

# 2

## Brute Force Attacks

– Pratul Goyal

Assistant Professor, Graphic Era Hill University

<https://orcid.org/0000-0003-1040-8109> [pratul.goyal111@gmail.com](mailto:pratul.goyal111@gmail.com)

The brute force attacks, the attacker tries a large number of probable credential combinations to gain unlicensed entry to a system or a file. These attacks are usually carried away through a script of all the common credentials available which is then used to decrypt the encrypted data such as passwords.

### ARTICLE HISTORY

**Paper Nomenclature:** Scrutiny Tip (ST)

**Paper Code:** CYBNMV2N7JULY2020ST1

**Submission Online:** 03-July-2020

**Manuscript Acknowledged:** 07-July-2020

**Originality Check:** 09-July-2020

**Originality Test Ratio:** 9% (Drillbit)

**Peer Reviewers Comment:** 13-July-2020

**Blind Reviewers Remarks:** 14-July-2020

**Author Revert:** 15-July-2020

**Camera-Ready-Copy:** 18-July-2020

**Editorial Board Citation:** 20-July-2020

**Published Online First:** 23-July-2020

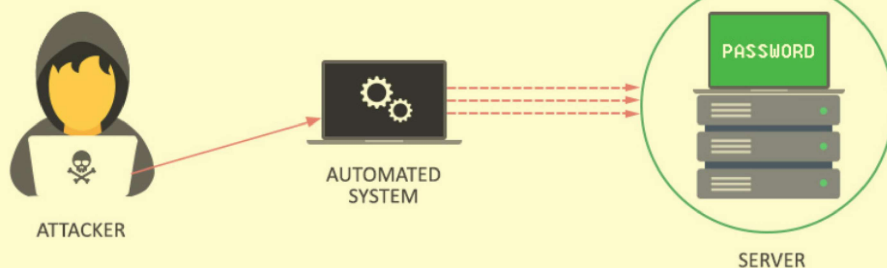
### Keywords

- Brute Force Attack
- IP
- Endpoint
- Social Media

### Introduction

Attackers can use this type of attack for permission to access any website or any attack and then can do whatever they want. It is effective, although a time-consuming approach as we must follow a hit and trial approach for all the possible combinations.

Automated tools are usually used to guess various combinations of credentials. It also depends upon the force of credentials. For example, if the password is complex then it will take longer to find the correct combination.



Most of the cases, usernames and passwords from past attacks are used which are generally available on the internet which act as the initial information to begin this type of attack.

### Interesting Cases for Brute Force Attacks

**Case 1: Brute Forcing a Web authentication endpoint.**

1. Web authentication endpoint which belongs to a well-known

site was found to be protecting against brute force attacks only via means of rate limiting based on IP.

2. We can carry out this brute force attack using the clear-text password databases which are available on the internet like: <https://wiki.skullsecurity.org/Passwords>
3. Our first attempt was to try brute forcing using the TOR network but there was a WAF present in their environment to block this activity right away.
4. It was found that the target also supports IPV6 address and thus an IPV6 Virtual Private Server (VPS) was configured to have different multiple IPV6 addresses based on the provided range.
5. The next step was to create a python script through which we can log in using different available IPs in the pool and having a gap of 3 seconds between the reuse of the same IP. (We calculated in the initial recon that any request within 3 seconds from the same IP was getting blocked).
6. Let's take out a list of the most commonly used 10,000 passwords and append it with one real password which belongs to our test account ([hackme@gmail.com](mailto:hackme@gmail.com)).
7. Let us start the python script on our target:

```
Usage: python endpoint.py  
<USERNAME> <PASSWORD_<br>DICTIONARY_FILENAME ><br><INTERFACE of VPS> <THREADS>
```

```
#python endpoint.py hackme@<br>gmail.com common_passwords.<br>txt vnet0 50
```

8. It took exactly 340 seconds to hit the right password at 10,001 positions on

the list. Thus, an attacker can predict the password at this rate as we can bypass the rate limiting and were able to send 10,000 wrong attempts on the target without any issues.

9. This was only possible as the target was not using any captcha mechanism or any account locking policy like locking out that account on observing more than "x" number of attempts.

#### ***Case 2: Ways to Brute Force a Social Networking Platform.***

1. There was a mobile endpoint for this site to perform authentication: `https://m.abc.com/api/v1/accounts/login/`
2. We tried to do a brute force attack using the Burp Intruder feature and for the first 1000 guesses we received a response "Entered password is incorrect". Please try again". All these attempts were done from a single IP only. After the first 1000 guesses, the response changed to "Entered username is incorrect" (Even when the username was correct). We got to know that there is a limiting rate which is getting triggered after the first 1000 attempts.
3. The same response was being provided by the target for the next 1000 attempts (Total 2000 attempts so far) but after that, we started getting a mixed response with the "Entered password is incorrect" followed by "Entered username is incorrect" consecutively.
4. A brute force strike can be carried away after observing the above pattern. We just need to replay the same input when the received response is "Entered username is incorrect" as we know from the observed pattern that it will take

the same password next time without any issues.

5. We just need to create a python script to brute force 10,000 most used passwords just like in the previous case which will be having the real password as the final entry for the test account.
6. It took 210 seconds to crack the right password stored at 10,001 locations in the text file and this vulnerability was exposed clearly.
7. There was no account lockout policy or IP address location-based fraud detection mechanism being used by the target to get rid of such brute force attempts which made it very easy for the attacker to exploit this vulnerability.

#### ***Case 3: Taking over the temporarily locked accounts on a Social Networking Site.***

1. We observed that even after providing the valid credentials, we were being sent to the page to verify our account due to inactivity. We were getting options to complete this verification by email or phone.
2. On observing the URL carefully of this verification page, it was found that it was having the unique user ID within it. This site was having incremental user IDs and thus we can brute force this parameter in the URL and then observe the outputs.
3. For very few accounts, we received the same response of verifying the account by email/ phone, but we cannot do that as we do not have access to the victim's email/phone.
4. For some accounts, the site asked us to verify our account through captcha, but the bizarre thing was that for other remaining

accounts, we got an option to update the email address.

5. Thus, we can change the email address and then alter the password to take over these accounts.
6. The most serious issue was discovered with the greatest number of accounts as the site was allowing us to update phone numbers and verify accounts. Thus, a password reset can be easily done after changing the victim's phone number.
7. There must be appropriate authentication on the pages that allow updating any information. Lack of this authentication can cause an attacker to exploit this vulnerability.

#### **Case 4: Taking over the account through token brute force attack.**

1. The target, in this case, is an app that can be used to build a workspace for any organization. Once the workspace is created, the admin can further invite the users to join the same workspace.
2. We observed one major disparity stuck between the invitation URLs being sent. If an admin invites any external user, the invitation URL

looked like this: [https://abc.com/account/?service=prod&digest=aa\\_sOBeXtSZDRqgVISRPagPXc0](https://abc.com/account/?service=prod&digest=aa_sOBeXtSZDRqgVISRPagPXc0)

3. But if the invite was sent to an existing user then the URL was different: <https://abc.com/invitations?inviteId=190000007658819&type=accept&source=mail> no hash or signature was used in this URL.
4. We tried to further investigate this URL after comparing other URL invites and got to know that the first 12 digits refer to the group and the last 3 digits refer to the invitation ID (which needs to be brute-forced).
5. On testing further, it was found that this user ID is not even getting expired if someone else is using it. For example - Suppose admin sent an invitation to "[abc@gmail.com](mailto:abc@gmail.com)" but the attacker was able to do a brute force strike on the user ID and was able to join the organization with "[xyz@yahoo.com](mailto:xyz@yahoo.com)" and the invitation will still remain active and the admin would see that the invitation is still pending.
6. This way an attacker can get control of the admin account with a great chance of not getting noticed at all. Such vulnerabilities are the most dangerous ones.

#### **Case 5: Getting into the accounts on Social Media without any user interaction.**

1. It was found that every time the user forgets their password, they get an option to reset the same by entering their phone or email address on this link: <https://www.godzilla.com/login/>

[identify?ctx=recover&lwv=110](#)  
(Actual target name changed)

2. This site will further verify the user by sending the 6-digit code to the provided phone or email address and then we can reset the password easily.
3. The first thing which arises in our brain is to brute force this 6 digit code on our target "[www.godzilla.com](http://www.godzilla.com)". We found that just after 10-12 attempts, we were getting blocked.
4. We further went ahead and tried the similar thing on the beta version of this site "beta.godzilla.com" and surprisingly there was no rate limiting present on this target.
5. We were able to brute force that 6-digit code and were capable of getting into any account present on their beta version.




**Pratul Goyal**, is an Assistant Professor with Graphic Era Hill University and IIM Postgraduate, He got an extensive experience vivid domain like data science and cyber security. He is also a consultant and have worked as a corporate trainer for Simplilearn. He also has his blogging website [datasciencejourney.com](http://datasciencejourney.com) and YouTube Channel.

 [pratul.goyal111@gmail.com](mailto:pratul.goyal111@gmail.com)

### Annexure I

Submission Date: 09-July-2020 | Submission Id: 168047 | Word Count: 1412 | Character Count: 7986



**9** SIMILARITY % | **9** MATCHED SOURCES | **A** GRADE

**A-Satisfactory (0-10%)**  
**B-Upgrade (11-40%)**  
**C-Poor (41-60%)**  
**D-Unacceptable (61-100%)**

S.No	LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1.		flylib.com	4	Internet
2.		www.comparitech.com	1	Internet
3.		docs.aws.amazon.com	<1	Internet
4.		www.aircse.org	<1	Publication
5.		IEEE 2015 International Conference on Cloud and Autonomic Computing by	<1	Publication
6.		www.doaj.org	<1	Publication
7.		Identification of the crystallographic polarity of the 111 CdTe surf by SC-1993	<1	Publication()
8.		Fractionation of casein hydrolysates using polysulfone ultrafiltration by Y-1993	<1	Publication
9.		PDF File Data web.eecs.umich.edu	<1	Internet

Note: The Cybernomics had used the DrillBit plagiarism [https://www.drillbitplagiarism.com/] tool to check the originality.



### Reviewers Comment

**Review Comment 1:** The author has explained very well what brute force attack is. It provides a glance as to how brute force attacks are a threat to several cyber appliances. The cases provided in the article further substantiates the cause. It can help in understanding which areas we need to work upon.

**Review Comment 2:** Brute force attacks have been occurring for about two decades now. The rise in usage of emails and profile based applications have increased these attacks. Almost all applications today demand to create a profile. If their systems are attacked, personal data of various users is at risk.

**Review Comment 3:** The article gives an insight on various ways which are used to implement Brute force attacks. It is very informative and explains the concept very well. With increasing usage of social media platforms, the risk of losing data that comes with brute force attacks also multiplies.



### Editorial Excerpt

The article has 9% plagiarism which is an acceptable percentage for publication. The comments related to the paper are noticeable to the theme about how the attackers affect the system, this paper follows 5 used cases on different scenarios of the attack, namely attack through web authentication endpoint, social network platform and site, token brute force attack and social media attack without any user interaction. This is based on the latest used cases. After the editorial remarks the article has been earmarked and finalized under the "Scrutiny Tip" category.

### Acknowledgement

Author on the other-hand is highly indebted to Scholastic Seed Inc. a publisher of Cybernomics Magazine & entire editorial team including Resident Associate Editors (Ms. Sonakshi, Ms. Jyoti & Ms. Shailza) who have facilitated at each juncture during and after the publications of articles in a camera ready shape in a particular volume and issue of a magazine and nonetheless also grateful to reviewers for their valuable comments.

### Disclaimer

All views expressed in this paper are my own, which some of the content are taken from open source websites for the knowledge purpose. Those some of I have mentioned above in the references section.



**Citation**  
 Pratul Goyal  
 "Brute Force Attacks"  
 Volume-2, Issue-7, July 2020.  
[www.cybernomics.in](http://www.cybernomics.in)

Frequency: Monthly, Published: 2020  
**Conflict of Interest:** Author of a Paper had no conflict neither financially nor academically.

