Brute-force Attack "Seeking but Distressing"

Konark Truptiben Dave
Department of Computer Engg. & Information Tech.
C.U.Shah Technical Institute of Diploma Studies,
Surendranagar-363001, Gujarat, India

Abstract- A common problem to website developers is password guessing attack known as Brute force attack. An attacker discovers a password by trying every possible combination of numbers, letters. Some people are showing carelessness in choosing username and password. This may be a risky step to choose a simple username and password. There is also a problem with the website developers for choosing username and password. So, what will be the solution, which policies are considered in choosing username and password and how can you defend against the loot of hackers are covered in this.

Keywords - Brute force attack, Trial and Error, Dictionary attack

I. INTRODUCTION

In this era, many people are eager to discern the person's user name, password of mail account, number of credit card etc. If any of encryption algorithm used then people are also interested in knowing key to get the original message. The different ways used by the people to get passwords and key (if an Encryption algorithm used) of others are known as attacks. And the people who perform these attacks are called **Attackers** or **Hackers**.

There are many type of attacks can be performed on system. One of the most famous and publicized attack is **Brute-force attack.**

II. HISTORY OF THE NAME 'BRUTE-FORCE'

Brute-force was actually a game for PC released in 2000. Brute Force was a third-person shooter and consisted of several characters. Each with their own strengths and capabilities.

The aim was to find several other characters who were reliable to the union. A team was formed named "brute-force team" to answer the union. Mission of the team was to find and fought with the aliens and armed force.

Whenever any of these aliens are seen, the members of the Brute force team battled with them.

III. WHAT THE BRUTE-FORCE ATTACK IS

The attack which uses the method "Trial and error" by guessing passwords is called Brute force attack. An attacker first gathers the fundamental information about the user. For example, user's full name, room number, vehicle number, children names etc.

The attacker continuously tries random passwords on the basis of the user's personal information. The attacker tries this until he/she gets success. This may take hours, days, months and years also.

The higher the type of encryption scheme (32,64,128,168-bit etc.) used, the more time required.

Table -1 CALCULATION

KEY SIZE	NO. OF ALTERNATION
32-bit	2^{32}
56-bit	2^{56}
128-bit	2^{128}
168-bit	2^{168}

As mentioned in above table, depending upon the key size, number of alteration is possible. The more long the key, less chance for compromise.

Brute force attack is also known as **"Dictionary attack"** or **"Hybrid Brute-force attack".**

IV. HOW THE ATTACKERS DO BRUTE-FORCE

If your website requires user authentication to go through it then it will be a fine target for a brute-force attack. The attack is an attempt to determine a password by analytically trying every possible combination of letters, numbers, and symbols etc. But the hindrance is that it could take a long period of time (i.e. years) to find depending upon the complexity and length of password. Many people wish to choose a meaningful dictionary word rather than selecting a random password.

If the attacker attacks on the basis of exact dictionary words, then it is known as "Dictionary attack". And if the attacker slightly modifies the dictionary words and perform attack is known as "Hybrid Brute-force attack".

There are many tools available with hackers to attack in which many possible combinations are fed. These tools use different IP address on each try. So, it is hard to trace a single account for unsuccessful password attacks.

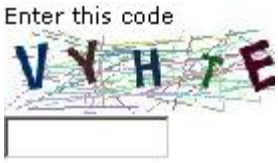
A most common way to avoid Brute force attack-

Today, a most common way to avoid Brute-force attack is to lock account on certain numbers of incorrect password attempts. This lockout can last up to specific duration (i.e. 1 hour, a day etc.).

In some cases, the account is locked until the Administrator unlocks it. But this is not a proper and practical solution to this attack because someone can easily abuse the security and lockout hundreds of accounts with certain tools.

Another common but proved way to avoid Brute force attack-

CAPTCHA



"**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part".

This is a better solution to the above problem. It is a program that was First widely used by Alta Vista to prevent automated search submissions. CAPTCHA code contains numeric, alphabets etc. They work by presenting some test that is simple for humans to pass but tough for computers to pass. A user has to enter the exact CAPTCHA code shown near the textbox control. Whenever a page is refreshed, code is changed.

If hacker uses any of the tools then it is not possible to enter into the system. Because tools or machines do not have intelligence and every time it is not possible for a machine to enter true CAPTCHA code. So, CAPTCHA will not allow doing it. This technique gives hundred percent result. That is why it is used widely.

V. PREVENTING BRUTE-FORCE ATTACKS(USER-SIDE AND DEVELOPER-SIDE)

User side-
Username Selection:-
A password is only half of the required login permit, half is username. Choosing a username is also an important one. A username is not likely to be a dictionary word.Some of the people select their names as usernames. And some are selecting their e-mal addresses as usernames because they are easy to remember.

This is benefit to hackers. They have arms of e-mail addresses and names to check with different tools.

Choose a Password Carefully!

Generally, people do not remember typical and complicated passwords. So, they are not interested to choose passwords which are difficult. Often, people pick simple password like “1234”,”abcd”,spouse name, favorite sports team name, spouse name etc. But sorry to say these types of passwords are very easy to guess by someone else. Hackers have some automated tools and these tools will easily guess dictionary words and hybrid dictionary words.

In such a way, users’ accounts are compromised. User need to develop a strong password policy to prevent attacks.

The policy should include.

1. **Minimum password length should be at least seven characters.**
2. **Should include both upper and lower case letters.**
3. **Should include numeric characters.**
4. **Should include some special characters like &,#,@,$,% etc.**

The advantage behind choosing the password form above policy is that if you use alphabet, numeric, special symbols in password then it is very difficult for hacker to guess your password.

Developer side-
Username and password selection:-
For a developer, it is seen that some usual usernames and passwords are chosen as an Administrator like “admin”, ’administrator”. Compromising an Administrator account means compromising all the registered users’ accounts. If the hacker's dictionary attack may gain access to an administrative account, he could probably do much more damage to the system than he could if he gained access to a regular user's account.

Carefully Word Your Error Messages:-

It is very important to generate appropriate error messages in response to failed login attempts. Many website developers display messages like “Incorrect username”, ”Wrong password”, ”User not found” etc. Displaying these types of message mean that providing the exact information about hacker’s failed attempt. These messages are very helpful to hackers and they can lead to a proper way that he/she wants to go.

For example, a screenshot is taken for failed login attempt**.**

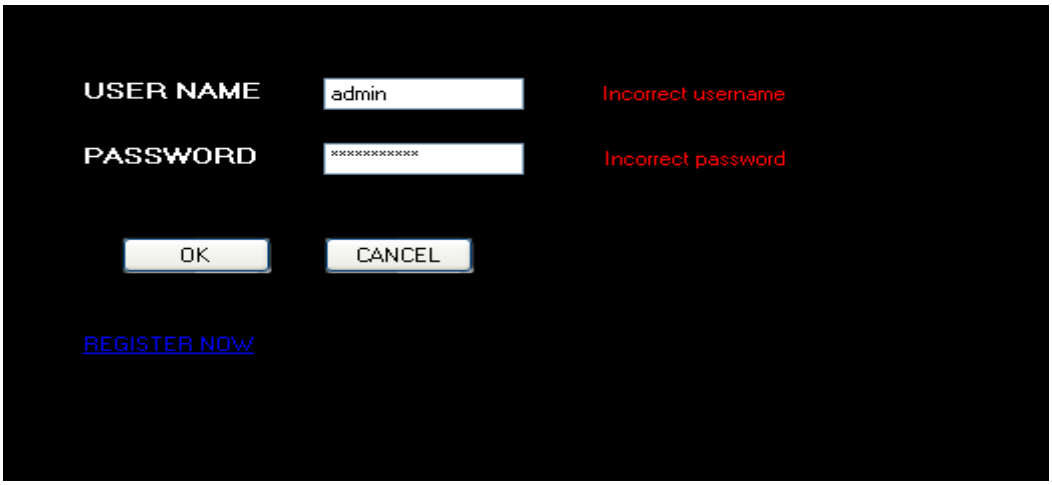


Figure-I Screen shot of login page

VI. CONCLUSION

A brute force attack can be very effective at compromising your web application unless proper defenses are used. A Brute-force attack can be a dangerous one to your system if carelessness is taken. With the above strategies these types of attack can be avoided.

REFERENCES

[1] Stallings William, (2008) "Cryptography and Network security" (Fourth edition)Pearson, New Delhi, pg no. 33,35
[2] https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks
accessed on dt. 24/02 /2013
[3] http://en.wikipedia.org/wiki/Brute-force_attack accessed on 2/3/2013
[4] http://www.codeproject.com/Articles/17111/Preventing-a-Brute-Force-or-Dictionary-Attack-How accessed on 5/3/2013