

NORTH

BRIGADE



# North Brigade

The First Defense

Alex J, William S, Nyan Z, Christopher G, Ryan R, Turjo C

# Password In-Security

- Data Breaches - Passwords made public
- Easy to guess/brute force
- Reused Passwords
- Weak Encryption passwords
- Phishing attacks
- Social Engineering

## TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at [hivesystems.com/password](https://hivesystems.com/password)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years



› Hardware: 12 x RTX 4090 | Password hash: bcrypt

# Cracking Passwords with John the Ripper

```
dgrbch1@DESKTOP-5HDT2P7: ~
```

Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Users\wqweq> wsl
```

```
dgrbch1@DESKTOP-5HDT2P7:/mnt/c/Users/wqweq$ echo -n 'mypassword123' | openssl passwd -6
```

Password:

Verifying - Password:

```
$6$fNh5qsxrjrU33YQK3$jzkycKHnERzrb7Cq4UhFJWLV.JoRXspj3Ch9q6Sb5srK0AJ5M0NXvJK1t8B9dy00yfp9ZVN1H3jNiQupbG42V.
```

```
dgrbch1@DESKTOP-5HDT2P7:/mnt/c/Users/wqweq$ echo '$6$fNh5qsxrjrU33YQK3$jzkycKHnERzrb7Cq4UhFJWLV.JoRXspj3Ch9q6Sb5srK0AJ5M0NXvJK1t8B9dy00yfp9ZVN1H3jNiQupbG42V.' > hash.txt
```

```
dgrbch1@DESKTOP-5HDT2P7:/mnt/c/Users/wqweq$ cat hash.txt
```

```
$6$fNh5qsxrjrU33YQK3$jzkycKHnERzrb7Cq4UhFJWLV.JoRXspj3Ch9q6Sb5srK0AJ5M0NXvJK1t8B9dy00yfp9ZVN1H3jNiQupbG42V.
```

```
dgrbch1@DESKTOP-5HDT2P7:/mnt/c/Users/wqweq$ john hash.txt --wordlist=rockyou.txt
```

Loaded 1 password hash (crypt, generic crypt(3) [?/64])  
Will run 16 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status

```
0g 0:00:00:10 0% 0g/s 8286p/s 8286c/s 8286C/s 071892..040977
```

```
0g 0:00:00:11 0% 0g/s 8283p/s 8283c/s 8283C/s 10021995..062807
```

```
0g 0:00:00:18 0% 0g/s 8328p/s 8328c/s 8328C/s maghanoy..lucy27
```

```
0g 0:00:00:19 0% 0g/s 8330p/s 8330c/s 8330C/s taurus20..sweetpea6
```

```
0g 0:00:00:20 1% 0g/s 8326p/s 8326c/s 8326C/s ashton23..arche
```

```
0g 0:00:00:49 2% 0g/s 8324p/s 8324c/s 8324C/s honeyque..home25
```

```
0g 0:00:00:50 2% 0g/s 8326p/s 8326c/s 8326C/s darkangel69..dannyjo
```

```
0g 0:00:00:51 2% 0g/s 8328p/s 8328c/s 8328C/s bailey93..baculo
```

```
0g 0:00:00:52 2% 0g/s 8323p/s 8323c/s 8323C/s 940706..920702
```

```
0g 0:00:00:53 2% 0g/s 8326p/s 8326c/s 8326C/s 13741374..132115
```

```
0g 0:00:00:54 2% 0g/s 8328p/s 8328c/s 8328C/s vanmark..valtierra
```

[?](#) **Payload Sets****Start attack**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:  Payload count: 0

Payload type:  Request count: 0

[?](#) **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Add

Enter a new item

Add from list ... [Pro version only]



Support Login +

Not secure | 10.10.213.195/support/login/

Bastion Hosting

# Support Login

Username  
user

Password  
\*\*\*\*

Login!

Burp Suite Community Edition v2023.1.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extensions Help

1 x 2 x +

Positions **Payloads** Resource pool Settings

**Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payloads can be customized in different ways.

Payload set: 2 Payload count: 100

Payload type: Simple list Request count: 100

**Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste bambam  
Load ... UnitedKingdom123  
Remove tq2q3q  
Clear valencia  
Deduplicate 258852  
10031991  
wolverine  
12111991

Add Enter a new item  
Add from list ... [Pro version only]

**Payload processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add ... Rule  
Edit  
Remove  
Up  
Down

**Payload encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: \<=>?+\*&{}^`#

# Solution

- Randomly Generate passwords with Uppercase, lowercase, numbers, and symbols.
  - Hard to guess and bruteforce
- Multi-Factor Authentication
- Change passwords every 3 months that auto-update to password manager
- Password Managers Store and manage complex passwords using trusted password manager tools
- Train and Educate people on strong passwords
- Don't reuse passwords across multiple accounts



# Additional Features

- Password Manager (Top Grade Encryption) - So the user doesn't forget their complicated passwords and have them all in one place
- Multi Factor authentication - Alerts the user when a sign in is attempted, and can ensure the proper user gains access to the website

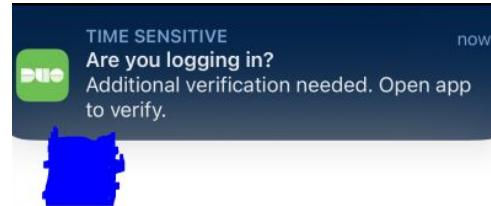
# Multi Factor authentication

## Is this your device?

If you're the only person who uses this device,  
Duo will remember it for future logins.

[Yes, this is my device](#)

[No, other people use this device](#)

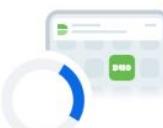


## Enter code in Duo Mobile

Verify it's you by entering this verification code  
in the Duo Mobile app...

8455

Sent to "iOS" (.....)



[Other options](#)

# Demo (Ease of Password Manager)



# Information regarding Advice and past incidents

1. **Tech.co.** "Weak and Strong Password Examples." *Tech.co*, <https://tech.co/news/weak-strong-password-examples>. Accessed 22 Nov. 2024.
2. **Stay Safe Online.** "Passwords: Securing Your Accounts." *National Cybersecurity Alliance*, <https://staysafeonline.org/online-safety-privacy-basics/passwords-securin>s-accounts/. Accessed 22 Nov. 2024.
3. **National Cyber Security Centre.** "Using Passwords." *Exercise in a Box*, <https://www.ncsc.gov.uk/section/exercise-in-a-box/using-passwords>. Accessed 22 Nov. 2024.
4. **CyberNews.** "RockYou2024: Largest Password Compilation Leak." *CyberNews*, <https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/>. Accessed 22 Nov. 2024.
5. **Expert Insights.** "The Most Significant Password Breaches." *Expert Insights*, <https://expertinsights.com/insights/the-most-significant-password-breaches/>. Accessed 22 Nov. 2024.
6. TryHackMe. "Cyber Security Training." *TryHackMe*, <https://tryhackme.com/>. Accessed 22 Nov. 2024.