# Brute-Force-Angriffe

Ein Passwort, bestehend aus **8 Kleinbuchstaben** (26 Möglichkeiten pro Buchstabe), hat **208.827.064.576** mögliche Kombinationen (etwa **200 Milliarden**). Wie lange würde ein moderner Rechner, deiner Einschätzung nach, brauchen, um alle Passwortvarianten zu testen, und das Passwort zu knacken?

→→ Die erschreckende Antwort ist: ungefähr **anderthalb Minuten**.

Solche Cyberattacken, bei denen einfach "durchprobiert" wird, werden als **Brute-Force-Angriffe** bezeichnet.

Aber was genau sind **Brute-Force-Angriffe** und wie funktionieren sie? Welche **Methoden** gibt es, um sich vor diesen Angriffen zu **schützen**?

# Brute-Force-Angriffe einfach erklärt

Ein **Brute-Force-Angriff** ist eine Methode, bei der ein Angreifer alle möglichen Kombinationen von Zeichen, Zahlen und Symbolen in einem Passwort ausprobiert, um das tatsächliche Passwort zu ermitteln. Hierbei steigt der Aufwand **exponentiell** mit der Anzahl der Zeichen des Passworts.

Aufgrund der **schnellen Rechenleistung** moderner Computer werden Brute-Force-Angriffe immer effektiver. Aus diesem Grund ist es wichtig, lange und sichere Passwörter zu verwenden (nicht drei Buchstaben, wie es noch in einem nicht näher benannten Unternehmen üblich ist), damit du dich vor diesen Angriffen schützen kannst.

> Ein **Brute-Force-Angriff** ist eine Technik, bei der ein Computerprogramm **alle möglichen Zeichenkombinationen** eines Passwortsystems durchprobiert, um das tatsächliche Passwort zu ermitteln. Deswegen spricht man auch von der **„Methode der rohen Gewalt“**.

Der geneigte Leser kann hier sein Wissen verfeinern, indem er auf den Pfeil klickt und dort tiefergehende Informationen zu diesem Thema findet. Da euch das auch privat passieren kann, würde ich empfehlen, diese paar Minuten Extra-Lesezeit zu investieren.

| **Arten von Brute-Force-Angriffen** |
| --- |

### Einfache Angriffe

Einfache **Brute-Force-Angriffe** sind Angriffsmethoden, bei denen Hacker Passwörter erraten, indem sie systematisch Kombinationen aus Wörtern, Buchstaben und Zeichen durchprobieren. Diese Technik kann sowohl manuell als auch durch Bots durchgeführt werden. Einfache Brute-Force-Angriffe sind jedoch nicht erfolgreich gegen längere und komplexere Passwörter.

→→ Trotzdem bleibt einfache Brute-Force eine Gefahr, da **viele Nutzer einfache Passwörter wählen**.

### Wörterbuchangriffe

**Wörterbuchangriffe** sind eine Form von Brute-Force-Angriffen, die auf komplexere Passwörter abzielen. Diese Angriffe unterscheiden sich von einfachen Brute-Force-Angriffen durch das Verwenden einer **vordefinierten Liste** von Wörtern, Namen, Daten und **häufig verwendeten** Passwörtern. Der Angreifer durchsucht die Liste und versucht jeden Eintrag als Passwort, bis er eine Übereinstimmung findet.

Im Vergleich zu einfachen Brute-Force-Angriffen sind **Wörterbuchangriffe wirksamer**, da sie häufig verwendete Wörter und Namen in ihre Überprüfung einbeziehen und somit die Möglichkeit haben, leicht erratbare Passwörter zu knacken. Da viele Benutzer einfache Passwörter aus Wörtern oder Namen verwenden, sind Wörterbuchangriffe eine wirksame Methode für Angreifer, Zugang zu geschützten Systemen zu erlangen.


**Hybride Angriffe**

**Hybride Brute-Force-Angriffe** sind eine Kombination aus einfachen **Brute-Force-Angriffen und Wörterbuchangriffen**. Hierbei versucht der Angreifer, das Passwort durch systematisches Durchprobieren von Kombinationen aus Wörtern, Buchstaben und Zeichen zu erraten. Die Methode kombiniert jedoch auch die Verwendung einer **vordefinierten Liste** von Namen, Daten und anderen häufig verwendeten Passwortkomponenten.

→→ Diese Kombination erhöht die Wahrscheinlichkeit, das korrekte Passwort zu erraten, da sie sowohl einfache, häufig verwendete Passwörter als auch komplexere Passwörter abdeckt.

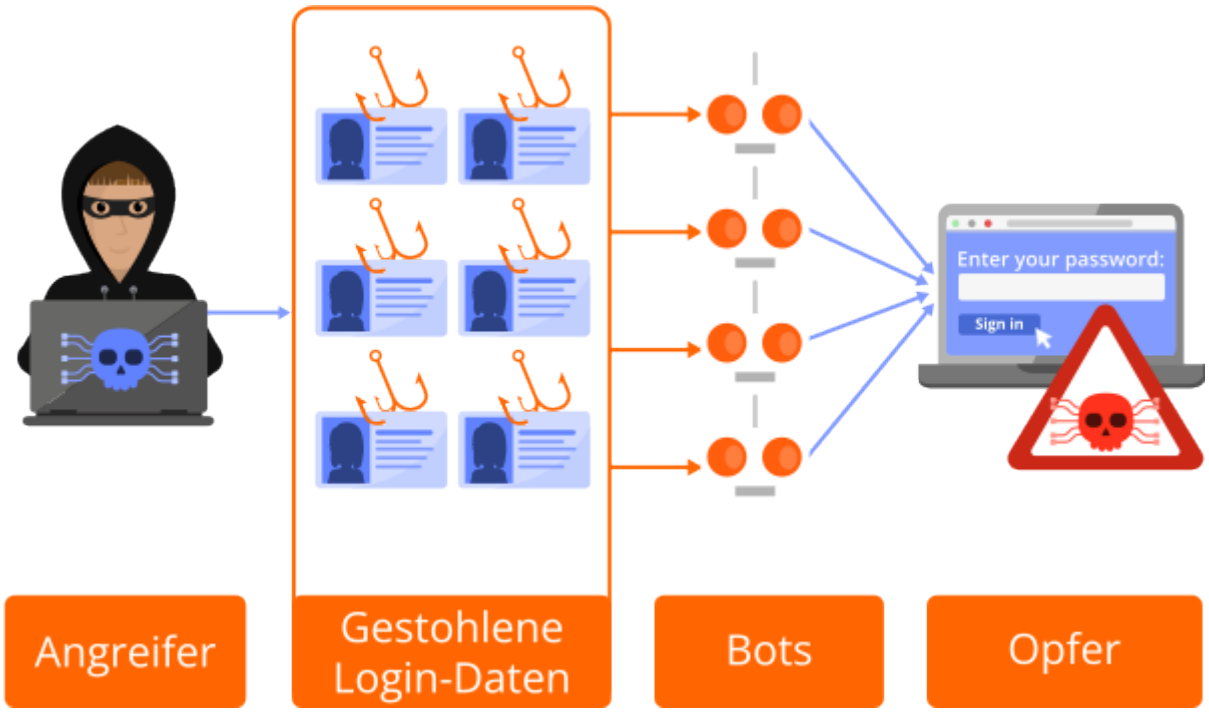
### Umgekehrte Angriffe

**Umgekehrte Brute-Force-Angriffe** sind eine spezielle Form der Brute-Force-Angriffe, bei denen der Angreifer das Ziel hat, **den Benutzernamen anstelle des Passworts zu ermitteln**. Hierbei wird mit einem bekannten oder häufig verwendeten Passwort begonnen und mittels Brute-Force-Methoden versucht, den zugehörigen Benutzernamen zu finden. Diese Art von Angriff wird häufig durch **Datenlecks im Internet** ausgelöst, bei denen kompromittierte Passwörter öffentlich gemacht werden.

### Credential Stuffing

**Credential Stuffing** ist ein Brute-Force-Angriff, bei dem ein Hacker gestohlene Benutzernamen und Passwörter nutzt, um zu versuchen, sich mit diesen Anmeldedaten auf verschiedenen Webseiten einzuloggen. Diese Daten werden häufig aus **Datenlecks** von Unternehmen und Webseiten gewonnen und im **Dark Web** verkauft.

Wenn ein Benutzer dasselbe Passwort oder denselben Benutzernamen auf mehreren Webseiten verwendet, kann ein kompromittiertes Konto zu einem **Sicherheitsrisiko** für alle anderen Konten werden, da der Hacker mit den gleichen Anmeldeinformationen auf diesen Konten Zugang erhält.



# Brute-Force-Angriffe verhindern

Es gibt verschiedene Methoden, um Brute-Force-Angriffe zu verhindern:

### Starkes Passwort

Wenn du dich vor Brute-Force-Angriffen schützen möchtest, ist es wichtig, **sichere Passwörter** zu verwenden. Ein sicheres Passwort ist ein Passwort, das schwer zu erraten ist und aus einer **Kombination von Buchstaben, Zahlen und Sonderzeichen** besteht. Es sollte **mindestens 12 Zeichen lang sein** und nicht aus Informationen bestehen, die leicht öffentlich verfügbar sind, wie deinem Namen, Geburtsdatum oder Adresse. Verwende für jeden Online-Account ein **einzigartiges Passwort** und vermeide es, dieselben Passwörter auf mehreren Websites zu verwenden.

Wenn es dir schwerfällt verschiedene Passwörter zu merken, kannst du einen **Passwort-Manager** verwenden, der diese für dich sicher speichert und automatisch einträgt, wenn du dich auf einer Webseite anmelden möchtest. Auf diese Weise musst du dir nur noch ein **Master-Passwort** merken und der Passwort-Manager kümmert sich um den Rest.

### gesalzenes Kennwort - Salt hinzufügen

**Salting** ist eine Technik, um Brute-Force-Angriffe zu **erschweren**. Hierbei wird ein zufälliger Wert, der sogenannte **Salt**, zum Passwort hinzugefügt, bevor es verschlüsselt wird. Diese Kombination aus Salt und Passwort wird dann gespeichert. Jedes Mal, wenn das Passwort benötigt wird, zum Beispiel bei der Anmeldung, wird der Salt zum Passwort hinzugefügt und die Kombination verglichen.

Wenn Dein Kennwort schlichter lautet und angenommen, die Eurobaustoff-Seite unterstützt salting, und würde zu deinem Kennwort als Salt deine Eurobaustoff-Mitgliedsnummer zufügen, sagen wir 1031, dann würde dabei folgendes rauskommen:

schlichter1031 --> wird verschlüsselt und als *58cccb8a5fa6fbaf8c7cf5b4bc14e5af2b50f064* in der Datenbank gespeichert.

Dies macht es für Hacker schwieriger, Passwörter mit Brute-Force-Methoden zu erraten, da sie nicht nur das Passwort kennen müssen, sondern auch den Salt, der für jeden Benutzer unterschiedlich ist.

Das bedeutet, wenn ein anderer Kollege auch das Kennwort schlichter verwendet aber seine Mitgliedsnummer (und damit sein Salt) 1421 ist, sieht sein verschlüsselter Datenbankeintrag so aus 1eec242af939bb26caf6399fbc5359ab80874075

Diese zusätzliche Schicht an Sicherheit erhöht den Aufwand für Hacker und macht es so unwahrscheinlicher, dass sie erfolgreich sein werden.

Das Salting wird in der Regel von Webseiten selbst implementiert und ohne euer Zutun geregelt.

### Zwei-Faktor-Authentifizierung

**Zwei-Faktor-Authentifizierung (2FA)** ist eine Methode der Überprüfung eines Benutzerkontos, bei der neben dem Passwort ein zusätzliches Sicherheitselement, wie zum Beispiel ein **SMS-Code** oder ein **Token**, verwendet wird. Das kennt ihr ja schon von eurem Microsoft-Konto

Bei einer zweistufigen Authentifizierung muss ein Benutzer nicht nur sein Passwort eingeben, sondern auch eine zusätzliche Überprüfung ausführen, um auf das Konto zuzugreifen. Dies kann beispielsweise durch die Verwendung einer App wie Google Authenticator oder durch die Eingabe eines SMS-Codes erfolgen, der an das Mobiltelefon des Benutzers gesendet wird.

Die zweistufige Authentifizierung bietet eine **höhere Sicherheit**, da es für einen Hacker schwieriger ist, sowohl das Passwort als auch den zusätzlichen Überprüfungscode zu erraten oder zu stehlen. Daher ist es eine empfohlene Maßnahme, um deine Konten vor Hackerangriffen zu schützen.


### Limitierung der Anmeldeversuche und CAPTCHAs

Die **Limitierung der Anmeldeversuche** bezieht sich darauf, die Anzahl der erlaubten Anmeldeversuche innerhalb eines **bestimmten Zeitintervalls** zu begrenzen. Das kennt so ziemlich jeder von uns: drei mal das falsche Kennwort und das Konto ist erstmal zu. Das ist zwar häufig nervig hilft aber dabei, Brute-Force-Angriffe zu verhindern, indem sie einem Angreifer die Möglichkeit nehmen, automatisierte Passwortberechnungen durchzuführen.

Eine andere Möglichkeit automatisierte Brute-Force-Angriffe zu verhindern sind **CAPTCHAs**. Diese stellen komplexe Aufgaben dar, die von einem menschlichen Benutzer gelöst werden können, aber für Computerprogramme viel schwieriger zu lösen sind. Somit kann man vor der Anmeldung herausfinden, ob es sich tatsächlich um einen Menschen handelt. Das kennt ihr als die nervigen Wimmelbilder, bei denen mal Autos, Boote oder Hydranten anklicken soll.

Wählen Sie alle Bilder mit **Kaffee** aus.


BESTÄTIGEN

# GAAAANZ Mathematisch!!!!

Damit ihr euch die Wichtigkeit KOMPLEXERER Kennwörter noch mal bildlich vor Augen führen könnt, ein paar Rechenbeispiele:

Nehmen wir an, jemand im Unternehmen hätte nur ein dreistelliges Kennwort, ausschließlich mit kleinen Buchstaben, dann ergibt das:

$26^3$ Kombinationsmöglichkeiten also 26x26x26. das ergibt 15.576 Kombinationsmöglichkeiten.

Erscheint erstmal viel, aber der selbst der billigste Werbegeschenktaschenrechner, den ihr in den Tiefen euerer Schränke und Rollwagen finden könnt, würde maximal etwas 4-5 Stunden brauchen um das Kennwort zu knacken. Jeder PC (selbst die lansamsten in unserem Betrieb) oder auch SmartPhones brauchen dafür nichtmal eine Sekunde.

Jetzt nehmen wir einfach mal Zahlen hinzu, bleiben aber dreistelling: Also $(26+10)^3$, was dann schon 238.328 Kombinationen sind. Macht schon was her, oder? Für einen PC immer noch nix. Ein zehn Jahre alter Standard-PC macht das in zweieinhalb Sekunden.

Hauen wir jetzt mal einen raus. 8 Zeichen, Zahlen, Buchstaben, Groß- und Kleinschreibung und ein Sonderzeichen. Das ergibt 6.095.689.385.410.816 (fast 6,1 Billiarden) Kombinationsmöglichkeiten. Ein aktueller HighEnd-Gaming-PC würde dafür schon 1-2 Tage brauchen.

Jetzt drehen wir mal ganz durch und folgen den Empfehlungen des BSI: 12 Stellen, Zahlen, Buchstaben in Groß- und Kleinschreibung und Sonderzeichen (beliebig viele an beliebiger Stelle) ergibt: 475.920.314.814.253.376.475.136 also etwa **475 Sextillionen** mögliche Kombinationen!

Das macht ein solches Passwort extrem sicher – mit Brute-Force ist es praktisch unmöglich, dieses in absehbarer Zeit zu knacken.

Revision #3
Created 27 January 2025 12:38:27 by Thomas Fried
Updated 27 January 2025 15:03:40 by Thomas Fried