

Intro to Cybersecurity

By Axel Reyes

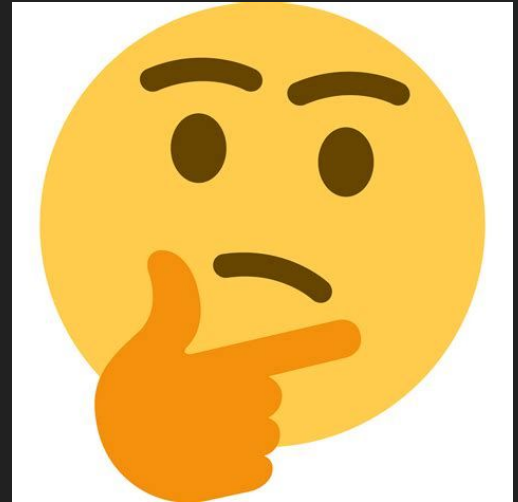
Are your accounts really secure?

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



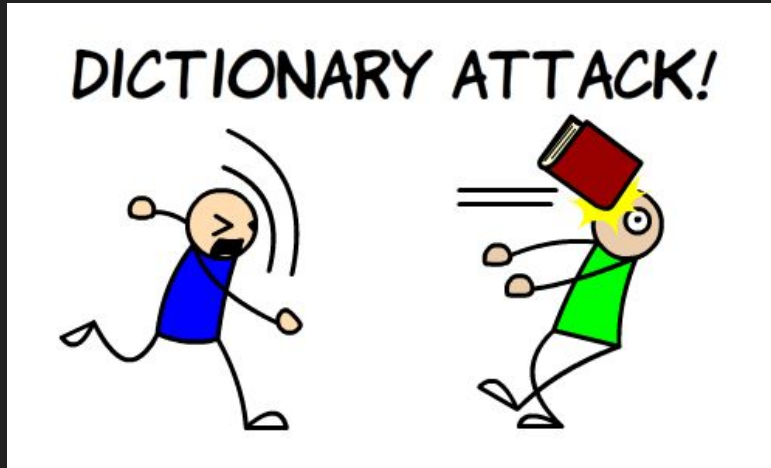
What is a Brute Force Attack?

- 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



3.14
159265358979323846264338327
950288419716939937510582097
49445923078164062862089986
28034825342117067982148086513282
30664709384460955058223172535940812848
1117450284102701938521105559644622948954
9303819644288109756659334461284756482337867831652712
01909145648566923460348610454326648213393607260249
1412737245870066063155881748815209209628292540917153
6436789259036001133053054882046652138414695194151160
9433057270365759591953092186117381932611793105118548074462379962749
567351885752724891227938183011949129833673362440656643086021394946
39522473719070217986094370277053921717629317675238467481846766940
51320005681271452635608277857134275778960817363717872146844090122
4953430146549585371050792279689258923542019956112129021960864034
418159813629774771309960518707211349999999837297804995105973173281609631859
50244594553469083028425223082533446850352619311881710100031378387528865875332083814206
17177669147303598253490428755468731159562863882353787593751957781857780532
17122680661300192278766111959092164201989380952572010654858632788659...

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

[Register](#)

Already registered? Click [here](#) to log in.

Burp Suite Community Edition

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

 DOWNLOAD

TRY PRO FOR
FREE

Target site: Blog

- Make your way over to the vulnerable [Blog](#) site

Login

Username

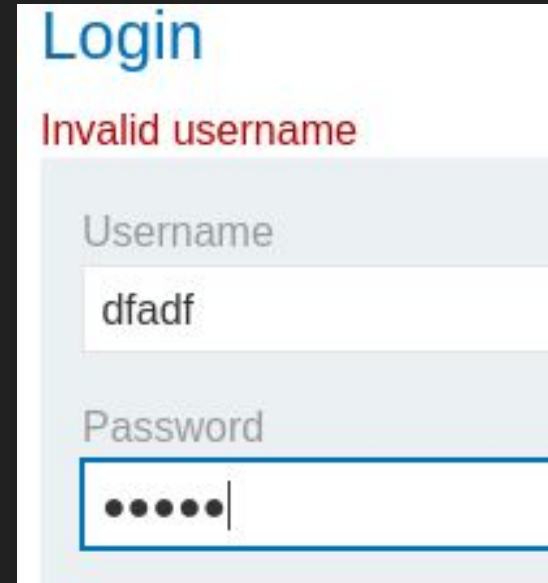
Password

Log in



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



The image shows a login interface with the title 'Login' in blue. Below the title, a red error message 'Invalid username' is displayed. The form contains two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'dfadf'. The 'Password' field is masked with five dots. The entire form is set against a light blue background.

Login

Invalid username

Username

dfadf

Password

.....

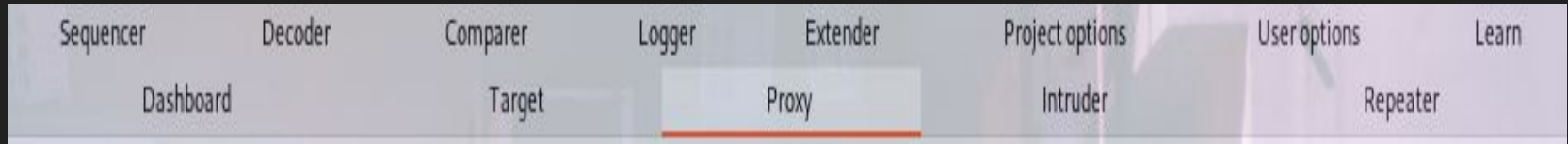
I can see that we don't have the proper credentials!

- 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”

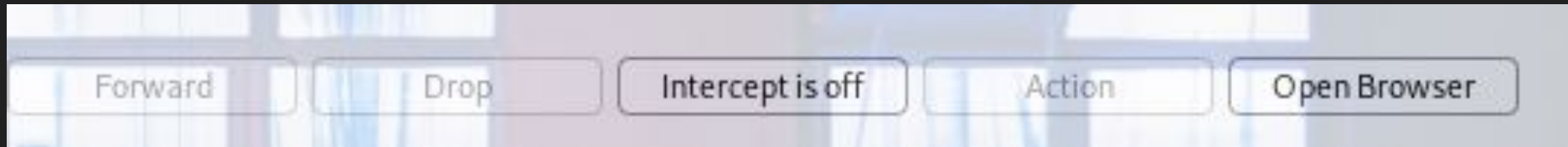


Tools to make our life easier!

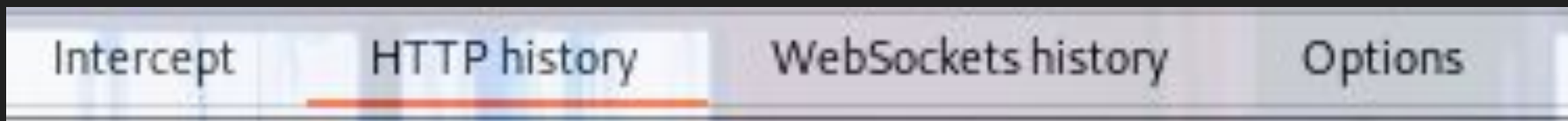
- Burpsuite lets us automate our hacking tasks while providing extra information to us!
- First step is to start up Burpsuite and navigate to the proxy tab



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



- Navigate to the “HTTP history” tab



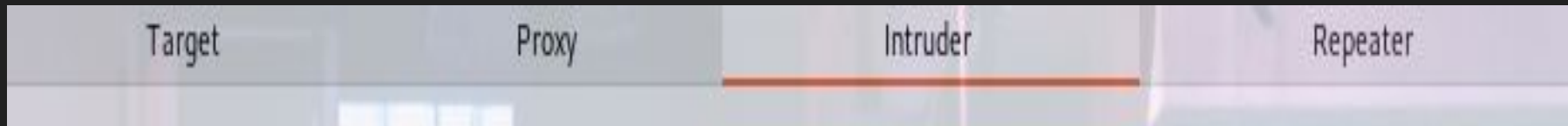
- Open the Blog site in the Burpsuite Browser and attempt to log in
- You will see an entry appear with POST under the Method column and a ‘/login’ under the URL column

#	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

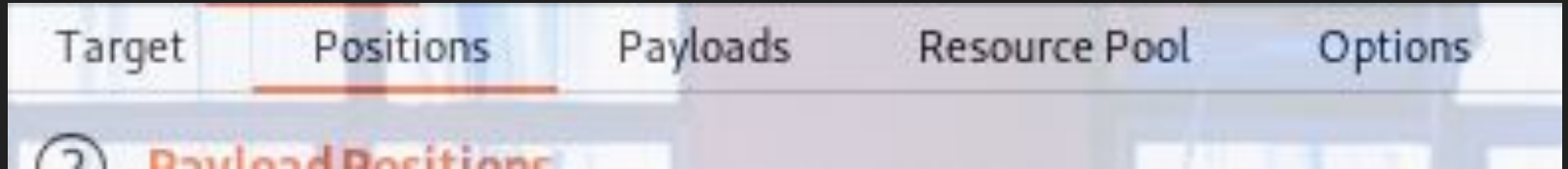
52	https://ac7f1f9b1ef25080c0ec0...	POST	/login	✓	200
51	https://ac7f1f9b1ef25080c0ec0...	GET	/aca	https://ac7f1f9b1ef25080c0ec...eb-security-academy.net/login	
49	https://ac7f1f9b1ef25080c0ec0...	GET	/log		
48	https://ac7f1f9b1ef25080c0ec0...	GET	/my	Add to scope	
46	https://ac7f1f9b1ef25080c0ec0...	GET	/aca	Scan	
45	https://ac7f1f9b1ef25080c0ec0...	GET	/res		
44	https://ac7f1f9b1ef25080c0ec0...	GET	/res	Send to Intruder	Ctrl-I

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

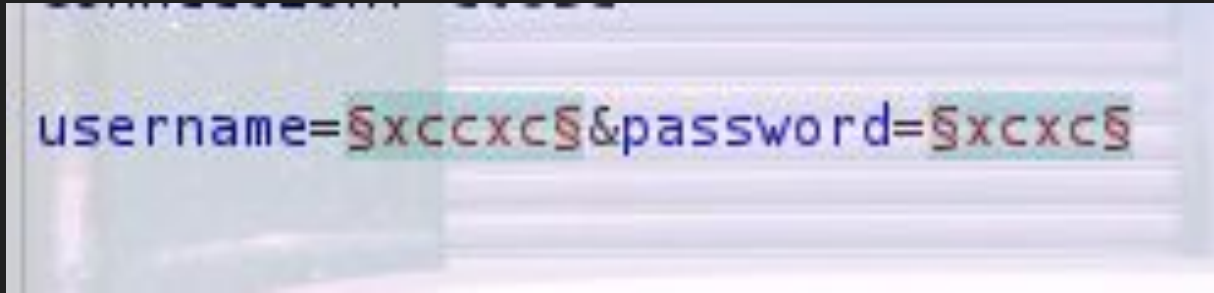


Automation time!

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

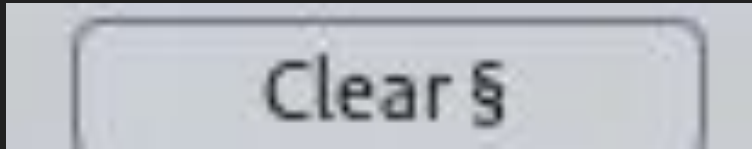


- You will be see lots of things going on, but relax! Try to focus on the bottom of the page

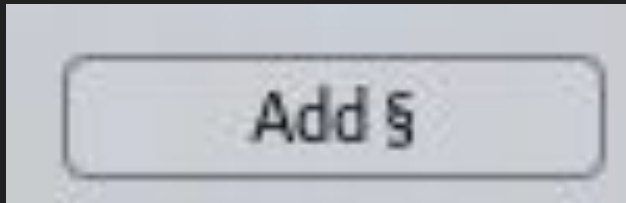


- This small section dictates what information you're going to send to this website's server
- You'll notice that it's the same information from when you attempted to login

- 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!

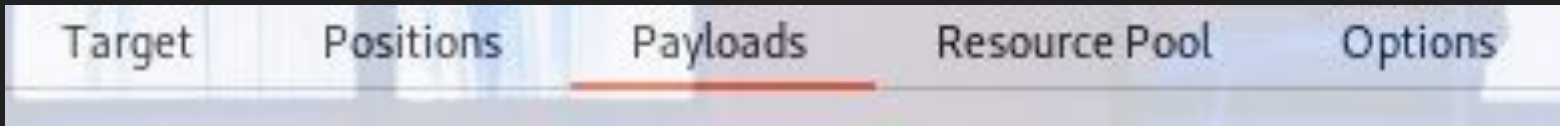


- Highlight the text set to equal "username" and click "Add §"

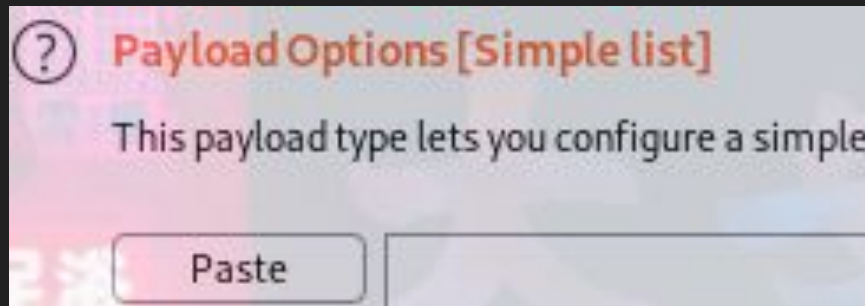


- It should look like this
username=§random_username§

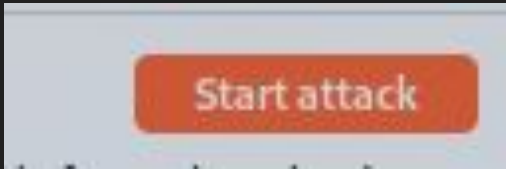
- Switch over to the payloads tab



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



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



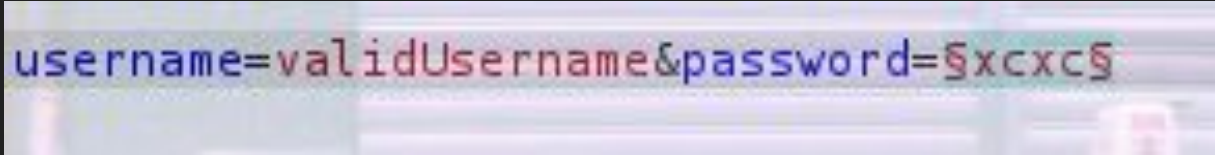
- Burp suite is now sending a POST request the same way you did, but it's automatically testing a list of usernames for you one by one! Isn't that great?

- You'll see a screen similar to this

0		504	<input type="checkbox"/>	<input type="checkbox"/>	309
1	carlos	504	<input type="checkbox"/>	<input type="checkbox"/>	309
2	root	504	<input type="checkbox"/>	<input type="checkbox"/>	309
3	admin	504	<input type="checkbox"/>	<input type="checkbox"/>	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!