Intro to Cybersecurity

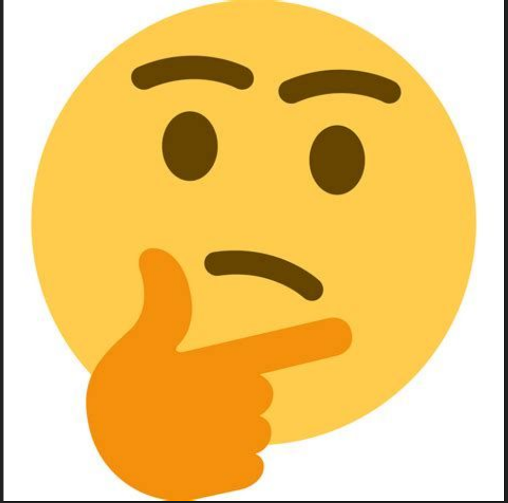
By Axel Reyes

Are your accounts really secure?

- Do you make strong passwords?
- Do share your information online?

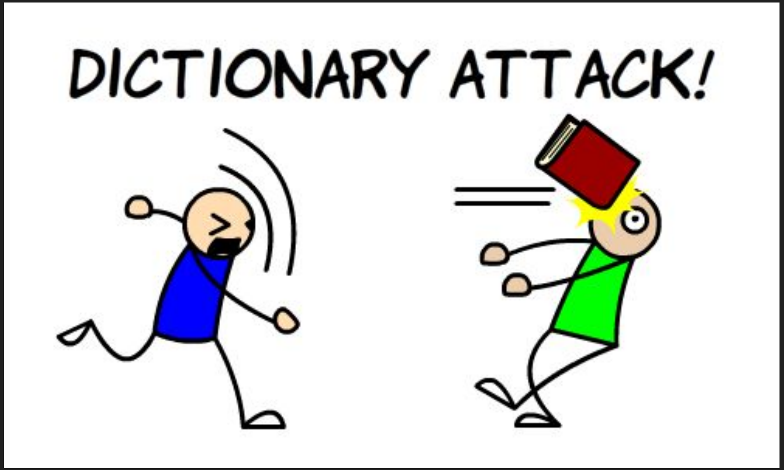
What is a Brute Force Attack?

- Guessing over and over again for the correct credentials using information you learn as you make more attempts
- An example is trying every combination of a padlock



Dictionary Attack

- A common type of Brute Force attack that guesses using common words in a dictionary or forgotten/common passwords rather than random strings but together

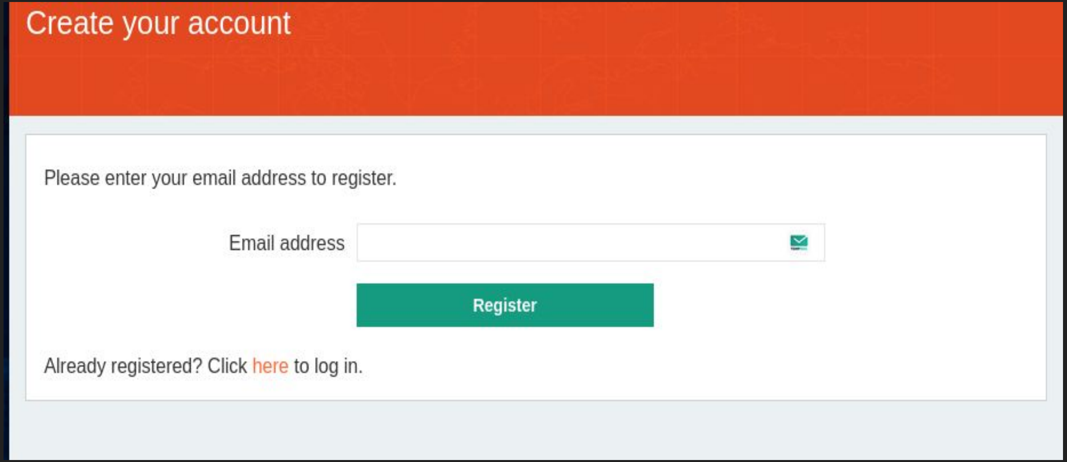


How to defend against it?

- Many people use common phrases for passwords and the same username for different platforms
- 2fa - 2 factor authentication prevents even people who can guess your credentials for even logging in
- Use complex passwords that are uncommon

Objective: Brute force Attack a Blog

- Let's see how easy it to perform a Brute Force Attack
- Make an account on Portswigger
- Download Burpsuite Community Edition

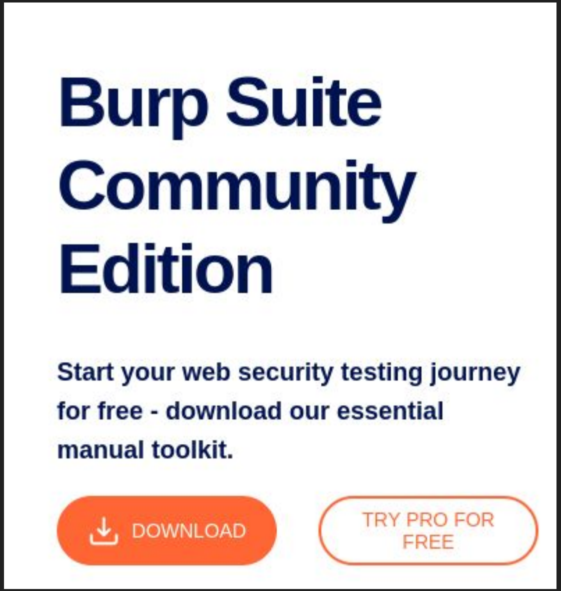


Create your account

Please enter your email address to register.

Email address

Already registered? Click here to log in.

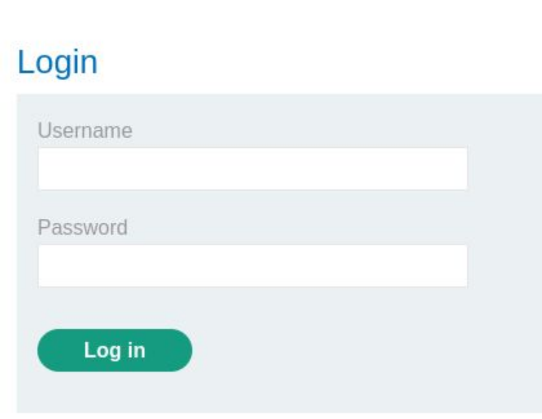


Burp Suite Community Edition

Start your web security testing journey for free - download our essential manual toolkit.

Target site: Blog

- Make your way over to the vulnerable Blog site



Login

Username

Password

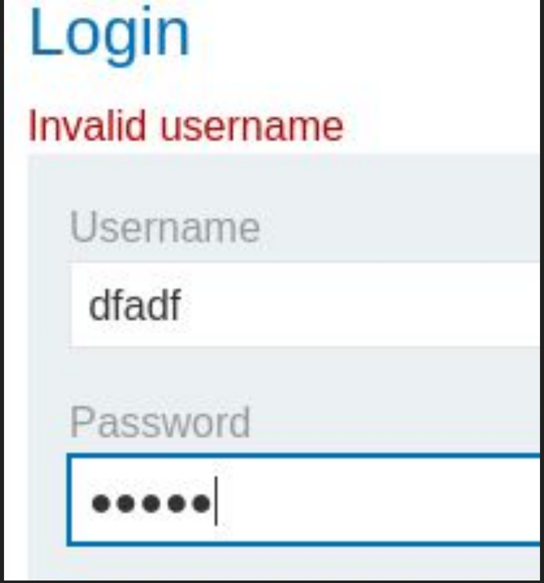
Look carefully!

- Attempt to log in
- What information does this website tell you

- Here we know that the entered username is

  Invalid and therefore the website will tell us

  If a username we enter is valid



Login

Invalid username

Username

dfadf

Password

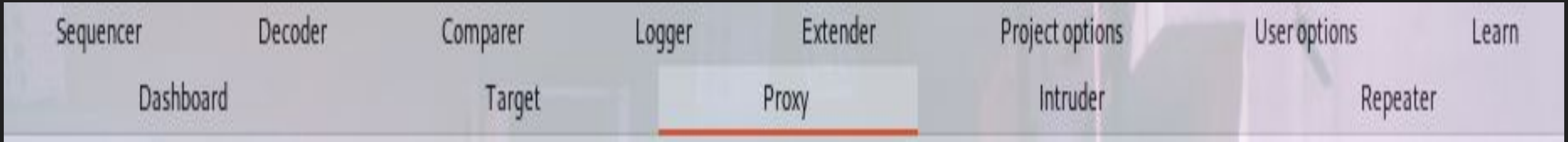
●●●●●

I can see that we don’t have the proper credentials!

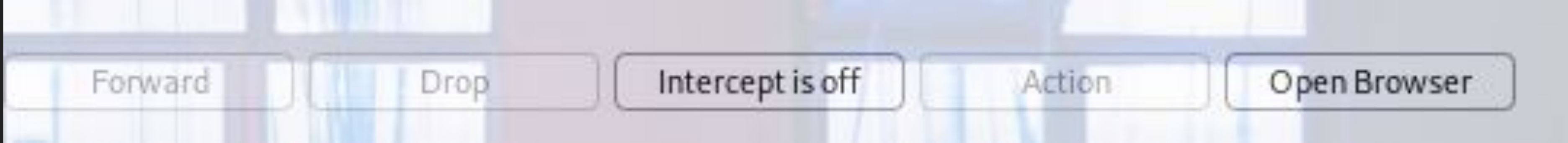
- If we guess enough random usernames we might be able to find one that works for us from a person that put a simple username like “user” or “admin” or “JaneDoe”

Tools to make our life easier!

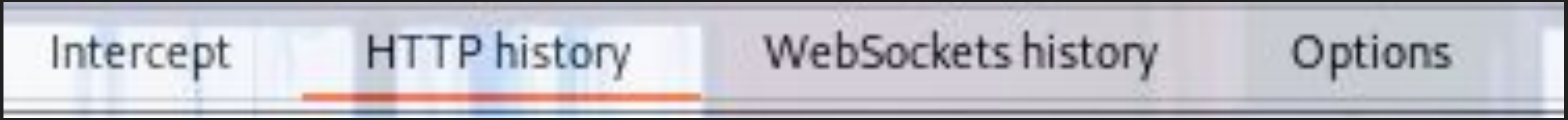
- Burpsuite lets us automate our hacking tasks while providing extra information to us!
- First step is to start up Burpsuite and navigate to the proxy tab



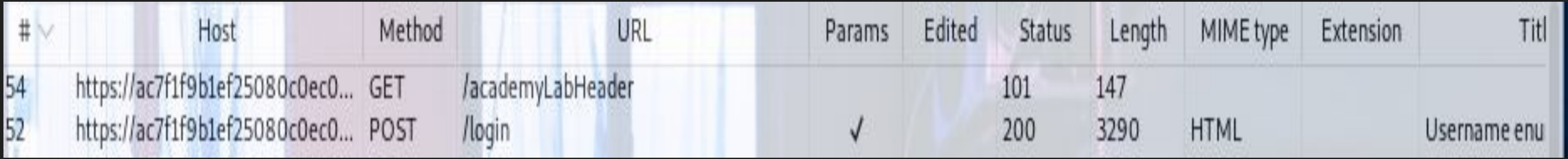
- Make sure Intercept is off and click Open Browser to use Burpsuite’s built in browser



- Navigate to the “HTTP history” tab

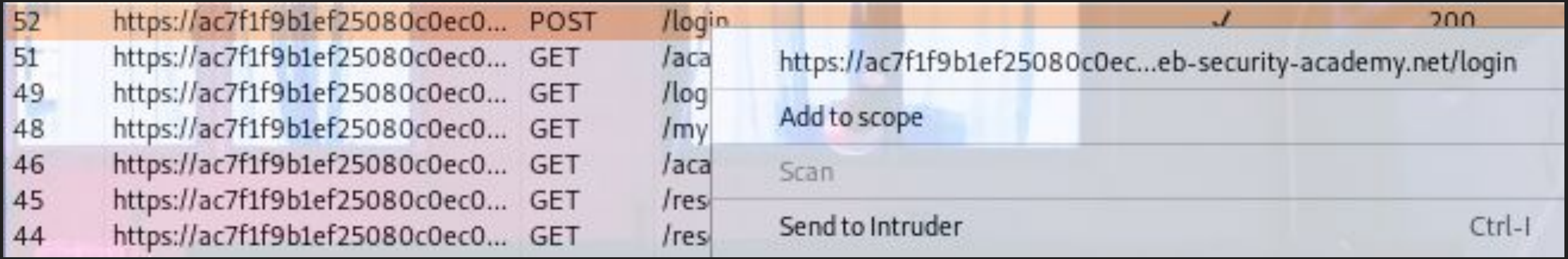


- Open the Blog site in the Burpsuite Browser and attempt to log in
- You will see an entry appear with POST under the Method column and a ‘/login’ under the URL column



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Titl
54	https://ac7f1f9b1ef25080c0ec0...	GET	/academyLabHeader			101	147			
52	https://ac7f1f9b1ef25080c0ec0...	POST	/login	✓		200	3290	HTML		Username enu

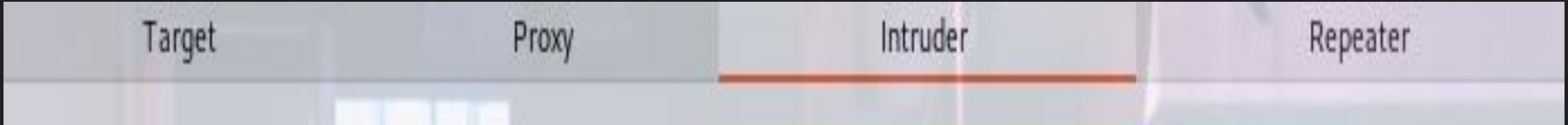
- Right click the entry and select the “Send to Intruder” option



```
52    https://ac7f1f9b1ef25080c0ec0...   POST   /login              ✓     200
51    https://ac7f1f9b1ef25080c0ec0...   GET    /aca
49    https://ac7f1f9b1ef25080c0ec0...   GET    /log
48    https://ac7f1f9b1ef25080c0ec0...   GET    /my
46    https://ac7f1f9b1ef25080c0ec0...   GET    /aca
45    https://ac7f1f9b1ef25080c0ec0...   GET    /res
44    https://ac7f1f9b1ef25080c0ec0...   GET    /res
```

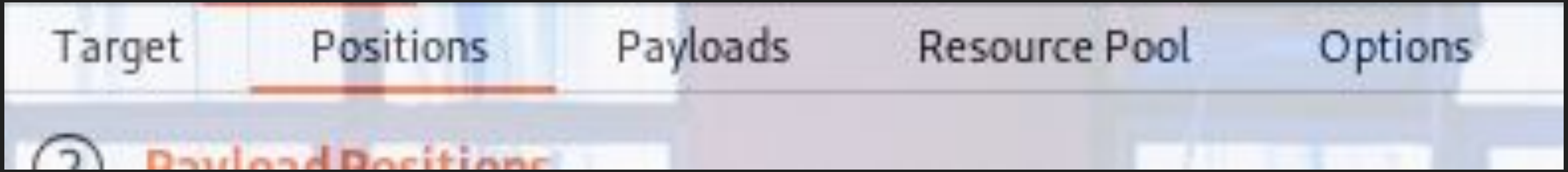
https://ac7f1f9b1ef25080c0ec...eb-security-academy.net/login
Add to scope
Scan
Send to Intruder
Ctrl-I

- Navigate to the Intruder tab to the right of the proxy tab

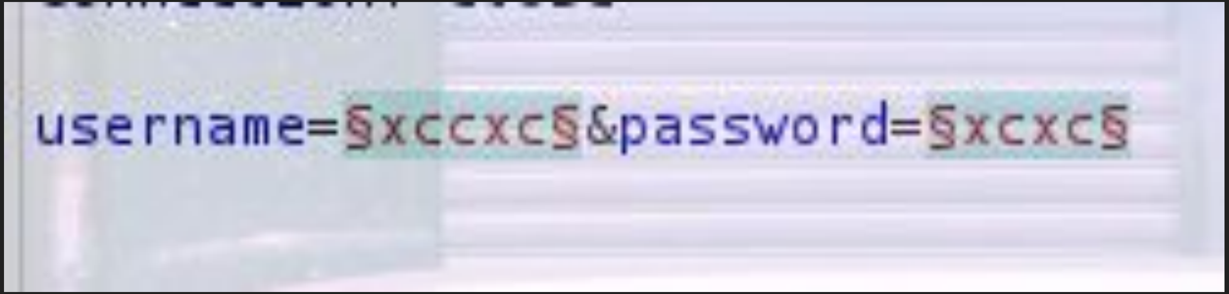


Automation time!

- Now we setup burpsuite to do the guessing for us!
- Navigate to the “positions” Tab within “Intruder”



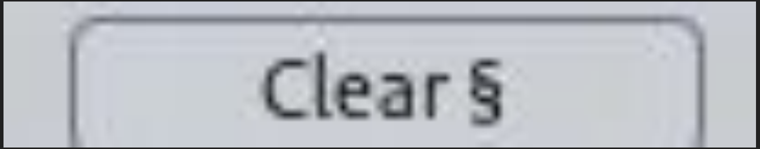
- You will be see lots of things going on, but relax! Try to focus on the bottom of the page



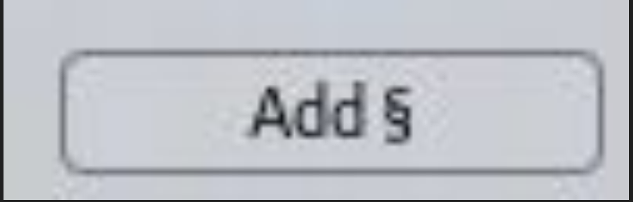
```
username=§xccxc§&password=§xcxc§
```

- This small section dictates what information you’re going to send to this website’s server
- You’ll notice that it’s the same information from when you attempted to login

- If you click the ‘Clear §’ button you’ll remove all those § symbols from the page
- They serve as place holder for inserting data like several usernames and passwords!

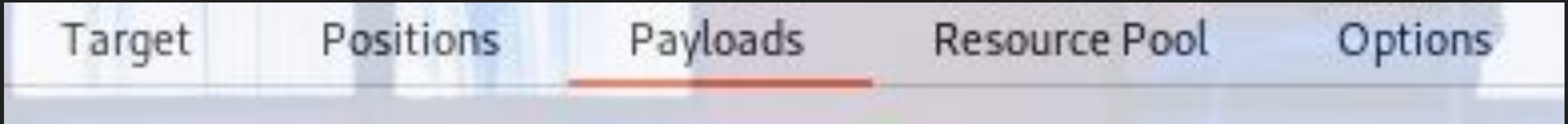


- Highlight the text set to equal “username” and click “Add §”

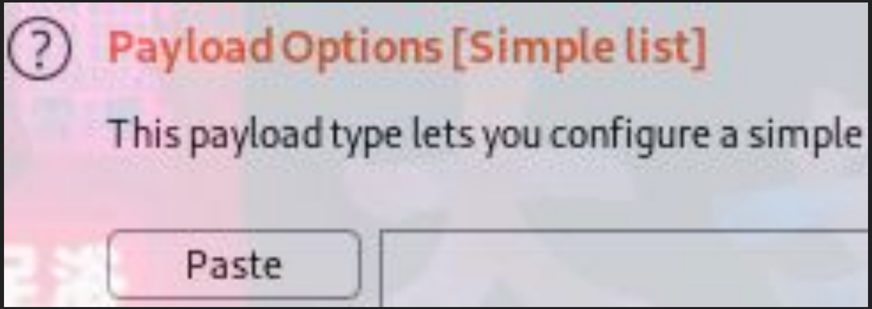


- It should look like this
username=§random_username§

- Switch over to the payloads tab

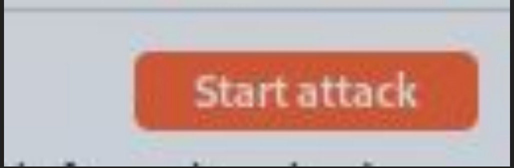


- Go to this link to copy all of the generic usernames and paste them with the “Past” button under Payload Options


Payload Options [Simple list]

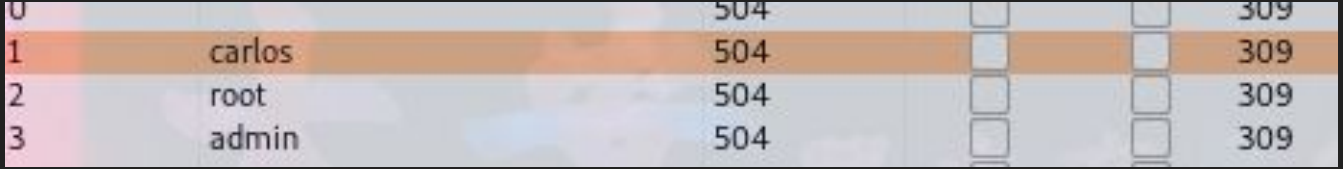
This payload type lets you configure a simple

- On the top right of the screen hit “Start Attack”



- Burp suite is now sending a POST request the same way you did, but it’s automatically testing a list of usernames for you one by one! Isn’t that great?

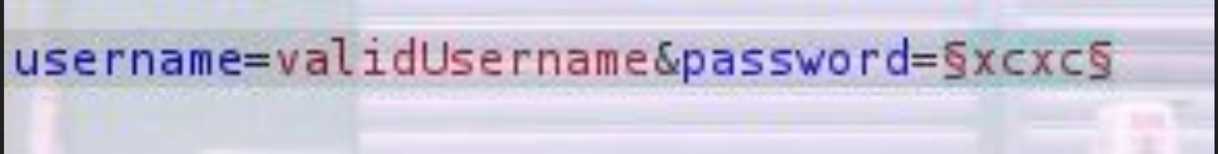
- You’ll see a screen similar to this



0		504	□	□	309
1	carlos	504	□	□	309
2	root	504	□	□	309
3	admin	504	□	□	309

- All of these are entries like the one you did at the start and they’re all wrong except for one
- Be on the lookout for an entry with a unique Length value
- This can indicate that the response from the website was different and not just a “wrong username”

- When you get a unique response it means you found a valid username
- Take your new found username and paste it into the Intruder-Positions section’s “username= “ area and repeat the steps but for the password section



```
username=validUsername&password=§xcxc§
```

- After doing this for username and password you will have found a valid set of credentials and can attempt to login!

Thank You For Listening!