**Segurança da informação: implementação de medidas de segurança para mitigar ataques *Brute Force* sobre HTML**

Gustavo Henrique de Carvalho

Kenny Giuliano Gonçalves de Oliveira

Eduardo Luis de Souza Lima

Vitor Henrique Moraes Mancinelli

Nicolas Matheus Rodrigues Viena

Rubens de Jesus Nogueira

Vinicius Afonso de Freitas Mendes

Prof. Me. Rodrigo Rodrigues

# RESUMO

1. Nesse artigo por meio de experimentos científicos e utilizando as funcionabilidades que o editor de código-fonte, Visual Studio Code, nos permite e também o pacote de servidores abertos XAMPP. Usamos o Visual Studio Code, é um programa que é utilizado para edição, interpretação e desenvolvimento de códigos, o qual possui as funcionalidades simples, como: edição de código de várias linguagens de programação , terminal de comandos e controle de versão, onde nesse artigo daremos foco a linguagem Python onde e apresentaremos um script de ataque com o XAMPP sendo utilizado para iniciar um servidor tanto para a página web ( com o uso para a demonstração de como se decorreram os processos), quanto para o banco de dados, e com a interfase web serão efetuados testes em sequência utilizando uma página web desenvolvida usando tecnologias, como: HTML, CSS, PHP, Javascript, onde, com o mesmo usuário e senhas com padrões pré-definidos para se analisar e averiguar não só a metodologia necessária para se aplicar uma técnica de ataque de força bruta deis do seu princípio como também sua efetividade em exemplos, e também nós iremos por meio desses mesmos testes demostrar o tempo necessário para se descobrir senhas e métodos para a aprimoração das senhas para diminuir as possiblidades desse tipo de técnica de ataque, assim como também mostraremos alguns limites da técnica!

**Palavras-chave:** força-bruta, multiprocessos, tempo, invasão e vulnerabilidade.

# *ABSTRACT*

*In this article, through scientific experiments and using the features that the Visual Studio Code source code editor allows us and also the XAMPP open server package, Visual Studio Code is a program that is used for editing, interpreting and developing codes .*

*Visual Studio Code has simple functionalities such as: code editing of several programming languages ​​and command terminal and version control. In this article, we will focus on the Python language, where we will present an attack script and XAMPP being used to start a server both for the web page (used to demonstrate how the processes took place), and for the database. . And with the web interface tests will be carried out in sequence using a web page developed using technologies such as: HTML, CSS, PHP, Javascript. The same username and passwords with pre-defined patterns to analyze and verify not only the methodology necessary to apply a brute force attack technique of its principles but also its effectiveness in examples. Also, we will, through these same tests, demonstrate the time needed to discover passwords and methods for improving passwords to reduce the possibilities of this type of attack technique, as well as showing some limits of the technique.*

*Keywords: brute force, multiprocesses, time, invasion and vulnerability.*

# INTRODUÇÃO

Com base nos dados oferecidos em MICROSOFT (2022) e DEVELOPER MOZILLA(2022) é possível compreender que existem muitas formas para pessoas com más intenções causar danos, muitas vezes irreversíveis, sobre o usuário e/ou os recursos de Tecnologia da Informação (TI), porém, este artigo pretende aprofundar sobre o funcionamento e prevenção de um estilo de ataques em especifico chamado, *Brute Force*, onde daremos foco nele em um ambiente HTML.

Baseando no site STARTI (2022) a tradução literária para “*brute force*” é “força bruta”, neste tipo de ataque, o invasor tenta diversas combinações de senha ou as mais usadas até que ele acerte e consiga invadir a conta do usuário, um outro ponto apresentado por STARTI (2022) é sobre a quantidade deste tipo de ataque, que tem aumentado significativamente desde 2020, um crescimento de 73%. É importante que este tipo de ataque tenha relevância e seja levado em consideração como uma das principais formas de invasão.

De acordo com BRASILCLOUD (2022) a forma mais utilizada é através de programas que utilizam bibliotecas pré-definidas ou personalizadas. Onde o mais básico nível de proteção seria senhas fortes, que teriam muitos caracteres, números, letras maiúsculas e minúsculas. E, um exemplo, de um mais “avançado” seria algo como minimizar a quantidade de tentativas que um usuário pode errar a senha.

Mas a técnica vai além disso, mostraremos alguns limites para determinadas situações, como limite de hardware ou do tempo que seria necessário para quebrá-lo. Mas mostraremos qual seria a contagem e possibilidades. Além de métodos de proteção que inviabilizam ou dificultam de forma significativa o método.

# OBJETIVOS

**Objetivo geral**

Este artigo tem por fim propor formas viáveis de mitigar ataques do tipo *Brute Force* sobre um ambiente Web.

**Objetivos específicos**

Objetivo específico 1: pesquisar sobre cibersegurança para compreender a dinâmica de ataques cibernéticos em HTML.

Objetivo específico 2: pesquisar sobre recursos de defesa cibernética para relacionar quais defesas permitem mitigar ataques do tipo *Brute Force*.

Objetivo específico 3: a partir do conhecimento adquirido através dos objetivos específicos 1 e 2, propor métodos e/ou ferramentas que possam mitigar ataques *Brute Force*.

# METODOLOGIA

Este artigo foi baseado em pesquisa literária para cumprir com os objetivos específicos 1 e 2. Outrossim, também foi baseado em pesquisa aplicada que apresentará testes de ataques *Brute Force,* sobre algumas características, sobre HTML, onde o objetivo principal é mostrar métodos de mitigar ataques e conscientizar sobre os métodos de defesa para os tipos de ataques presentes, e tipos de ataques onde o estudo de caso por pesquisa aplicada se dá através de levantamento de dados obtidos através da análise de resultados obtidos através dos exemplos nas ferramentas utilizadas.

Para a elaboração da página web foram usadas as ferramentas citadas: HTML, a qual se baseia em uma linguagem de hipertexto que define a estrutura e significado do conteúdo web, geralmente são usadas para descrever a aparência ou a funcionalidade do website. O HTML usa uma espécie de marcação para imprimir textos, imagens e outros conteúdos para exibição em um navegador. Os elementos presentes no HTML são separados em um documento por “tags”, no qual baseiam-se no nome do elemento entre “<” (menor) e “>” (maior) que podem ser vários itens como títulos, parágrafos ou imagens, entre outros.

Onde também foi utilizado na página web para melhorar as características visuais junto a ela o CSS (Cascading Style Sheets). O código CSS pode ser aplicado diretamente nas tags ou ficar contido dentro das tags <style>. Também é possível, em vez de colocar a formatação dentro do documento, criar um link para um arquivo CSS que contém os estilos. Além também da utilização do JavaSript que é uma linguagem de programação interpretada estruturada, de script em alto nível com tipagem dinâmica fraca e multiparadigma. Juntamente com HTML e CSS, o JavaScript é uma das três principais tecnologias da World Wide Web.

A linguagem Javascript, que é uma parte essencial deste projeto do website, é a linguagem mais popular da programação, isto é, devido ao fato de ela ser uma linguagem extremamente flexível e multifacetada, ou seja, pessoas usuárias interajam com página e a tore muito mais dinâmica para o usuário.

Outra linguagem usada em abundancia seria a linguagem PHP que seria uma linguagem interpretada livre, que é seria usada originalmente apenas para o desenvolvimento de aplicações presentes e atuantes no lado do servidor. Alguns pontos interessantes sobre o PHP seria sua eficiência em relação ao seu desempenho para garantir a estabilidade da aplicação, a possibilidade de integração com diferentes bancos de dados como MYSQL, que será abordado mais a frente, além de suportar um processamento de um grande volume de dados com o consumo de poucos recursos do servidor.

As aplicações desenvolvidas em PHP podem ser desenvolvidas e utilizadas em sistemas operacionais como Windows, Linux, UNIX, e MacOS, sendo possível também ser instalada em plataformas em computações em nuvem e acessos permitidos por diferentes navegadores.

Após a criação do website, é iniciado o desenvolvimento da técnica de força bruta, o qual foi criado usando Python, uma linguagem de programação simples, multiplataforma e orientada a objetos que possibilita um maior controle e desempenho de códigos para projetos de grande proporção.

Durante os primeiros testes foi utilizada a ferramenta BurpSwitch como primeiro meio de ataque, mas após alguns testes e dificuldades encontradas para fazer a automatização, o próximo método e principal foi realizar o desenvolvimento de um scrip na linguagem de programação Python, utilizando algumas bibliotecas como: time, que foi utilizado para cronometrar o tempo para a quebra a senha, threading que foi utilizado para otimização na velocidade em que os POST (método de requisição suportada pelo HTTP) são feitos ao utilizar a URL selecionada passando a informação de login e senha, itertools, foi utilizado para gerar as combinações possíveis de senhas.

Para o gerenciamento do banco de dados, quanto o host do servidor está sendo usado o XAMPP que é um programa gratuito e multiplataforma em que consiste na simulação de um servidor web em seu próprio PC ou notebook. Além de ter mais desempenho, o desenvolvedor(a) não depende de conexão com a internet para usá-lo e está incluso os principais servidores de código aberto, como Apache HTTP Server, o MYSQL e principalmente o PHP.

Onde dentre os métodos de mitigação a forma mais comumente utilizada seria o rate limiting, ele é a identificação da origem de transferência de dados hostil que faz tentativas de acessos de uma rede (internet). Uma boa forma de segurança web que será mais explorada nos resultados, onde ele monitora a frequência e o cronometragem das requisições.

Por exemplo: Em uma página de login é muito comum ter limites. Todos os usuários cadastrados são capais de completar o processo de login no máximo de três tentativas a cada minuto, hora ou até dias isso vai ser definido pelos desenvolvedores. No sistema de login caso o usuário tenta três vezes e nas três tentativas a senha ou o usuário estiver errado ele só poderá tentar novamente depois de um tempo definido pelo sistema.

Outra maneira de defender-se sobre esse tipo de ataque que exploraremos é o reCAPTCHA *(completely automated public Turing test to tell computers and humans apart*) que foi criado no departamento de computação da Universidade Carnegie Mellon por um grupo, Luis von Ahn, Nicholas Hopper, and John Langford e liderado pelo Manuel Blum, teria a função de não só lidar com a quantidade de spam, mas também com a quantidade de bots, mas que aqui será aplicada para impedir o envio de senhas.

Por fim, para guardar as informações inseridas pelo usuário, para que ele possa acessar seu login, foi utilizada a linguagens de banco de dados MYSQL. O MYSQL, considerado como um gerenciador de dados relacional, é uma linguagem de código aberto usado em aplicações gratuitas para inserir, acessar e gerenciar o conteúdo armazenado num banco de dados.

Com a utilização das ferramentas MYSQL e PHP, para a criação do website, foi necessário um ambiente de testes, para realizar o desenvolvimento localmente. Para ser evitado o trabalho de usar um servidor HTTP remoto para desenvolver os testes iniciais na elaboração do site, o qual receberá o ataque pelo brute force, escolhemos usar a ferramenta denominada XAMPP.

Para a elaboração do arquivo que realizará a invasão à página HTML, utilizaremos o conceito de threads para a automatização da técnica brute force que será realizada.

Suas instruções são processadas no servidor em que o site exerce a hospedagem, retornando ao navegador e carregando tudo que foi processado. A linguagem de programação PHP funciona muito bem para construção de páginas HTML, pois ela é processada no momento que é executada, já que é uma linguagem de script. Dito isso, este pode ser inserido entre o código HTML, por dentro de tags que o interpretador possa reconhecer.

Onde entre os métodos utilizados para ser feita a inserção de senhas foi utilizando threads que são fluxos de programas que executam em paralelo dentro de uma aplicação, ou seja, são executados de forma independente e escalonada apesar do fluxo inicial de uma aplicação. Caso compilemos o arquivo de ataque usando threads, para descobrir a senha do usuário as saídas podem variar até informar a senha correta, pois a alocação dos threads para execução no processador não é um processo determinado.

Usamos métodos diferentes de formas de *Brute Force* onde seus diversos modos de invasão podem ocorrer, por exemplo, de duas formas que são na vertical ou na horizontal, onde na vertical eles usam como base a senha que é testado vários tipos de senhas até encontra-lo, ou também da mesma forma para o nome do usuário, que seria a horizontal.

# DESENVOLVIMENTO

No desenvolvimento desse artigo utilizaremos ferramentas como o *Burp Suite*, software do fabricante *Port Swigger* (2022)para a automatização de ataques personalizados sobre aplicações web. Que pode ser encontrado e adquirido de forma gratuita através do site https://portswigger.net/users/register. Assim como um scrip utilizando a linguagem de programação Python para fazer as inserções de senhas na página HTML desenvolvida, onde usaremos a versão 3.10, que pode ser adquirida em suas versões no site https://www.python.org/ por meio do menu onde pode ser escolhido todas as versões da linguagem, onde precisa ser escolhido o próprio sistema operacional que é realizado o desenvolvimento, nesse artigo é usado a versão do Windows.

Foi realizada uma simulação de uma situação em tempo real para a realização do ataque, onde é usado uma página web, criada pelo nosso grupo, no intuito de mostrar uma ação cotidiana em que um usuário acessa sua área local da empresa, no qual irá consistir em que ele precise entrar na página de login para que enfim ele possa acessar a tela principal.

A página Web criada está utilizando o HTML, CSS, JavaScript orientado a objeto, e PHP. O HTML é usado para criar as páginas de login e painel do paciente, o CSS é usado para estabilizar os componentes das páginas web, o Javascript é usado para os avisos e animação do painel do paciente, o PHP é usado para fazer a conexão com o banco de dados, POO (programação orientado a objeto) foi usado para manter uma organização e reutilização de trechos de códigos.

Está sendo utilizado uma página Web fictícia de um hospital, que foi desenvolvida no intuito de mostrar as invasões na área de login, onde é testado as senhas possíveis do usuário.

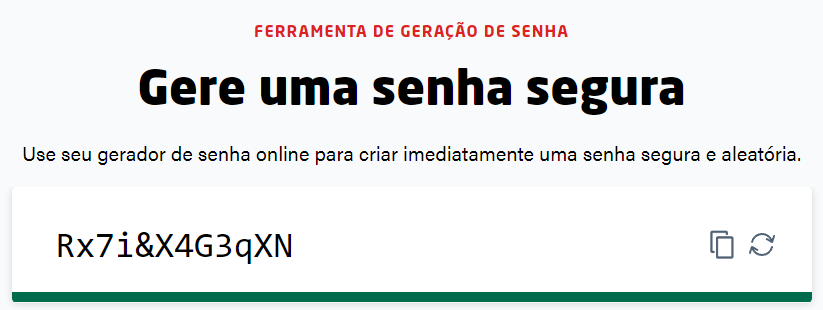
O primeiro teste é um exemplo simples e irreal de uma senha com apenas 1 carácter, onde iremos mostrar de forma gradual e proporcional no número de caracteres na senha, como também no tipo, passando de número para letra, além dos resultados que levara as medidas de tempo para cada caractere a mais. Em resumo será mostrado os resultados de 1 a 5 caracteres e sua diferença de tempo entre os resultados, onde também apresentaremos as possibilidades possíveis de 6 a 8 unidades onde mostraremos os valores referentes a quantidade de possibilidades.

O ataque seria ocorre a partir do scrip de Python que monta as combinações possíveis que usando a quantidade e o tipo de caractere utilizado no método POST para tentar as combinações possíveis através da regra da senha testada.

Encontramos três principais tipos de defesa que irá mitigar de forma significante e tornara inviável o método do brute force, o RateLimit, o reCAPTCHA e senhas caracterizadas de forma aleatória com tipos diferentes de caracteres. No RateLimit nós testaremos um método que previna o ataque através da limitação de tentativa por tempo, onde após um determinado número de tentativas ele irá parar as requisições por um certo tempo. Em nosso caso foi utilizado para a cada a três tentativas ele para por 10 segundos, onde...

Já no reCAPTCHA ele foi criado inicialmente como uma forma de limitar o acesso de bots e spam, mas ele é utilizado aqui para não permitir que ele passe a senha sem passar pelo teste de turing que vai dificultar o avanço. Onde por causa disso ele coloca as senhas, mas por não habilitar o reCAPTCHA mesmo com a senha correta ele não irá passar por ele.

Agora o método das senhas caracterizadas mais é do que uma senha forte com muitos caracteres aleatórias e muitas características diferentes, por exemplo o site: https://www. lastpass.com /pt/features/password-generator, ele consegue gerar senhas muito fortes a partir de uma simples configuração, como apresentado na imagem a baixo:



Onde tem uma senha bem forte, com várias características que dificultariam o uso da técnica, mas mesmo sendo um meio simples de solucionar, não é algo que uma pessoa faria pela dificuldade de lembrar ou de escrever toda vez que fosse necessário entrar, ainda mais se fosse varias senhas dessa maneira pra cada lugar que a pessoa possua uma senha.

# RESULTADOS

A partir da pagina web os resultados obtidos foram os seguintes:

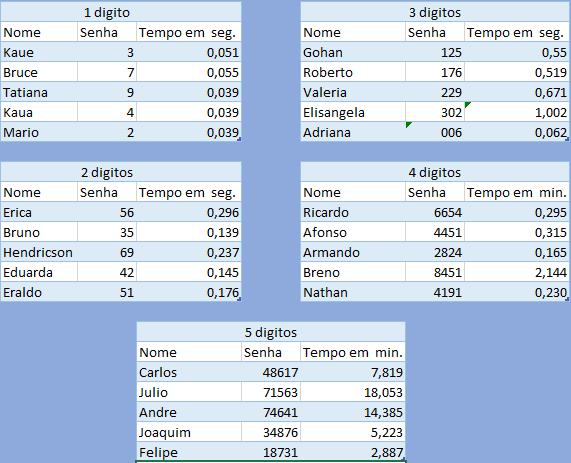
Usando um computador com as configurações: Um Processador Ryzen 7 5700x, nas

Memórias RAM 2x16 GB de 3200MHz DDR4;



Usando um Notebook com as configurações: Um Processador Intel i7 7700hq, em uma

Memória RAM 1x16 GB de 2400MHz DDR4:



Os testes realizados foram de 1 a 5 caracteres numérico, e para letras de 1 a 4 apenas minúsculo, apenas maiúsculo e a versão mista aleatória de 1 a 4.

Os testes realizados foram em dois dispositivos um notebook e um computador note que as configurações do computador são melhores que o notebook tendo o dobro de memória RAM e um processador AMD 52% mais rápido do que o processador da Intel.

# CONSIDERAÇÕES FINAIS

A partir deste trabalho de conclusão de curso, em que escolhemos como tema “implementação de medidas de segurança para mitigar ataques Brute Force”, o qual passamos por intensos estudos, pesquisas e testes consistidos em aplicar a técnica em um ambiente web, desenvolvido pelo nosso grupo, com o intuito de apresentar uma situação em tempo real, concluímos que

# FONTES CONSULTADAS

DONDA, Daniel, (2018). Banco de dados de senhas. Disponível em: https://github.com/danieldonda/wordlist. Acesso em: 13 set. 2022.

PIKI, Freepik, (`2022´). Médicos e Enfermeiros. Disponível em: https://br.freepik.com/vetores-gratis/obrigado-medicos-e-enfermeiros\_7965272.htm#query=medico&position=42&from\_v iew=search&track=sph. Acesso em: 6 out. 2022.

Momento Editorial, (2020). No último trimestre aumentaram os ataques “força bruta” na região. Disponível em: https://www.telesintese.com.br/brasil-teve-26-bilhoes-de-tentativas-de-ataques-ciberneticos-em-seis-meses/#:~:text=Seguran%C3%A7a-,Brasil%20teve%202%2C6%20bilh%C3%B5es%20de%20tentativas,ataques%20cibern%C3%A9ticos%20em%20seis%20meses&text=A%20Fortinet%20anunciou%20os%20resultados,cibern%C3%A9tica%20em%20todo%20o%20mundo. Acesso em: 23 set. 2022.

FERNANDES, Miriam, (2022). BRUTE FORCE: Tudo o que você precisa saber! Disponível em: https://blog.starti.com.br/brute-force/. Acesso em: 3 out. 2022.

FERNANDES, Vitor, (2019). Ataques de força bruta – Definição e prevenção. Disponível em: https://www.noticiastecnicas.com/ataques-de-forca-bruta-definicao-e-prevencao/. Acesso em: 1 out. 2022.

MAGALHÃES, Erasmo, (2021). Brute Force: O que é e Como se Prevenir. Disponível em: https://blog.brasilcloud.com.br/brute-force-o-que-e-e-como-se-prevenir/. Acesso em: 28 set. 2022.

Hive Systems, (2022). How Long It Would Take A Hacker To Brute Force Your Password In 2022, Ranked. Disponível em: https://digg.com/technology/link/how-long-it-takes-to-get-password-hacked-1IvDFspF6p. Acesso em: 26 set. 2022.

Wikipédia, (2022).HTML. Disponível em: https://pt.wikipedia.org/wiki/HTML. Acesso em: 25 sets 2022.

Wikipédia, (2022). Thread (computação). Disponível em: https://pt.wikipedia.org/wiki/Thread\_(computa%C3%A7%C3%A3o). Acesso em: 19 set 2022.

Rossum, Guido van. (2022). threading — Thread-based parallelism. Disponível em:

https://docs.python.org/3/library/threading.HTML. Acesso em: 3 out 2022.

Reitz, Kenneth. (2022). Quickstart. Disponível em: https://requests.readthedocs.io/en/latest/user/quickstart/. Acesso 30 ago 2022.

Wikipédia, (2022). Cascading Style Sheets. Disponível em:

https://pt.wikipedia.org/wiki/Cascading\_Style\_Sheets. Acesso em: 28 ago 2022.

Wikipédia, (2022). JavaScript. Disponível em:

https://pt.wikipedia.org/wiki/JavaScript. Acesso em: 10 set 2022.

Icon, Scout. (2022). 4,500+ icon fonts and SVG icons with Unicons. Disponível em:

https://iconscout.com/unicons. Acesso em: 2 out 2022.

Wikipédia, (2022). PHP. Disponível em: https://pt.wikipedia.org/wiki/PHP. Acesso em: 23 jul 2022.

Wikipédia, (2022). XAMPP. Disponível em: https://pt.wikipedia.org/wiki/XAMPP. Acesso em: 12 ago 2022.

Wikipédia, (2022). Python. Disponível em: https://pt.wikipedia.org/wiki/Python. Acesso em: 22 ago 2022.

Hanashiro, Akira. (2021). VS Code - O que é e por que você deve usar?. Disponível em: https://www.treinaweb.com.br/blog/vs-code-o-que-e-e-por-que-voce-deve-usar. Acesso em: 15 set 2022.

Higa, Paulo. (2012). O que é XAMPP e para que serve. Disponível em: https://www.techtudo.com.br/noticias/2012/02/o-que-e-xampp-e-para-que-serve.gHTML. Acesso em: 28 set 2022.

Rossum, Guido van. (2022). Python is a programming language that lets you work quickly

and integrate systems more effectively. Disponível em: https://www.python.org/. Acesso em: 15 set 2022.

Swigger, Port. (2022). Burp Community. Disponível em: https://portswigger.net/users/register. Acesso em: 2 set 2022.

Blog, Aiqon. (2020). Rate Limit: Uma Parte Vital da Segurança Web Moderna. Disponível em: https://aiqon.com.br/blog/rate-limit-uma-parte-vital-da-seguranca-web-moderna/. Acesso em: 25 out 2022.

N-MIT, LEMELS. (2020). Luis von Ahn ReCAPTCHA, co-inventor of CAPTCHA & Duolingo. Disponível em: https://lemelson.mit.edu/resources/luis-von-ahn. Acesso em: 18 set 2022.

Burling, Stacey. (2012). CAPTCHA: The story behind those squiggly computer letters. Disponível em: https://phys.org/news/2012-06-captcha-story-squiggly-letters.HTML. Acesso em: 10 out 2022.

Garcia, Guilherme. (2021). ReCAPTCHA. Disponível em: https://www.ufsm.br/pet/sistemas-de-informacao/2021/08/16/recaptcha/#:~:text=Evolu%C3%A7%C3%A3o%20do%20ReCAPTCHA,apareciam%20em%20uma%20imagem%20distorcida. Acesso em: 14 out 2022.

Hosch, William L. (2022). CAPTCHA computing. Disponível em: https://www.britannica.com/technology/CAPTCHA. Acesso em: 30 set 2022.

Tech, Oráculo. (2017). O que é e para que serve o XAMPP?. Disponível em: https://oraculoti.com.br/2019/07/01/o-que-e-e-para-que-serve-o-xampp/. Acesso em: 13 out 2022

Bruno. (2015). MYSQL Tutorial. Disponível em: https://www.devmedia.com.br/MYSQL-tutorial/33309. Acesso em: 18 out 2022.

Noleto, Cairo. Javascript: o que é, aplicação e como aprender a linguagem JS. Disponível em: https://blog.betrybe.com/javascript/. Acesso em: 23 set 2022.

Contributors, MDN. HTML: Linguagem de Marcação de Hipertexto. Disponível em: https://developer.mozilla.org/pt-BR/docs/Web/HTML. Acesso em: 15 out 2022.

Noleto, Cairo. (2022). Javascript: o que é, aplicação e como aprender a linguagem JS. Disponível em: https://blog.betrybe.com/javascript/. Acesso em: 23 set 2022.

Contributors, MDN. (2022). HTML: Linguagem de Marcação de Hipertexto. Disponível em: https://developer.mozilla.org/pt-BR/docs/Web/HTML. Acesso em: 15 out 2022.

Pass, Last.(2022). Ferramenta de Geração De Senha. Disponível em: https://www.lastpass.com/pt/features/password-generator. Acesso em: 22 out 2022

Moura, Beatriz. (2021). O que é o HTML e suas tags?. Disponível em: https://www.alura.com.br/artigos/o-que-e-html-suas-tags-parte-1-estrutura-basica. Acesso em: 29 set 2022.

PHP. (2022). O que é o PHP?. Disponível em: https://www.php.net/manual/pt\_BR/intro-whatis.php#:~:text=O%20PHP%20(um%20acr%C3%B4nimo%20recursivo,ser%20embutida%20dentro%20do%20HTML. Acesso em: 02 out 2022.