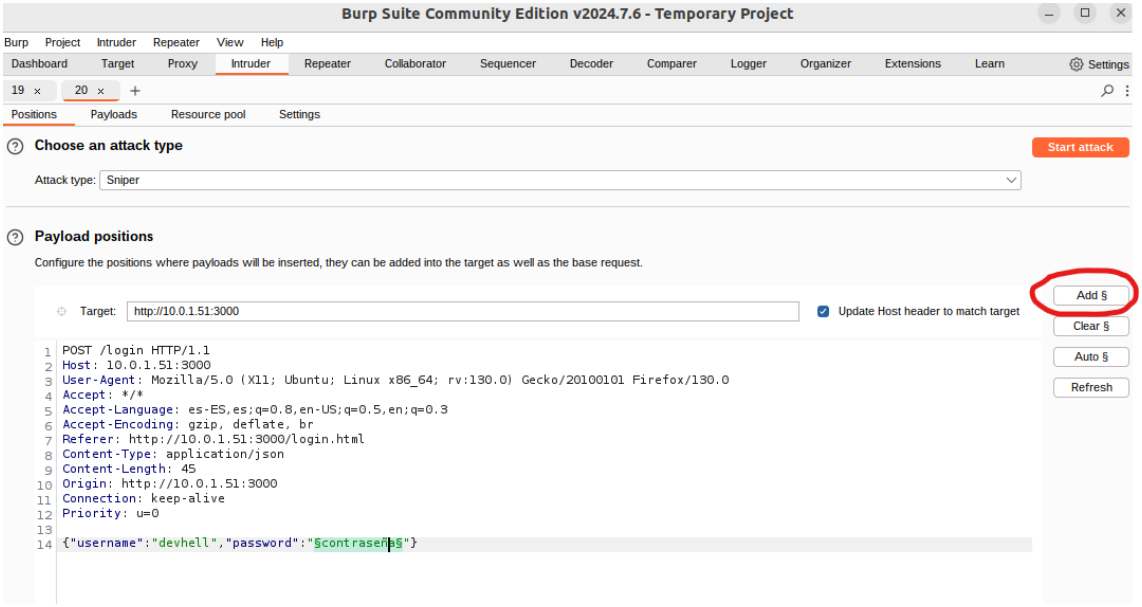
Response

Pretty Raw Hex Render

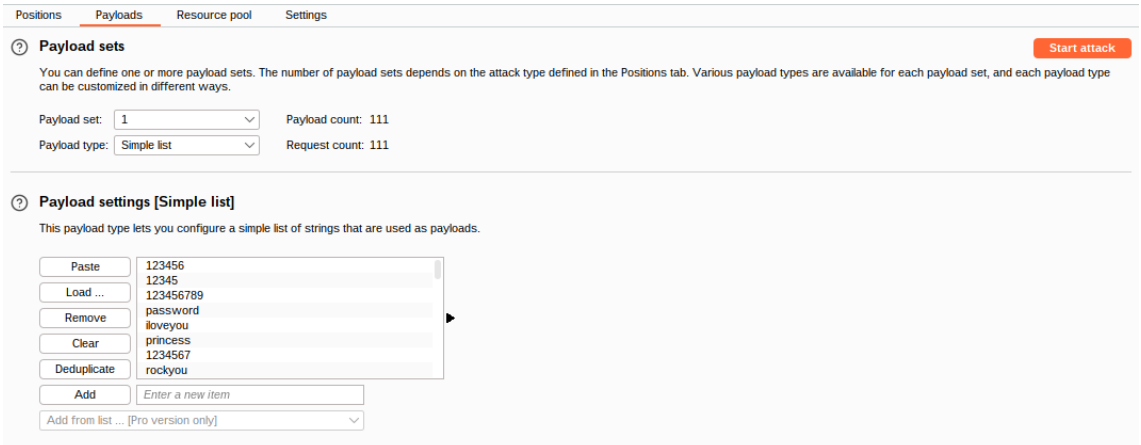
```
HTTP/1.1 404 Not Found
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 28
ETag: W/"1c-ZEVVcvtFhxKX/QUvVKqKxwGbbNA"
Date: Mon, 30 Sep 2024 15:42:07 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "message":"User not found"
}
```

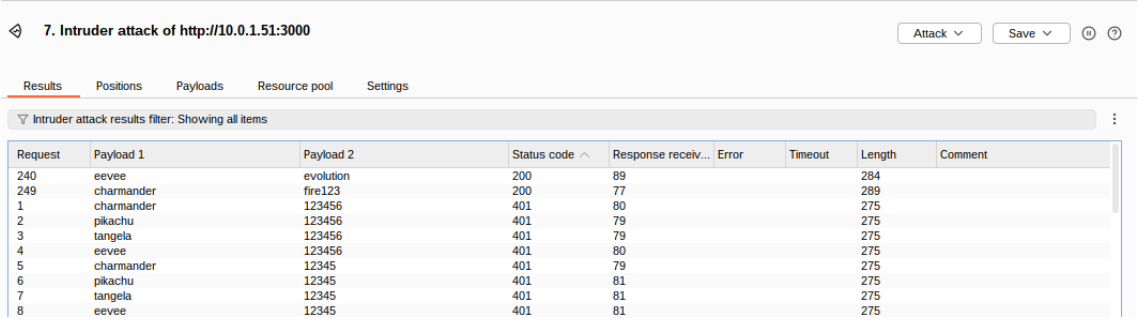
5. Como ya conocemos un usuario podemos utilizar una lista para saber su contraseña



Añadimos la lista para probar contraseña



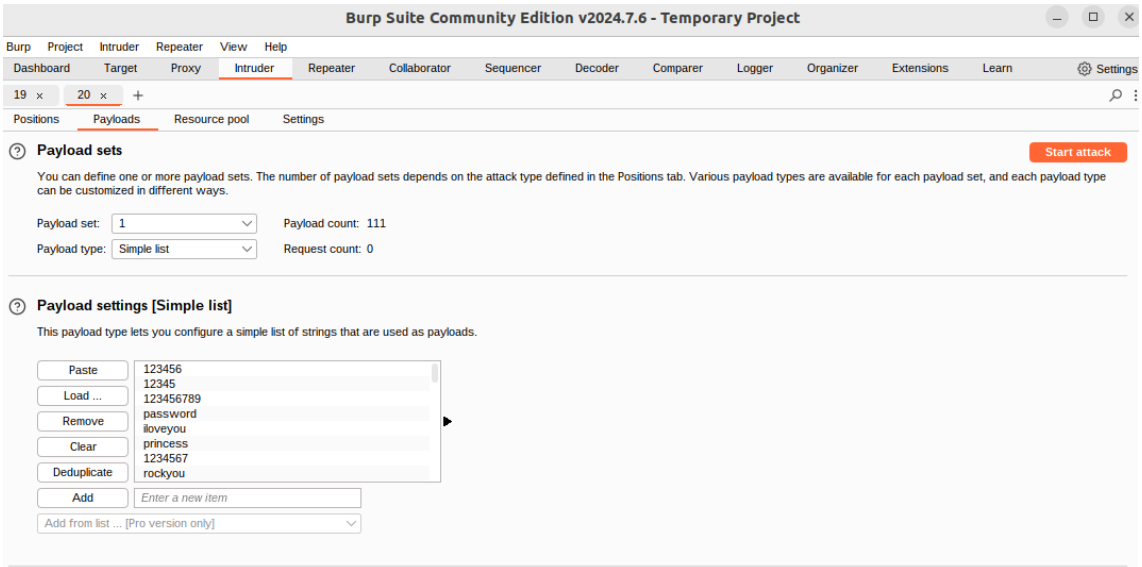
Empezamos el ataque, si alguna contraseña coincide pues nos dará un código 200



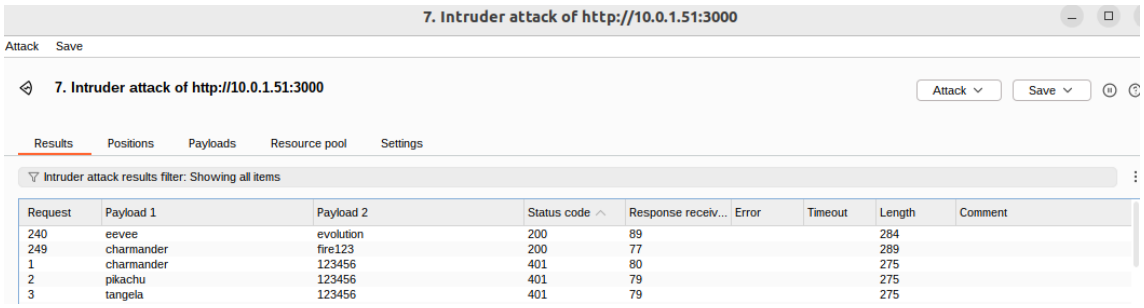
Request	Payload 1	Payload 2	Status code	Response receiv...	Error	Timeout	Length	Comment
240	eevee	evolution	200	89			284	
249	charmander	fire123	200	77			289	
1	charmander	123456	401	80			275	
2	pikachu	123456	401	79			275	
3	tangela	123456	401	79			275	
4	eevee	123456	401	80			275	
5	charmander	12345	401	79			275	
6	pikachu	12345	401	81			275	
7	tangela	12345	401	81			275	
8	eevee	12345	401	81			275	

5. También como sabemos que hay algunos usuarios con nombre de pokemon hemos generado una lista para que nos descubra usuarios de pokemon, complementándola con su contraseña.

6. Añadir en los payloads cada uno en su sitio e iniciamos el ataque



Aquí algo de los resultados


7. Intruder attack of http://10.0.1.51:3000
Attack
Save
7. Intruder attack of http://10.0.1.51:3000
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items
Request
Payload 1
Payload 2
Status code
Response receiv...
Error
Timeout
Length
Comment
240 eevee evolution 200 89 284
249 charmander fire123 200 77 289
1 charmander 123456 401 80 275
2 pikachu 123456 401 79 275
3 tangela 123456 401 79 275