

# **Ataque de força bruta**

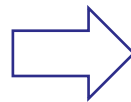
# Ataque de força bruta

- É um tipo de ataque utilizado pelo malfeitor para descobrir as credenciais de um sistema na qual ele não possui acesso.
- Baseia-se na técnica de tentativa e erro, onde o malfeitor submete diversas combinações de usuário e/ou senha, até encontrar a combinação que concede acesso.
- Pode ser feita manualmente ou através de uma ferramenta de automação
  - A malfeitor pode optar por utilizar um ataque manual caso conheça informações da conta

# Ataque de força bruta

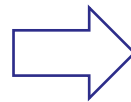
Frequentemente utiliza-se alguma ferramenta de automação.  
Por exemplo:

```
POST /users/authenticate
JSON
1 {
2   "login": "gabriel",
3   "password": "$i4A9302*"
4 }
```



```
200 OK 11.2 ms 20 B
Preview
1 {
2   "status": "Success"
3 }
```

```
POST /users/authenticate
JSON
1 {
2   "login": "gabriel",
3   "password": "123"
4 }
```



```
401 Unauthorized 372 ms 32 B
Preview
1 {
2   "status": "Invalid credencials"
3 }
```

# Ataque de força bruta

- O ataque por força bruta gera milhões de combinações, até encontrar a combinação que retorna o resultado que indica sucesso na autenticação

A	AA	BA		ZA	AAA	ABA		ZZA
B	AB	BB		ZB	AAB	ABB		ZZB
C	AC	BC		ZC	AAC	ABC		ZZC
D	AD	BD	...	ZD	AAD	ABD	...	ZZD
E	AE	BE		ZE	AAE	ABE		ZZE
F	AF	BF		ZF	AAF	ABF		ZZF
G	AG	BG		ZG	AAG	ABG		ZZG
...	...	...		...	...	...		...
Z	AZ	BZ		ZZ	AAZ	ABZ		ZZZ
	⏟				⏟			
26	676				17576			

# Ataque de força bruta

- A quantidade de tentativas depende de dois fatores:
  - O tamanho do mapa de caracteres utilizado
  - O tamanho da senha
- Para uma senha de tamanho variável, a quantidade de possíveis valores é calculada com a fórmula:

$$\sum_{i=\min}^{\max} tam^i$$

Onde:

min: extensão mínima

max: extensão máxima

tam: tamanho do mapa

# Exemplo

Considerar que a senha pode ser composta somente por letras minúsculas e maiúsculas sem acento (a..z, A..Z) e dígitos (0..9) e extensão de 4 à 8 caracteres. A quantidade de combinações distintas é:

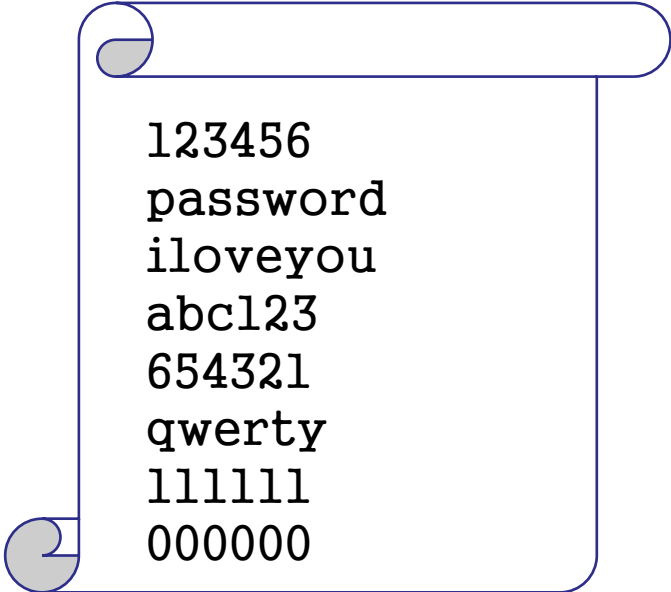
$$\sum_{i=4}^8 62^i = 62^4 + 62^5 + 62^6 + 62^7 + 62^8$$
$$= 221.919.451.335.856 \text{ combinações}$$

# Exemplo

- Se cada combinação consumir 1 segundo para ser realizada, testar todas as combinações levaria 7.037.019 anos.
- O tempo médio para identificar a combinação correta seria a metade do tempo (ou seja, 3.518.509 anos).
- O ataque de força bruta pode ser feito com processamento paralelo

# Ataques de dicionário

- Ao invés de explorar todas as combinações possíveis, o ataque pode ser feito a partir de uma lista de palavras. A lista contém uma compilação de palavras conhecidas ou variações de palavras.



123456  
password  
iloveyou  
abc123  
654321  
qwerty  
111111  
000000

A lista é conhecida como “dicionário”. Por isso, o ataque também é conhecido como “ataque de dicionário”



# Ataques reversos

- Neste tipo de ataque, o malfeitor conhece previamente a senha, mas não conhece o usuário. Neste caso, o objetivo é encontrar o usuário.
- As combinações e tentativas buscam encontrar um usuário que possui a senha.
- Geralmente o malfeitor utiliza uma lista “vazada” de senhas

# Ataque de preenchimento de credenciais

- Este ataque considera que muitas pessoas reutilizam suas credenciais em vários sistemas.
- Neste caso, considerando que alguma credencial tenha vazado, o malfeitor pode explorar diversos sistemas, buscando acesso com tais credenciais

# **Restrição inadequada de tentativas excessivas de autenticação**

**CWE-307: Improper Restriction of Excessive Authentication Attempts**

# **Restrição inadequada de tentativas excessivas de autenticação**

- Todo software deveria implementar medidas para evitar tentativas de autenticação com falha em excesso
- Quando o software não adota medidas suficientes, torna o software sujeito à ataques de força bruta

# Como prevenir o ataque de força bruta

- Algumas formas de prevenir o ataque de força bruta envolvem:
  - Usar senhas “fortes”
  - Limitar tentativas de login
  - Bloquear contas
  - Utilizar autenticação multi-fator
  - Uso de CAPTCHA

# Senhas “fortes”

## Como prevenir o ataque de força bruta

- Não usar informações pessoais para escolha de senhas. Não utilizar data de nascimento, nome, endereço de email, etc.
- Não reusar senhas
- Usar senhas únicas para cada serviço
- Usar senhas longas (mais de 6 caracteres). O ideal seria utilizar senhas de 15 caracteres
- Utilizar mapas de caracteres extensos e exigir o uso de tipos de caracteres distintos (exigir letra minúscula, maiúscula, algarismos, símbolos especiais)
- Não utilizar palavras do dicionário. Usar caracteres aleatórios

# Limitar tentativas de login

## Como prevenir o ataque de força bruta

- Uma das alternativas é limitar a quantidade de tentativas mal sucedidas de autenticação para um usuário num determinado período de tempo.
  - Exemplo: no intervalo de 30 minutos, o usuário pode errar no máximo 5 vezes a senha
- Além disso, pode ser implementada funcionalidade para bloquear a conta do usuário
  - Requer construir um recurso para desbloquear a conta
  - Pode possibilitar que o malfeitor utilize este recurso para causar indisponibilidade

# Autenticação multifator

## Como prevenir o ataque de força bruta

- A autenticação multifator (*multi-factor authentication* - MFA) é um método de autenticação que usa dois ou mais fatores para confirmar a identidade de uma pessoa
- Inicialmente o usuário informa seus dados de autenticação (usuário e senha, por exemplo) e em seguida, serão solicitados os próximos fatores que podem ser:
  - Fator de conhecimento
  - Fator de posse
  - Fator de inerência
  - Fator baseado em localização

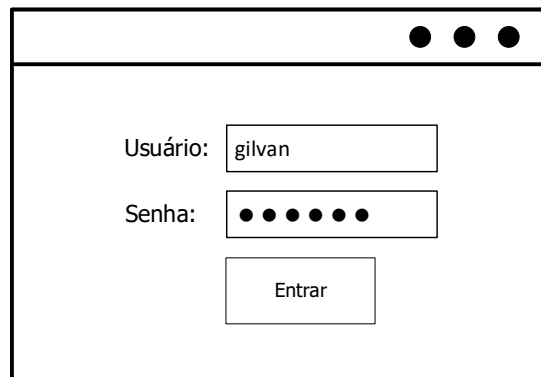


# Autenticação multifator (MFA)

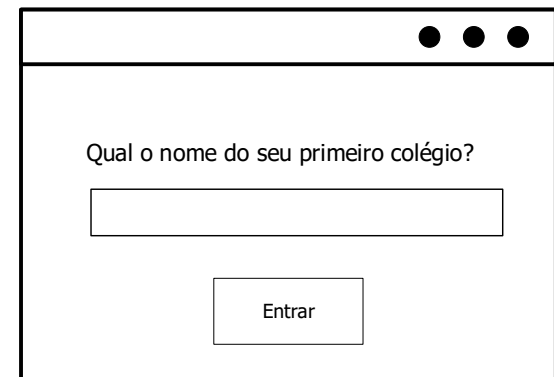
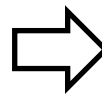
Como prevenir o ataque de força bruta

**Fator de conhecimento.** Neste fator, o usuário deve provar que conhece (sabe) alguma informação. Pode ser:

- Número de identificação pessoal (PIN)
- Senha
- Resposta de “perguntas secretas”



A diagram of a web browser window showing a login form. It has two input fields: 'Usuário:' with the text 'gilvan' and 'Senha:' with six dots. Below the fields is an 'Entrar' button.



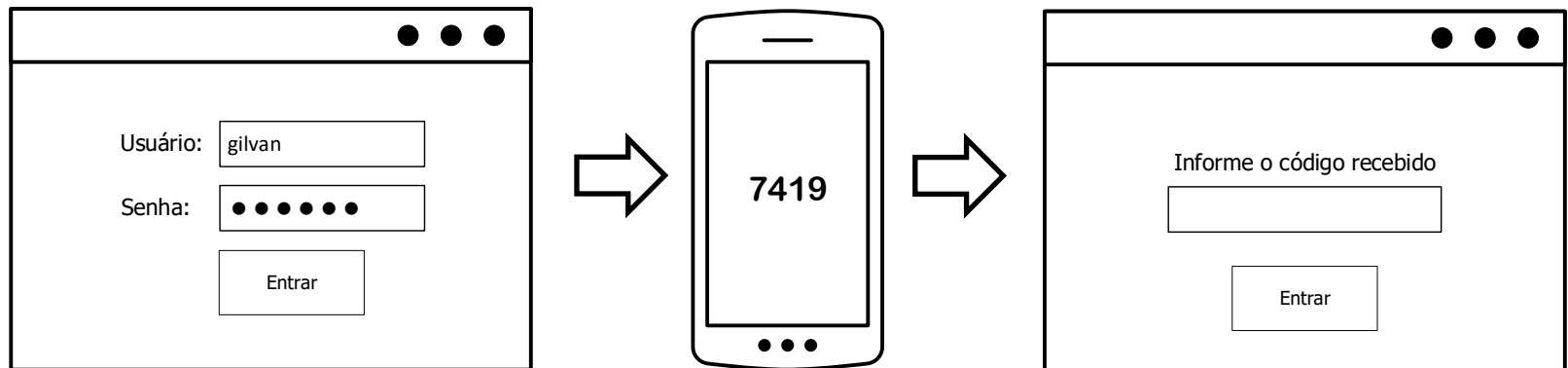
A diagram of a web browser window showing a second step in the login process. It asks 'Qual o nome do seu primeiro colégio?' with a single input field below it and an 'Entrar' button at the bottom.

# Autenticação multifator (MFA)

Como prevenir o ataque de força bruta

**Fator de posse.** Neste fator, a pessoa deve provar que possui determinado item físico ou acesso a algum recurso. Pode ser:

- Celular
- Email
- Chave de segurança física

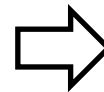
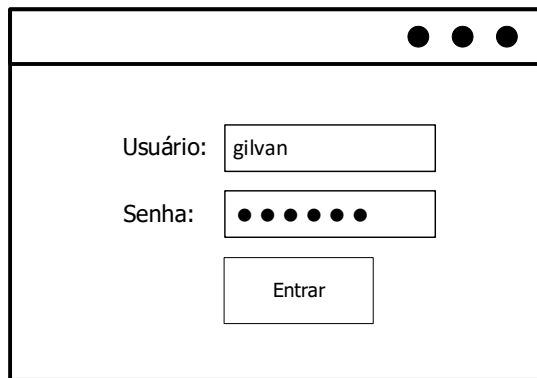


# Autenticação multifator (MFA)

Como prevenir o ataque de força bruta

**Fator de inércia.** Um atributo pessoal, normalmente obtido através de recurso biométrico. Pode ser:

- Face
- Impressão digital
- Leitura de iris
- Impressão de voz



# Autenticação multifator (MFA)

Como prevenir o ataque de força bruta

**Fator baseado em localização.** Valida a localização em que a pessoa está. Pode ser:

- GPS
- Conexão a uma rede específica

# CAPTCHA

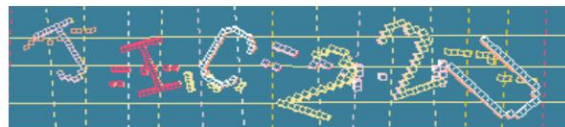
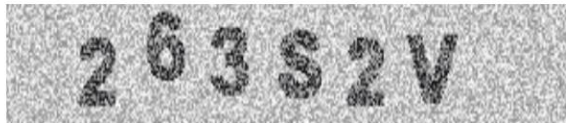
## Como prevenir o ataque de força bruta

- A fim de dificultar a ação de um ataque de força bruta via automação, utilize-se um teste em seja fácil para um humano realizar, mas difícil para ser resolvido por um programa.
- CAPTCHA vem de *Completely Automated Public Turing test to tell Computers and Humans Apart* (“Teste de Turing Público Completamente Automatizado para Diferenciar Computadores e Humanos”)

# CAPTCHA

## Como prevenir o ataque de força bruta

- O CAPTCHA baseado em texto utiliza letras e números aleatórios, com combinações de escala, rotação e distorção de caracteres. Também podem ser combinados com outros elementos gráficos, como linhas, pontos.
- Exemplos:



# CAPTCHA

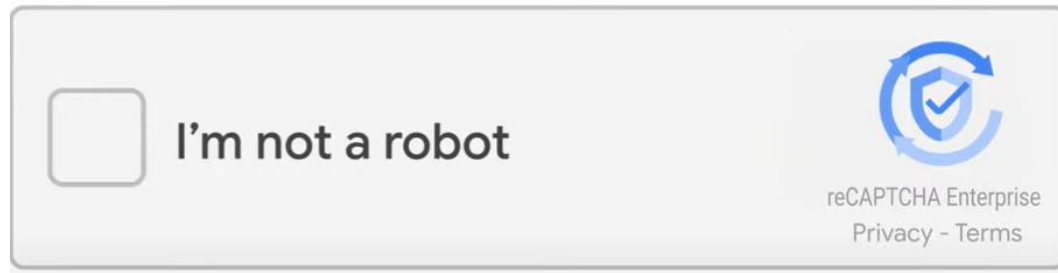
## Como prevenir o ataque de força bruta

- O CAPTCHA baseado em imagens geralmente requer que o usuário selecione imagens que combinam com um tema.
- São mais difíceis de serem interpretados por bots.



# reCAPTCHA

- Utiliza apenas uma caixa de seleção “Eu não sou um robô” que o usuário deve clicar.



- Captura os momentos do usuário e outros movimentos para identificar se assemelha à atividade humana ou a um bot. Direciona para um CAPTCHA tradicional caso não seja possível diferenciar.
- Trata-se de uma variação do CAPTCHA do Google.



# CAPTCHA

## Como prevenir o ataque de força bruta

- Alguns obstáculos do CAPTCHA:
  - Pode ser frustrante para o usuário
  - Pode ser difícil para ser reconhecido para alguns públicos
  - Pode ser difícil para ser reconhecido em alguns dispositivos