UNIVERSIDADE FEDERAL DO MARANHÃO – UFMA

CURSO DE LICENCIATURA EM COMPUTAÇÃO

JADILSON DOS REIS SILVA

SEGURANÇA DA INFORMAÇÃO EM SISTEMAS WEB

NINA RODRIGUES – MA

2022

JADILSON DOS REIS SILVA

SEGURANÇA DA INFORMAÇÃO EM SISTEMAS WEB

Monografia apresentada ao curso de Licenciatura em Computação e Informática da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de licenciado em Computação e Informática.

NINA RODRIGUES – MA

2022

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

dos Reis Silva, Jadilson.
SEGURANÇA DA INFORMAÇÃO EM SISTEMAS WEB / Jadilson dos Reis Silva. - 2022.
48 f.

Orientador(a): Giovanni Lucca Silva.
Monografia (Graduação) - Curso de Computação e Informática, Universidade Federal do Maranhão, Nina Rodrigues-MA, 2022.

1. Hackers. 2. Informação. 3. Segurança da Informação. 4. Sistemas Web. 5. Softwares. I. Lucca Silva, Giovanni. II. Título.

JADILSON DOS REIS SILVA

SEGURANÇA DA INFORMAÇÃO EM SISTEMAS WEB

Monografia apresentada como pré-requisito de conclusão do curso de Licenciatura em Computação da Universidade Federal do Maranhão – UFMA

BANCA EXAMINADORA

_____

_____

_____

Nina Rodrigues, 27 de janeiro de 2021.

AGRADECIEMENTOS

Agradeço primeiramente a Deus, que me concedeu essa oportunidade. Também agradeço a minha família que sempre me desejou sucesso e me motiva a lutar e enfrentar todos desafios que surgem.

RESUMO

Nos sistemas Web modernos são projetados inúmeros métodos de proteção das informações contra ameaças internas e externas. As técnicas de proteção de dados contra ataques de hackers são extremamente importantes e fundamentais para a integridade digital de uma empresa. Esses métodos minimizam em grande parte as possibilidades de captura de dados sigilosos por pessoas e softwares não autorizados, são implementadas camadas extras a um determinado código fonte de uma linguagem de programação, sendo aplicado filtros extras na hora da inserção de dados como login, senha. Este trabalho visa mostrar como o uso da linguagem de programação pode adicionar camadas extras para a segurança das informações de uma pessoa ou empresa, mostrar técnicas de segurança para que usuários comuns possam navegar na web de forma segura para evitarem ter seus dados roubados por pessoas mal-intencionadas.

Palavras-chave: Segurança da Informação. Sistemas Web. Softwares. Informação. Hackers.

ABSTRACT

Web systems are tuned to protect from external and external threats. The techniques of protection against hacker attacks are extremely important and fundamental for a company's digital data. These methods are minimized in parts as possibilities of unauthorized people and data, are defined as extra password sources to a given code of a programming language, being applied to extra sources of data entry of sensitive data. work aims to show how using the programming language can add the use of extras for the security of a person's or company's information, show security techniques so that ordinary users can browse the web safely to avoid their data stolen by malicious -intentioned people.

Keywords: Information Security. Web Systems. Programs. Information. Hackers.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

As tecnologias atuais são resultadas do desenvolvimento tecnológico alcançado pelo ser humano e têm um papel fundamental no âmbito da inovação. Os avanços da tecnologia provocam grande impacto na sociedade, resulta em inovações que proporcionam melhor nível de vida ao Homem (ROSSETTI; MORALES, 2007).

Com o surgimento da internet que foi criada em 1969, nos Estados Unidos. Chamada de Arpanet, tinha como função interligar laboratórios de pesquisa, neste período tornou-se possível o compartilhamento de conteúdo através dos web sites, e também a comunicação através de e-mails e chats (ABREU, 2009). Naquele ano, um professor da Universidade da Califórnia passou para um amigo em Stanford o primeiro e-mail da história.

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais (SÊMOLA, 2014 P.41).

Os princípios básicos da segurança da informação são representados pela tríade conhecida por CIA: Confidencialidade, Integridade e Disponibilidade. Segundo sugere Stoneburner (2001), a segurança é obtida somente através da relação e correta implementação desses princípios da segurança.

1.1 PROBLEMA DE PESQUISA

Através deste trabalho é pretendido apresentar uma solução para o problema de segurança em sistemas web usando linguagem de programação Server-Side, traçando metodologias de inserção de códigos fontes mais elaborados para o gerenciamento de informações sigilosas de uma pessoa ou empresa.

A segurança da informação nesse contexto se mostra essencial, e até mesmo crítica em alguns casos, para que a consistência dos sistemas não seja afetada, garantindo a redução de riscos de fraudes, erros, vazamento, roubo e uso indevido e uso indevido de informações.

A segurança pode ser afetada por certos comportamentos de seus usuários, pelo ambiente ou estrutura que a cerca, ou por sujeitos mal intencionados com o objetivo de furtar, destruir ou alterar alguma informação. Existem níveis de segurança que podem ser estabelecidos, tais como identificados em políticas de segurança para garantir que o nível de segurança que se deseja estabelecer seja mantido. Para a construção de uma política de segurança existem alguns fatores que devem ser considerados, tais quais, riscos, benefícios, custos e esforços de implementação dos mecanismos.

1.2 JUSTIFICATIVA

A segurança da informação é um conjunto de práticas destinadas a manter os dados protegidos contra acessos não autorizados ou alterações, tanto quando estão sendo armazenados quanto quando estão sendo transmitidos de uma máquina ou local físico para outro. Às vezes, podemos vê-lo referido como *segurança de dados.* À medida que o conhecimento se tornou um dos ativos mais importantes do século 21, os esforços para manter as informações seguras tornaram-se cada vez mais importantes.

Neste contexto, mostrará como o estudo do tema pode ser aplicado na área de desenvolvimento de softwares web. O trabalho traz informações de como a Segurança da Informação é tão importante para o funcionamento e a estabilidade de um sistema web. Os códigos utilizados para gerar filtros são de fácil compreensão para que todos possam entender com clareza o real objetivo da Segurança da Informação e como os dados são tratados.

1.3 OBJETIVOS

Objetivo geral:

Mostrar o uso da segurança da informação com o auxílio da linguagem de programação para adicionar camadas de proteção e diminuir as chances de vazamento de dados de uma pessoa ou empresa.

Objetivos específicos:

- Desenvolver e implementar filtros seguros para um sistema web para acessar e gerenciar informações sigilosas referentes a dados de uma pessoa ou empresa que podem ser inseridas ou consultadas.
- Estudar a aplicabilidade da Segurança da Informação em sistemas Web.
- Implementar códigos PHP para manipular dados inseridos por um usuário.
- Aplicar melhorias no código para tornar a informação inserida mais segura e inacessível por pessoas ou softwares não autorizados.

2. REFERENCIAL TEÓRICO

2.1 INFORMAÇÃO

Segundo Sêmola (2014, p. 43), ele conceitua que a informação é " conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou maquinas".

Nos tempos em que vivemos, a informação tornou-se um bem muito valioso, pois é através dessas informações é que são tomadas decisões e novas ideias de negócios surgem. O avanço tecnológico nos proporcionou ter acesso a informações de forma muito fácil, hoje em dia podemos receber uma informação no smartphone através de aplicativos de conversa, ou no e-mail, com isso a difusão da informação tomou proporções desmesuradas e pensando nisso vem o desafio de como a protegê-la.

Os sistemas web sofrem diversos ataques por criminosos que querem obter informações sigilosas de uma empresa ou pessoa, devido a esses ataques e métodos de segurança devem ser aplicados para assim garantir que indivíduos não autorizados possam acessar determinadas áreas de um sistema. (VIANA 2013) nos apresenta uma metodologia que é direcionada à construção de sistemas Web onde todas as fases da construção e etapas definidas são contempladas com aspectos de segurança, nos detalha e deixa bem especificado todas as fases e etapas necessárias para a construção de um sistema seguro.

2.2 SEGURANÇA DA INFORMAÇÃO E SEUS MECANISMOS

O suporte para as recomendações de segurança pode ser encontrado em:

- **Controles físicos:** são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.
  Existem mecanismos de segurança que apoiam os controles físicos: Portas / trancas / paredes / blindagem / guardas / etc...
- **Controles lógicos:** são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico,

e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

2.3 MECANISMOS DE SEGURANÇA QUE APOIAM OS CONTROLES LÓGICOS

- **Mecanismos de criptografia.** Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

- **Assinatura digital.** Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.

- **Mecanismos de garantia da integridade da informação.** Usando funções de "Hashing" ou de checagem, consistindo na adição.

- **Mecanismos de controle de acesso**. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

- **Mecanismos de certificação**. Atesta a validade de um documento.
- **Integridade.** Medida em que um serviço/informação é genuíno, isto é, esta protegido contra a personificação por intrusos.

- **Honeypot:** É o nome dado a um software, cuja função é detectar ou de impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

2.4 LINGUAGEM DE PROGRAMAÇÃO NO TRATAMENTO DE INFORMAÇÕES

Uma das linguagens que pode ser exemplificada que é usada no tratamento dos dados durante um acesso a um servidor web é a linguagem PHP. O Hypertext Preprocessor (PHP) é uma linguagem de desenvolvimento de código aberto amplamente utilizada e conhecida. Segundo (CONVERSE; PARK, 2003), o PHP é uma linguagem para criação de scripts que são interpretadas do lado servidor (server-side), que pode ser incorporada em HTML (que é uma linguagem de marcação de texto) ou utilizada como um binário independente. Um exemplo bastante utilizado, é a facilidade que o PHP tem para interagir com um banco de dados SQL onde comandos SQL são executados em conjunto com o PHP.

O PHP é utilizado para programar e executar métodos e funções para filtrar e proteger informações durante o acesso de um usuário a um determinado servidor, o qual manipula as requisições recebidas do usuário e realiza as devidas atualizações no banco de dados.

2.5 COMPUTAÇÃO EM NUVEM

Segundo (TAURION, 2009), a computação em nuvem pode ser usada para descrever um ambiente computacional baseado em uma imensa rede de máquinas servidoras, podendo elas serem virtuais ou físicas. O autor ainda sugere algumas características deste paradigma que podem ser reunidas:

- A computação em nuvem cria uma ilusão da disponibilidade de recursos infinitos acessáveis sob demanda;
- A computação em nuvem elimina a necessidade de adquirir e provisionar recursos antecipadamente;
- A computação em nuvem oferece elasticidade, permitindo-se que as empresas usem os recursos na quantidade que forem necessários;
- O pagamento de serviços em nuvem é pela quantidade de recursos utilizados.

Já segundo (NIST, 2018), a computação em nuvem é um modelo para acessar convenientemente e sob demanda um conjunto de recursos computacionais

compartilhados configuráveis (como por exemplo redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente adquiridos e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços.

2.6 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um conjunto de práticas destinadas a manter os dados protegidos contra acessos não autorizados ou alterações, tanto quando estão sendo armazenados quanto quando estão sendo transmitidos de uma máquina ou local físico para outro (Sêmola, 2014 p.41). Às vezes, podemos vê-lo referido como segurança de dados. À medida que o conhecimento se tornou um dos ativos mais importantes do século 21, os esforços para manter as informações seguras tornaram-se cada vez mais importantes.

A Segurança da Informação se refere à proteção existente sobre os dados de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais (Sêmola, 2014 p.41). Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

Nos sistemas Web modernos são projetados inúmeros métodos de proteção das informações diante de ameaças internas e externas são extremamente importantes e fundamentais para a integridade digital de uma empresa. Esses métodos minimizam em grande parte as possibilidades de captura de dados sigilosos por pessoas e softwares não autorizados, são implementadas camadas extras a um determinado código fonte de uma

linguagem server-side, sendo aplicado filtros extras na hora de inserção de dados como login, senha. Com essas camadas de proteção pode ser evitado danos para o andamento das operações e até prejuízos financeiros. Estes esforços estão contemplados na Segurança da Informação (SI).

2.7 SEGURANÇA DA INFORMAÇÃO VERSUS SEGURANÇA CIBERNÉTICA

Os componentes básicos da segurança da informação são mais frequentemente resumidos pela chamada tríade da CIA: *confidencialidade, integridade* e *disponibilidade.*

- **A confidencialidade** é talvez o elemento da tríade que mais imediatamente vem à mente quando se pensa em segurança da informação. Os dados são confidenciais quando apenas as pessoas autorizadas a acessá-los podem fazê-lo; para garantir a confidencialidade, precisamos ser capazes de identificar quem está tentando acessar os dados e bloquear tentativas de pessoas sem autorização. Senhas, criptografia, autenticação e defesa contra ataques de penetração são técnicas projetadas para garantir a confidencialidade.

- **Integridade** significa manter os dados em seu estado correto e evitar que sejam modificados indevidamente, seja por acidente ou maliciosamente. Muitas das técnicas que garantem a confidencialidade também protegerão a integridade dos dados – afinal, um hacker não pode alterar dados que não podem acessar – mas existem outras ferramentas que ajudam a fornecer uma defesa da integridade em profundidade: as somas de verificação podem ajudá-lo a verificar os dados integridade, por exemplo, e software de controle de versão e backups frequentes podem ajudá-lo a restaurar os dados para um estado correto, se necessário. A integridade também abrange o conceito de não repúdio : devemos ser capaz de *provar* que manteve a integridade de seus dados, especialmente em contextos legais.

- **A disponibilidade** é a imagem espelhada da confidencialidade: enquanto precisamos garantir que os dados não possam ser acessados por usuários não autorizados, nós também precisamos garantir que eles *possam* ser acessados por aqueles que têm as devidas permissões. Garantir a disponibilidade dos dados significa combinar os recursos de rede e de computação com o volume de acesso de dados que se espera e implementar uma boa política de backup para fins de recuperação de desastres.

Em um mundo ideal, seus dados devem ser sempre mantidos em sigilo, em seu estado correto e disponíveis; na prática, é claro, muitas vezes precisamos fazer escolhas sobre quais princípios de segurança da informação enfatizar, e isso requer a avaliação de seus dados. Se estivermos armazenando informações médicas confidenciais, por exemplo, nos concentraremos na confidencialidade, enquanto uma instituição financeira pode enfatizar a integridade dos dados para garantir que a conta bancária de ninguém seja creditada ou debitada incorretamente.

2.8 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Os meios pelos quais esses princípios são aplicados a uma organização assumem a forma de uma *política de segurança.* Este não é um hardware ou software de segurança; em vez disso, é um documento que uma empresa elabora, com base em suas próprias necessidades e peculiaridades específicas, para estabelecer quais dados precisam ser protegidos e de que maneira. Essas políticas orientam as decisões da organização sobre a aquisição de ferramentas de segurança cibernética e também determinam o comportamento e as responsabilidades dos funcionários.

Entre outras coisas, a política de segurança da informação da sua empresa deve incluir:

- Uma declaração descrevendo o propósito do programa segurança da informação e seus objetivos gerais

- Definições de termos-chave usados no documento para garantir o entendimento compartilhado
- Uma política de controle de acesso, determinando quem tem acesso a quais dados e como eles podem estabelecer seus direitos
- Uma política de senha
- Um plano de operações e suporte de dados para garantir que os dados estejam sempre disponíveis para quem precisa deles
- Funções e responsabilidades dos funcionários quando se trata de proteger os dados, incluindo quem é o responsável final pela segurança da informação

Uma coisa importante a ter em mente é que, em um mundo onde muitas empresas terceirizam alguns serviços de informática ou armazenam dados na nuvem, sua política de segurança precisa abranger mais do que apenas os ativos que possuímos. Precisamos saber como lidará com tudo, desde informações de identificação pessoal armazenadas em instâncias da AWS até contratados terceirizados que precisam se autenticar para acessar informações corporativas confidenciais.

2.9 MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

Como já deve estar claro, quase todas as medidas técnicas associadas à segurança cibernética tocam em segurança da informação até certo ponto, mas vale a pena pensar nas medidas de segurança da informação de uma maneira geral:

- **As medidas técnicas** incluem o hardware e o software que protegem os dados — desde criptografia até firewalls
- **As medidas organizativas** incluem a criação de uma unidade interna dedicada à segurança da informação, bem como a inclusão da segurança da informação nas funções de alguns colaboradores de cada departamento

- **As medidas humanas** incluem fornecer treinamento de conscientização para usuários sobre práticas adequadas de segurança da informação.
- **As medidas físicas** incluem o controle de acesso aos escritórios e, principalmente, aos data centers.

2.10 VIOLAÇÃO DE DADOS

No decorrer dos anos diversas soluções têm sido implementadas para a proteção de dados, como a aplicação de algoritmos genéticos para a criação de perfis de segurança voltados a situações genéricas (GUPTA et al., 2004), mas um longo caminho ainda está por ser percorrido.

Os ataques ou a tentativa de violar dados é uma ameaça, uma das definições apresentadas para ameaça é “evento ou atitude indesejável (roubo, apagar, vírus, etc.) que potencialmente remove, desabilita, danifica ou destrói um recurso” (DIAS, 2000, p. 55).

O Internet Engineering Task Force - IETF, organização independente que é dedicada à realizar análises e prevenir eventos de segurança e realiza gestão da redes, conceitua incidente como sendo “um evento que envolve uma violação de segurança” (SHIREY, 2000).

Durante os primeiros seis meses de 2019, mais de 4 bilhões de registros foram expostos por violações de dados. Essa é uma estatística chocante que se torna ainda mais quando percebemos que as senhas foram incluídas em massa. Em 4 de dezembro, um pesquisador de segurança descobriu um tesouro de mais de um bilhão de senhas de texto simples em um banco de dados online não seguro (ALMEIDA).

No processo de classificação, pesquisadores do NordPass que é um gerenciador de senhas proprietário lançado em 2019 com objetivo de ajudar seus usuários a organizar suas senhas e notas seguras, mantendo-as em um único lugar, usaram um gerenciador de senhas das pessoas que estão por trás do aplicativo NordVPN , começaram a classificar as senhas mais usadas e menos seguras. Armados com um banco de dados de cerca de 500 milhões de

senhas vazadas como resultado de violações de dados em 2019, os pesquisadores do NordPass conseguiram classificá-las em ordem de uso.

2.11 A HIGIENE DA SENHA É UMA PRIORIDADE DE SEGURANÇA MÁXIMA

As três principais senhas mais usadas, com 6.348.704 aparições entre elas, são incrivelmente inseguras, fracas e totalmente previsíveis. No entanto, também existem muitas senhas inesperadas na lista e isso é o mais preocupante. Bem, preocupando-se se acontecer de alguém estar usando algum deles, isso é, se uma senha que utilizamos estiver na lista, a postura de segurança acabou de ser enfraquecida (WINDER, FORBES, 2019).

Os hackers podem entrar com força bruta nas contas lançando senhas comuns conhecidas, bem como palavras do dicionário, para elas. Se usamos a mesma senha em vários sites e serviços, nossa postura de segurança é tão ruim que precisaremos urgentemente consultar um quiroprático cibernético. Em 6 de dezembro, a Microsoft analisou um banco de dados de 3 bilhões de credenciais vazadas de violações de segurança e descobriu que mais de 44 milhões de contas da Microsoft estavam usando senhas que já haviam sido comprometidas em outros lugares. A reutilização de senha é uma maneira infalível de colocar nossos dados em apuros, especialmente se estivermos usando uma das piores senhas do mundo.

2.12 CLASSIFICAÇÃO DAS 20 PIORES SENHAS DO MUNDO

Nº	SENHA
1	12345
2	123456
3	123456789
4	teste1
5	senha
6	12345678
7	zinco

8	**g_czechout**
9	**asdf**
10	**qwerty**
11	**1234567890**
12	**1234567**
13	**aa123456**
14	**eu amo você**
15	**1234**
16	**abc123**
17	**111111**
18	**123123**
19	**dubsmash**
20	**teste**

Tabela 1 – Classificação das 20 piores senhas

2.13 NAVEGADOR DA WEB

Um navegador da web é um programa de software que permite ao usuário localizar, acessar e exibir páginas da web. No uso comum, um navegador da Web geralmente é abreviado para "navegador".

Os navegadores da Web são usados principalmente para exibir e acessar sites na Internet, bem como outros conteúdos criados usando linguagens como Hypertext Markup Language (HTML) e Extensible Markup Language (XML).

Os navegadores traduzem páginas da Web e sites entregues usando Hypertext Transfer Protocol (HTTP) em conteúdo legível por humanos. Eles também têm a capacidade de exibir outros protocolos e prefixos, como HTTP seguro (HTTPS), Protocolo de transferência de arquivos (FTP), manipulação de e-mail (mailto:) e arquivos (arquivo:).

Além disso, a maioria dos navegadores também oferece suporte a plug-ins externos necessários para exibir conteúdo ativo, como vídeo na página, áudio e conteúdo de jogos.

2.14 SURGIMENTO E AVANÇO DOS NAVEGADORES WEB

Os primeiros navegadores da Web começaram antes do início do século 21, com um navegador somente texto chamado Lynx e outro navegador chamado Mosaic.

Mais tarde, o Netscape Navigator e o Microsoft Internet Explorer surgiram como as duas principais opções, até o lançamento do Mozilla Firefox em 2004.

Enquanto isso, os produtos Safari da Apple foram lançados em 2003 e se tornaram o sistema operacional padrão para os iPhones da empresa em 2007.

Desde então, o Google Chrome também se tornou um concorrente na guerra dos navegadores – a competição para impulsionar a maior parte da atividade do usuário final.

2.15 O QUE FAZ UM NAVEGADOR DA WEB

Essencialmente, um navegador da Web lida com a atividade HTTP entre um cliente e um servidor que é a espinha dorsal do uso da World Wide Web. URLs são direções de tráfego para o navegador da web, e o navegador usa endereços IP e outras ferramentas para estabelecer essas conexões.

Além de facilitar a navegação na web, novos tipos de navegadores da web têm funcionalidade adicional por meio de uma variedade de plug-ins que podem adicionar recursos após o fato. Alguns deles têm a ver com segurança e acessibilidade, enquanto outros têm a ver com conveniências do usuário final ou agregação de dados.

2.16 DESENVOLVIMENTO CONTÍNUO DO NAVEGADOR DA WEB

Alguns dos maiores desenvolvimentos em navegadores da web têm a ver com segurança cibernética. Por exemplo, o Google Chrome foi pioneiro em

proteger seus sistemas contra sites que não possuem um certificado SSL válido, o que evita vários tipos de hackers e vulnerabilidades.

Os navegadores da Web também podem ser feitos para lidar com protocolos mais recentes, como alguns dos criados pela Internet Engineering Task Force para aumentar a segurança da Web.

Outras novas tecnologias incluem a ideia de isolamento do navegador, onde as empresas direcionam a atividade de forma segmentada, separando a atividade da rede interna da atividade do navegador da web.

Quando a atividade do navegador pode ser colocada fora de um firewall e monitorada durante a entrada, a rede interna pode desfrutar de maiores proteções.

Enquanto isso, as linguagens de codificação da Web subjacentes que são usadas também evoluíram. HTML tornou-se HTML 5, e folhas de estilo em cascata ou CSS revolucionaram a forma como o design consistente do site é mantido.

O navegador da web é uma tecnologia favorita muito usada na barra de tarefas do usuário médio, mas ainda está sendo evoluída e desenvolvida para atender às nossas necessidades modernas de Internet.

É interessante notar que, à medida que surge o fenômeno da Internet das Coisas (IoT), onde aparelhos mais diversos acessam a Internet, apenas dispositivos tradicionais, como telefones celulares e laptops, realmente usam um design de navegador da web.

Outros dispositivos só podem enviar e receber dados sem eventos direcionados ao usuário final, embora coisas como geladeiras inteligentes e outros dispositivos domésticos inteligentes possam ter navegadores da Web instalados.

Eles podem ser fundamentalmente diferentes dos designs de navegadores da Web com os quais estamos familiarizados até o momento.

Por exemplo, as primeiras implementações de navegadores da Web para dispositivos inteligentes mostram como eles promovem tipos específicos de interfaces visuais embutidos na frente do aparelho e com que facilidade alguns desses navegadores da Web podem ser invadidos por malware que infecta o dispositivo.

2.17 O USO DA LINGUAGEM PHP NOS SISTEMAS WEB

Segundo (CONVERSE; PARK, 2003), o PHP é a linguagem de script do lado do servidor mais popular. Ele é projetado para desenvolvimento web e programação de uso geral em 1994 por Rasmus Lerdorf. Com mais de duas décadas de desenvolvimento, o PHP viu os altos e baixos. Agora, o PHP é gerenciado pelo The PHP Group e está em desenvolvimento contínuo. PHP significa Hypertext Preprocessor que foi alterado de um nome inicial de “Personal Home Page”.

O PHP é usado principalmente em conjunto com código HTML, sistema de gerenciamento de conteúdo da web, sistemas de modelo da web e outros frameworks populares da web. A linguagem PHP é processada pelo servidor ou pela Common Gateway Interface (CGI). De qualquer forma, ele pode ser usado para criar uma aplicação web incrível onde o código PHP é sempre executado no lado do servidor. Você também pode executar o código PHP com a ajuda da interface de linha de comando (CLI). Além disso, ele também pode ser usado para implementar um aplicativo gráfico autônomo por natureza.

2.18 HISTÓRIA DO PHP

A história do PHP é única à sua maneira. Tudo começou quando Rasmus Lerdorf começou a experimentar e trabalhar no Command Gateway Interface (CGI) com foco na criação de sua página pessoal. Ele queria estender a funcionalidade do CGI aos formulários e garantir que os formulários pudessem se comunicar com o banco de dados para transferir e armazenar informações. Ele teve sucesso em suas tentativas e nomeou a solução como PHP/FI ou "Personal Home Page/Forms Interpreter". O nome foi alterado posteriormente para *" Hypertext Preprocessor ".*

Seu trabalho foi feito principalmente com Zeev Suraski e Andi Gutman. Ambos trabalharam no analisador que foi usado no PHP 3.

Ele foi inicialmente usado para criar aplicativos web simples, mas dinâmicos. Para garantir o crescimento adequado e o desenvolvimento do núcleo do PHP, Lerdorf lançou o PHP no grupo de discussão Usenet em 8 de junho de 1995, sob a versão PHP 1.0. A versão inicial era forte e a versão PHP de 2013 carregava os recursos básicos da primeira versão. Mais tarde, novos recursos são adicionados, incluindo variáveis Per-like, incorporação de HTML, manipulação de formulários. Na parte da sintaxe, ele tem semelhanças com o Perl, mas é mais simples comparado a ele.

PHP/FI pode ser usado para construir aplicações web simples e dinâmicas. Para acelerar o relatório de bugs e melhorar o código, Lerdorf anunciou inicialmente o lançamento do PHP/FI como "Personal Home Page Tools (PHP Tools) versão 1.0" no grupo de discussão Usenet em 8 de junho de 1995 Esta versão já tinha a funcionalidade básica que o PHP tem a partir de 2013. Isso inclui variáveis do tipo Perl, manipulação de formulários e a capacidade de incorporar HTML. A sintaxe se assemelhava à do Perl, mas era mais simples, mais limitada e menos consistente.

Como todos sabemos, o PHP nunca foi pensado para ser uma linguagem de programação, mas já chamou a atenção do público, e o tráfego orgânico foi crescendo lentamente. Para garantir que o PHP cresça na direção certa, uma nova equipe de desenvolvimento é formada em meados de 1997. Em novembro de 1997, uma versão funcional da linguagem de programação PHP foi lançada e ficou conhecida como PHP/FI 2.

Como todos sabemos, o PHP nunca foi pensado para ser uma linguagem de programação, mas já chamou a atenção do público, e o tráfego orgânico foi crescendo lentamente. Para garantir que o PHP cresça na direção certa, uma nova equipe de desenvolvimento é formada em meados de 1997. Em novembro de 1997, uma versão funcional da linguagem de programação PHP foi lançada e ficou conhecida como PHP/FI 2.

2.19 PHP7

O PHP 7 agora é lançado trazendo novas mudanças para a plataforma. As novas mudanças garantem que as falhas antigas sejam corrigidas e os novos recursos podem ajudá-lo a tirar o máximo proveito da linguagem de programação. A convenção de nomenclatura também tem sido um problema entre a comunidade.

O PHP 7 traz muitos novos recursos, incluindo melhoria de desempenho.

2.20 A LINGUAGEM DE MARCAÇÃO HTML

HTML é uma linguagem de marcação muito utilizada para criar páginas da web e aplicativos da web. HTML, quando combinado com JavaScript e CSS, tornou-se um marco para o desenvolvimento web . Um dos aspectos úteis do HTML é que ele pode incorporar programas escritos em uma linguagem de scriptcomo JavaScript, que é responsável por afetar o comportamento e o conteúdo das páginas da web. A inclusão de CSS afetaria o layout e a aparência do conteúdo. Os blocos de construção básicos de qualquer página HTML são elementos HTML. Um documento estruturado pode ser criado com a ajuda de texto semântico-estrutural como título, parágrafo, lista, link e outros itens. Na verdade, o navegador não exibe as tags HTML, mas as utiliza para interpretar o conteúdo da página. É preciso estudar várias tags e então entender seu comportamento.

HTML é usado para um documento da web, navegação na internet, etc. Neste artigo sobre Usos do HTML, vamos nos concentrar nos principais usos do HTML.

2.21 OS PRINCIPAIS USOS DO HTML

Desenvolvimento de páginas web

HTML é muito usado para criar páginas que são exibidas na rede mundial de computadores. Cada página contém um conjunto de tags HTML, incluindo hiperlinks que são usados para se conectar a outras páginas. Cada

página que vemos na world wide web é escrita usando uma versão do código HTML .

Criação de documentos da Web

A criação de documentos na internet é dominada pelo HTML e seu conceito básico via tag e DOM, ou seja, modelo de objeto do documento. Tags HTML são inseridas antes e depois ou frases para localizar seu formato e localização na página. Um documento da web consiste em três seções: título, cabeçalho e corpo. Head inclui as informações para identificar o documento, incluindo título e qualquer outra palavra-chave importante. Um título pode ser visto na barra do navegador, e a seção do corpo é a parte principal do site visível para o visualizador. Todos os três segmentos são projetados e criados pelo uso de tags HTML. Cada seção tem seu próprio conjunto específico de tags, que são renderizadas de forma dedicada, mantendo os conceitos de cabeça, título e corpo em um loop.

Navegação na Internet

Este é um dos usos mais importantes do HTML, que é revolucionário. Esta navegação é possível utilizando o conceito de Hipertexto. É basicamente um texto que se refere a outras páginas da web ou texto , e quando o usuário clica nele, navega para o texto ou página referenciada. HTML é muito usado para incorporar o hiperlink nas páginas da web. Um usuário pode navegar facilmente pelas páginas da web e também entre sites, localizados em servidores diferentes.

3. MATERIAIS E MÉTODOS

Para atingir os objetivos propostos e comprovar os resultados da usabilidade da segurança da informação, foi realizado uma pesquisa em duas fases. A primeira fase foi a busca pelas informações sobre as primeiras fases da evolução da tecnologia e a criação da internet que foi criada em 1969, nos Estados Unidos. Chamada de Arpanet, que tinha como função interligar laboratórios de pesquisa. Naquele ano, um professor da Universidade da

Califórnia passou para um amigo em Stanford o primeiro e-mail da história (FOLHA DE SÃO PAULO, 2001).

Foi buscado informações sobre criação do primeiro site que foi resultado do avanço da internet que impulsionou a criação desse site. The Project, como é conhecido o primeiro site da história, foi criado por Tim Berners-Lee, conhecido como o Pai da World Wide Web (WWW). Este grande acontecimento foi realizado no dia 6 de agosto de 1991 e, nele, seu criador descreve brevemente detalhes da World Wide Web. O objetivo deste espaço principal era permitir que os profissionais do Centro de Europeu de Pesquisa Nuclear (CERN) no qual Berners-Lee atuava como físico tivessem acesso rápido aos códigos e procedimentos para criar sites semelhantes (ALMEIDA, 2021).

Após os avanços e melhorias nos sistemas web o surgimento de linguagens de programação mais avançadas e com o objetivo de adicionar uma camada extra de segurança, podemos citar o PHP. Hypertext Preprocessor (PHP) é uma linguagem de desenvolvimento de código aberto amplamente utilizada e conhecida. o PHP é uma linguagem para criação de scripts que trabalha em conjunto com o HTML, esses comandos são interpretados do lado servidor (server-side), manipula as requisições recebidas do usuário e realiza as devidas atualizações no banco de dados.

Foi pesquisado códigos fontes e exemplos no site oficial do PHP que fica localizado em https://www.php.net/. Com esses códigos foi possível obter informações valiosas de como filtrar dados inseridos em campos de texto como login e senha, adicionando camadas extras de proteção para dificultar o vazamento de dados sigilosos para uma empresa ou pessoa.

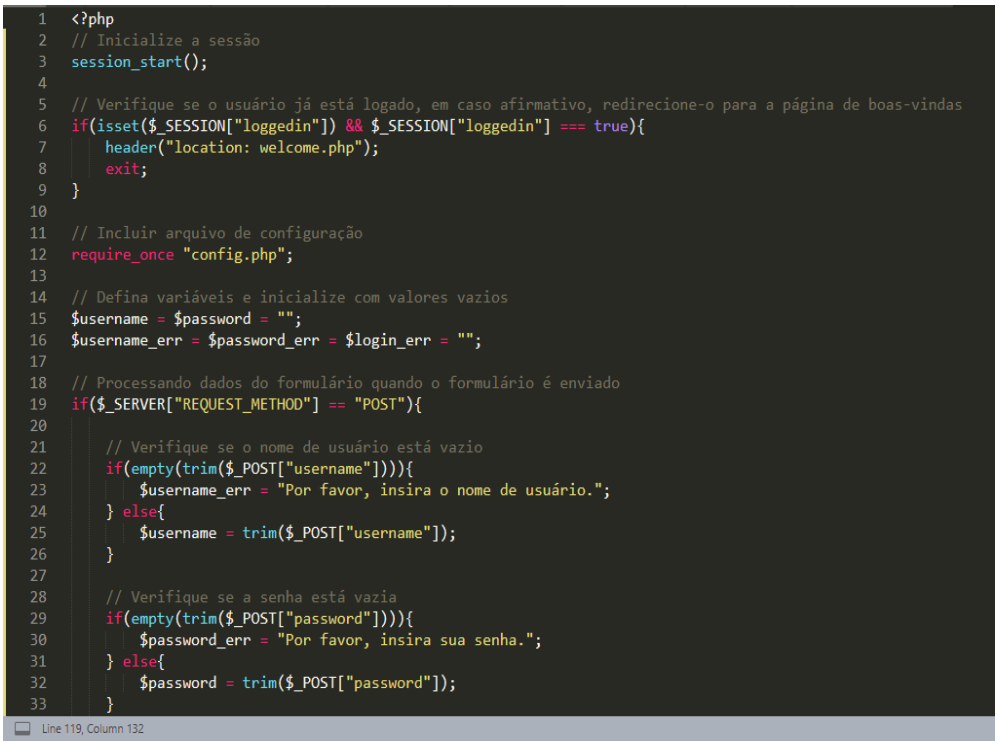
Na segunda fase foi realizado a aplicação dos dados e códigos fontes obtidos através da pesquisa. Testes práticos foram feitos para se obter um resultado real.

Foi realizado os testes práticos dos códigos utilizando um editor de texto chamado Sublime Text. Sublime Text é um editor de código para diversas linguagens de programação como Javascript, HTML, PHP dentre outras. O programa tem interface com diferentes cores para facilitar a compreensão e

construção dos códigos, ao contrário de editores de linguagem de programação que costumam ser complicados, principalmente para usuários iniciantes.

Logo abaixo na figura 1 podemos ver a utilização da linguagem PHP para exemplificar um código de tratamento de informações inseridas por um usuário em um sistema que precisa das credenciais do mesmo para acessa-lo.

Figura 1 - Script para logar um usuário de forma segura utilizando a linguagem PHP, mysql e um banco de dados hospedado localmente.



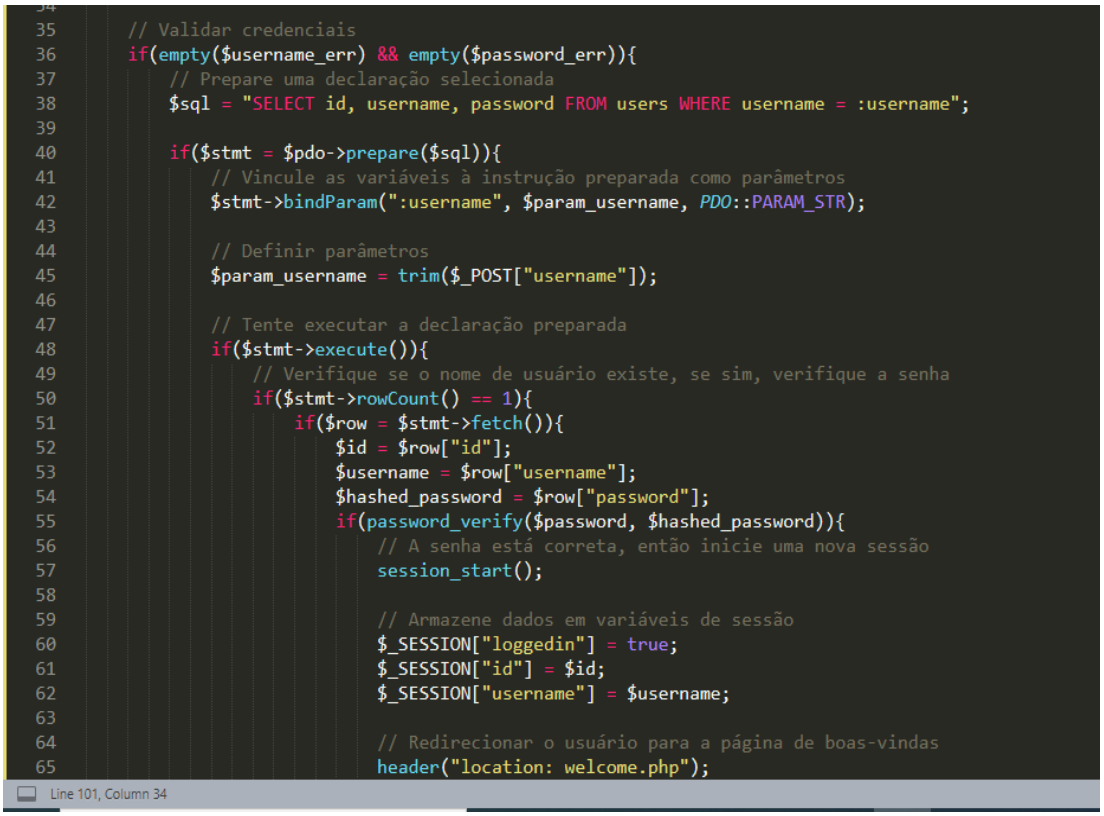
```php
<?php
// Inicialize a sessão
session_start();

// Verifique se o usuário já está logado, em caso afirmativo, redirecione-o para a página de boas-vindas
if(isset($_SESSION["loggedin"]) && $_SESSION["loggedin"] === true){
    header("location: welcome.php");
    exit;
}

// Incluir arquivo de configuração
require_once "config.php";

// Defina variáveis e inicialize com valores vazios
$username = $password = "";
$username_err = $password_err = $login_err = "";

// Processando dados do formulário quando o formulário é enviado
if($_SERVER["REQUEST_METHOD"] == "POST"){

    // Verifique se o nome de usuário está vazio
    if(empty(trim($_POST["username"]))){
        $username_err = "Por favor, insira o nome de usuário.";
    } else{
        $username = trim($_POST["username"]);
    }

    // Verifique se a senha está vazia
    if(empty(trim($_POST["password"]))){
        $password_err = "Por favor, insira sua senha.";
    } else{
        $password = trim($_POST["password"]);
    }
```

Line 119, Column 132

Fonte: Elaborado pelo autor

Neste exemplo na figura 2, podemos ver um exemplo de script onde é feita uma consulta utilizando o comando (prepare) que nada mais é do que consultas “pré-prontas” a diferença é que em lugar das variáveis é colocado um placeholder (marcador de lugar) e na hora da consulta informa a ordem das variáveis a serem substituídas usando o comando (bindParam), evitando assim injeções sql injetadas por usuários mal intencionados.

Figura 2 - Script para realizar uma consulta no banco de dados dentro da tabela de usuários.



```
    // Validar credenciais
    if(empty($username_err) && empty($password_err)){
        // Prepare uma declaração selecionada
        $sql = "SELECT id, username, password FROM users WHERE username = :username";

        if($stmt = $pdo->prepare($sql)){
            // Vincule as variáveis à instrução preparada como parâmetros
            $stmt->bindParam(":username", $param_username, PDO::PARAM_STR);

            // Definir parâmetros
            $param_username = trim($_POST["username"]);

            // Tente executar a declaração preparada
            if($stmt->execute()){
                // Verifique se o nome de usuário existe, se sim, verifique a senha
                if($stmt->rowCount() == 1){
                    if($row = $stmt->fetch()){
                        $id = $row["id"];
                        $username = $row["username"];
                        $hashed_password = $row["password"];
                        if(password_verify($password, $hashed_password)){
                            // A senha está correta, então inicie uma nova sessão
                            session_start();

                            // Armazene dados em variáveis de sessão
                            $_SESSION["loggedin"] = true;
                            $_SESSION["id"] = $id;
                            $_SESSION["username"] = $username;

                            // Redirecionar o usuário para a página de boas-vindas
                            header("location: welcome.php");
```

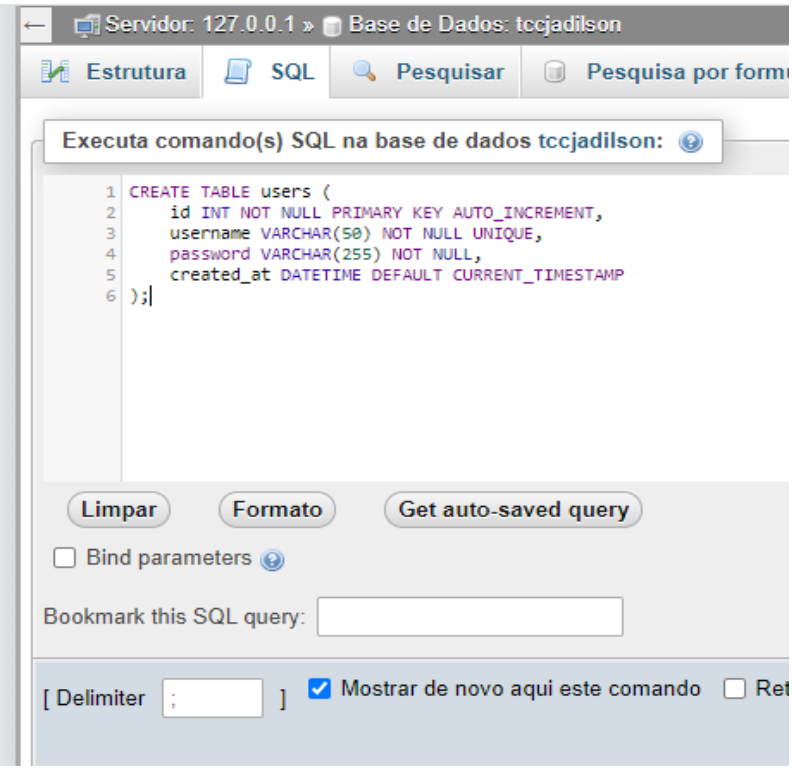
Line 101, Column 34

Fonte: Elaborado pelo autor

Após a conclusão dos scripts de tratamento de dados inseridos e scripts de consultas no banco de dados, chega o momento de criar as tabelas do banco de dados utilizando o administrador de banco de dados PHPMyadmin.

Na figura 3 podemos visualizar um comando SQL inserido para a criação dos campos das tabelas que irá armazenar os dados dos usuários como login e senha dentro do banco de dados.

Figura 3 - Script para a criação de uma tabela no banco de dados para armazenar informações do usuário.



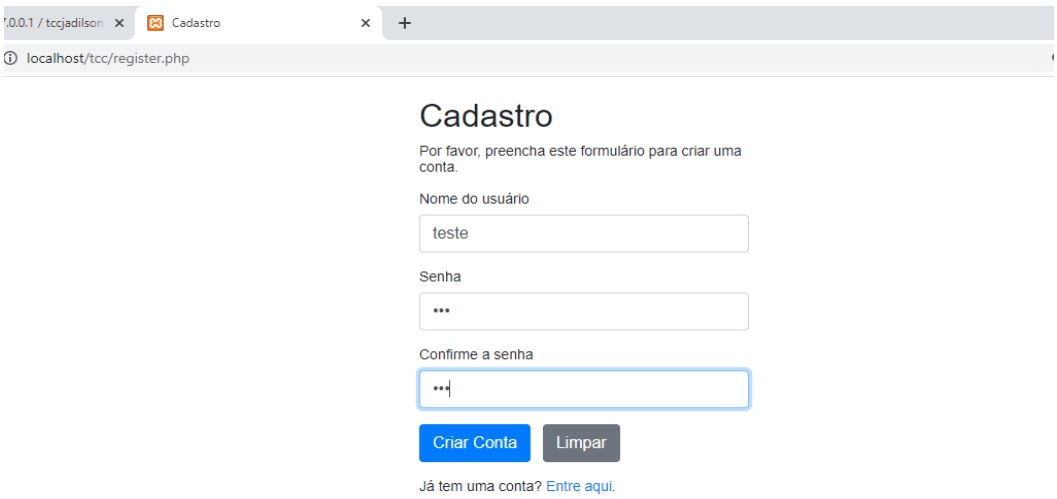
Fonte: Elaborado pelo autor

No processo de criação das telas do sistema, foi utilizado componentes HTML, CSS e JavaScript pré-formatados com o auxílio do framework Bootstrap, onde pode ser acessado no site https://getbootstrap.com/docs/4.0/components/.

O Bootstrap é o framework utilizado para criar layouts e telas de sistemas web. Este framework facilita muito o trabalho de front-end que é a parte visível do site como, textos, botões, tabelas e muitos outros.

Na figura 4 podemos ver um exemplo de uma tela de cadastro usando componentes do Bootstrap para dar uma visibilidade mais agradável ao sistema e facilitar na navegação do usuário pelo mesmo.

Figura 4 – Tela de cadastro utilizando a linguagem PHP e o framework Bootstrap.

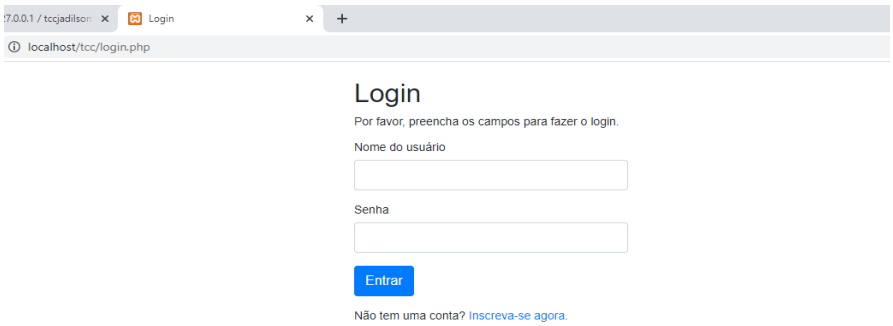


Fonte: Elaborado pelo autor

Após a tela de cadastro vem a hora do usuário acessar a página de login onde deverá inserir seu login e senha cadastrados anteriormente.

Na figura 5 logo abaixo podemos ver a tela de login onde o script PHP irá trabalhar tratando os dados inseridos pelo usuário, se todas as credenciais exigidas forem satisfatórias ao sistema, o mesmo irá redireciona-lo de forma segura para a página de boas-vindas.

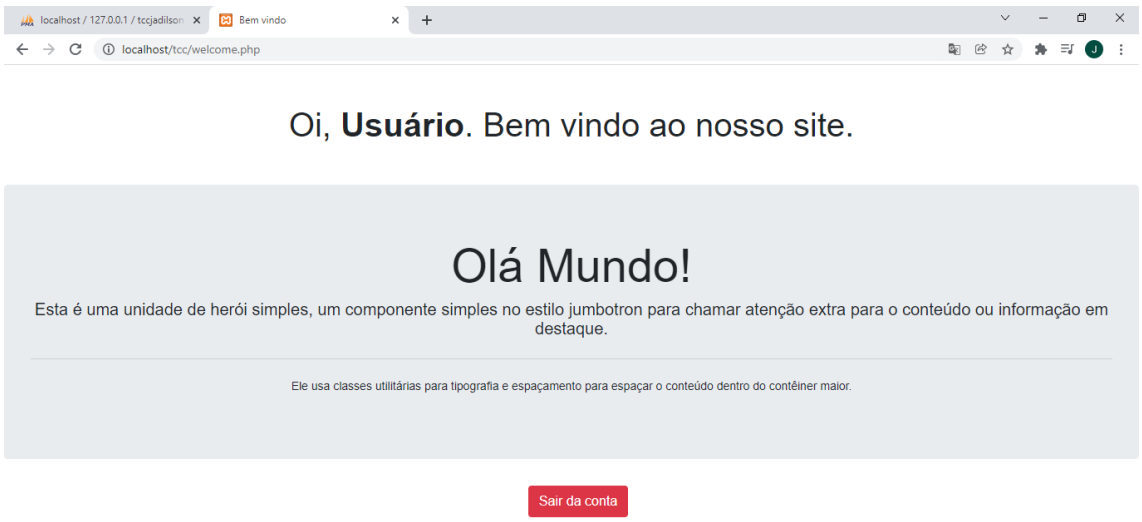
Figura 5 – Tela de login utilizando a linguagem PHP e o framework Bootstrap.



Fonte: Elaborado pelo autor

Após o login bem-sucedido e o usuário redirecionado com sucesso, podemos observar na figura 6 a tela de boas-vindas na qual o usuário poderá navegar pelo sistema.

Figura 6 – Tela de boas-vindas utilizando a linguagem PHP e o framework Bootstrap.



Fonte: Elaborado pelo autor

4. RESULTADOS

Este trabalho traz informações de como a Segurança da Informação é tão importante para o funcionamento e a estabilidade de um sistema web.

Após os uma pesquisa aprofundada para a construção de um script para tratamento de dados de um usuário no processo de cadastro, login e navegação por um sistema web, foi descoberto a importância de proteger esses dados utilizado a linguagem de programação PHP para proteger esses dados de outros usuários não autorizados.

- **injeção SQL**

Durante a pesquisa e execução dos códigos pode-se observar que os sistemas que trabalham com banco de dados e utiliza a linguagem SQL no processo de leitura e escrita de dados no banco de dados podem sofrer ataques para que as informações de usuários sejam obtidas de forma ilícita. Um dos ataques mais comuns é a injeção SQL. A injeção de SQL (ou SQL injection) é uma vulnerabilidade de segurança da web que permite que um invasor interfira nas consultas que um sistema faz ao seu banco de dados. Geralmente, permite que um invasor visualize dados que normalmente ele não é capaz de recuperar. Isso pode incluir dados pertencentes a outros usuários ou quaisquer outros dados que o próprio sistema é capaz de acessar. Em muitos casos, um invasor pode modificar ou excluir esses dados, causando alterações persistentes no conteúdo ou comportamento do sistema.

Em algumas situações, um invasor pode escalar um ataque de injeção de SQL para comprometer o servidor subjacente ou outra infraestrutura de back-end, ou realizar um ataque de negação de serviço.

- **Exemplos de injeção SQL:**

Há uma grande variedade de vulnerabilidades, ataques e técnicas de Injeção SQL que surgem em diferentes situações. Alguns exemplos comuns de injeção de SQL incluem:

  - **Recuperando dados ocultos,** onde você pode modificar uma consulta SQL para retornar resultados adicionais.

- **Subvertendo a lógica do aplicativo,** onde você pode alterar uma consulta para interferir com a lógica do aplicativo.
- **Ataques UNION**, onde você pode recuperar dados de diferentes tabelas de banco de dados.
- **Examinando o banco de dados**, onde você pode extrair informações sobre a versão e estrutura do banco de dados.
- **Injeção cega de SQL**, onde os resultados de uma consulta que você controla não são retornados nas respostas do aplicativo.

- **Recuperando dados ocultos:**

Considere um site de compras que exibe produtos em diferentes categorias. Quando o usuário clica na categoria Presentes, o navegador solicita o URL: *http://insecure-website.com/products?category=Gifts*

Isso faz com que o aplicativo faça uma consulta SQL para recuperar detalhes dos produtos relevantes do banco de dados:

*SELECT * FROM products WHERE category = 'Gifts'--' AND lancados = 1*

Esta consulta SQL pede ao banco de dados para retornar:

- todos os detalhes (*)
- da tabela de produtos
- onde a categoria é Gifts e lancados é 1.

A restrição lançada = 1 está sendo usada para ocultar produtos que não foram lançados.

Para produtos não lançados, presumivelmente **lançado = 0**.

O aplicativo não implementa nenhuma defesa contra ataques de injeção de SQL, então um invasor pode construir um ataque como: http://insecure-website.com/products?category=Gifts'--

Isso resulta na consulta SQL:

*SELECT * FROM products WHERE category = 'Gifts'--' AND lancado = 1*

O principal aqui é que a sequência de dois traços -- é um indicador de comentário em SQL e significa que o resto da consulta é interpretado como um comentário. Isso remove efetivamente o restante da consulta, de forma que não inclui mais **AND lancado = 1** . Isso significa que todos os produtos são exibidos, incluindo os não lançados.

Indo além, um invasor pode fazer com que o aplicativo exiba todos os produtos em qualquer categoria, incluindo categorias que ele não conhece: http://insecure-website.com/products?category=Gifts'+OR+1=1– Isso resulta na consulta SQL:

*SELECT * FROM products WHERE category = 'Gifts' OR 1=1--' AND lancado = 1*

A consulta modificada retornará todos os itens em que a categoria seja Gifts ou 1 é igual a 1. Como 1 = 1 é sempre verdadeiro, a consulta retornará todos os itens.

- **Como evitar injeção de SQL:**

A maioria das instâncias de injeção de SQL pode ser evitada usando consultas parametrizadas (também conhecidas como instruções preparadas) em vez da concatenação de strings na consulta.

O código a seguir é vulnerável à injeção de SQL porque a entrada do usuário é concatenada diretamente na consulta: Consulta string = *"SELECIONE * DE produtos ONDE categoria = '" + input + "'"*;

Com o aprimoramento dos códigos PHP pensados para atuar na segurança da informação, foi possível corrigir as falhas de segurança e a vulnerabilidade a injeção SQL. No exemplo a seguir é utilizado os recursos do PDO (PHP Data Objects) para alocação de variáveis com a função bindValue, vejamos o exemplo a seguir:

```
$stmt = $this->pdo->prepare("SELECT * FROM users WHERE login = :parametro1 AND senha = :parametro2");
$stmt->bindValue(':parametro1' , 'loginuser');
$stmt->bindValue(':parametro2' , 'password');
$stmt->execute();
```

As consultas parametrizadas podem ser usadas para qualquer situação em que a entrada não confiável apareça como dados dentro da consulta, incluindo a cláusula ONDE e valores em uma declaração INSERIR ou ATUALIZAR. Elas não podem ser usadas para lidar com entradas não confiáveis em outras partes da consulta, como nomes de tabela ou coluna, ou a cláusula ORDENAR POR.

A funcionalidade do aplicativo que coloca dados não confiáveis nessas partes da consulta precisará adotar uma abordagem diferente, como valores de entrada permitidos na lista branca ou usando uma lógica diferente para fornecer o comportamento necessário.

Para que uma consulta parametrizada seja eficaz na prevenção da injeção de SQL, a string usada na consulta deve ser sempre uma constante embutida no código e nunca deve conter dados variáveis de qualquer origem. Não fique tentado a decidir caso a caso se um item de dados é confiável e continue usando a concatenação de string dentro da consulta para casos considerados seguros.

Dentro desse senário podemos entender que a Segurança da informação é muito importante nos sistemas de hoje, não somente na aplicação, mas também nos servidores físicos, rede de dados, etc. Podemos entender que com pequenos ajustes podemos evitar grandes problemas no futuro.

5. DISCUSSÃO

Nos sistemas Web modernos são projetados inúmeros métodos de proteção das informações diante de ameaças internas e externas e esses métodos são extremamente importantes e fundamentais para a integridade digital de uma empresa. Além disso esses métodos minimizam em grande parte as possibilidades de captura de dados sigilosos por pessoas e softwares não autorizados, são implementadas camadas extras a um determinado código fonte de uma linguagem server-side, sendo aplicado filtros extras na hora de inserção de dados como login, senha. Com essas camadas de proteção pode ser evitado danos para o andamento das operações e até prejuízos financeiros. Estes esforços estão contemplados na Segurança da Informação (SI).

Segundo Campos (2007), as informações são elementos de grande importância no processo de negócio de uma organização. A segurança da informação está diretamente ligada em maneiras de proteger os dados sejam de pessoa física ou jurídica estando sob a responsabilidade de uma empresa. São aplicados esforços para garantir a integridade dos dados para a redução de riscos de vazamento de informações sigilosas e para que o sistema mantenha sua estabilidade funcionando de maneira correta.

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto as pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

Neste trabalho podemos enfatizar diversas informações de como a Segurança da Informação é tão importante para o funcionamento e a estabilidade de um sistema web.

Após muitas pesquisas podemos descobrir fatos relevantes que mostram informações sobre as primeiras fases da evolução da tecnologia e a criação da internet que foi criada em 1969, nos Estados Unidos. Chamada de Arpanet, que tinha como função interligar laboratórios de pesquisa. Naquele ano, um professor da Universidade da Califórnia passou para um amigo em Stanford o primeiro e-mail da história.

Na prática do desenvolvimento e a utilização das ferramentas de Segurança da Informação os códigos utilizados para gerar filtros são de fácil

compreensão para que todos possam entender com clareza o real objetivo da Segurança da Informação e como os dados são tratados.

A solução apresentada neste trabalho, são as maneiras corretas de usabilidade de scripts para resolver problemas de segurança em sistemas web usando linguagem de programação Server-Side, traçando metodologias de inserção de códigos fontes mais elaborados para o gerenciamento de informações sigilosas de uma pessoa ou empresa.

A segurança da informação nesse contexto se mostra essencial, e até mesmo crítica em alguns casos, para que a consistência dos sistemas não seja afetada, garantindo a redução de riscos de fraudes, erros, vazamento, roubo e uso indevido e uso indevido de informações. A segurança pode ser afetada por certos comportamentos de seus usuários, pelo ambiente ou estrutura que a cerca, ou por sujeitos mal intencionados com o objetivo de furtar, destruir ou alterar alguma informação.

Existem níveis de segurança que podem ser estabelecidos, tais como identificados em políticas de segurança para garantir que o nível de segurança que se deseja estabelecer seja mantido. Para a construção de uma política de segurança existem alguns fatores que devem ser considerados, tais quais, riscos, benefícios, custos e esforços de implementação dos mecanismos.

6. CONCLUSÃO

Analisando os assuntos propostos e as atividades desenvolvidas, podemos ver e entender a grande importância do uso da Segurança da Informação em Sistemas Web para proteger nos dados sigilosos, a maneira que são acessados e por onde são acessados de forma correta e segura.

As tecnologias atuais são resultados do desenvolvimento tecnológico alcançado pelo ser humano e têm um papel fundamental no âmbito da inovação. Os avanços da tecnologia provocam grande impacto na sociedade, resulta em inovações que proporcionam melhor nível de vida ao Homem.

Com o avanço da internet surge a criação do primeiro site. The Project, como é conhecida o primeiro site da história, foi criado por Tim Berners-Lee, conhecido como o Pai da World Wide Web (WWW). Sua estreia aconteceu no dia 6 de agosto de 1991 e, nele, seu criador descreve brevemente detalhes da World Wide Web. O objetivo deste espaço principal era permitir que os profissionais do Centro de Europeu de Pesquisa Nuclear (CERN) no qual Berners-Lee atuava como físico tivessem acesso rápido aos códigos e procedimentos para criar sites semelhantes.

Para atingir os objetivos propostos e comprovar os resultados da usabilidade da segurança da informação, foi realizado uma pesquisa em duas fases. A primeira fase foi a busca pelas informações sobre as primeiras fases da evolução da tecnologia e a criação da internet que foi criada em 1969, nos Estados Unidos. Chamada de Arpanet, que tinha como função interligar laboratórios de pesquisa. Naquele ano, um professor da Universidade da Califórnia passou para um amigo em Stanford o primeiro e-mail da história.

Foi buscado informações sobre criação do primeiro site que foi resultado do avanço da internet que impulsionou a criação desse site. The Project, como é conhecido o primeiro site da história, foi criado por Tim Berners-Lee, conhecido como o Pai da World Wide Web (WWW). Este grande acontecimento foi realizado no dia 6 de agosto de 1991 e, nele, seu criador descreve brevemente detalhes da World Wide Web. O objetivo deste espaço principal era permitir que os profissionais do Centro de Europeu de Pesquisa Nuclear (CERN) no qual

Berners-Lee atuava como físico tivessem acesso rápido aos códigos e procedimentos para criar sites semelhantes.

Este trabalho traz informações de como a Segurança da Informação é tão importante para o funcionamento e a estabilidade de um sistema web. Os códigos utilizados para gerar filtros são de fácil compreensão para que todos possam entender com clareza o real objetivo da Segurança da Informação e como os dados são tratados.

Neste trabalho podemos enfatizar diversas informações de como a Segurança da Informação é tão importante para o funcionamento e a estabilidade de um sistema web.

A segurança da informação nesse contexto se mostra essencial, e até mesmo crítica em alguns casos, para que a consistência dos sistemas não seja afetada, garantindo a redução de riscos de fraudes, erros, vazamento, roubo e uso indevido e uso indevido de informações. A segurança pode ser afetada por certos comportamentos de seus usuários, pelo ambiente ou estrutura que a cerca, ou por sujeitos mal intencionados com o objetivo de furtar, destruir ou alterar alguma informação.

Existem níveis de segurança que podem ser estabelecidos, tais como identificados em políticas de segurança para garantir que o nível de segurança que se deseja estabelecer seja mantido. Para a construção de uma política de segurança existem alguns fatores que devem ser considerados, tais quais, riscos, benefícios, custos e esforços de implementação dos mecanismos.

6.1 TRABALHOS FUTUROS

Como sugestão para a continuação desse trabalho, deve ser feita uma pesquisa em algumas empresas para determinar a necessidade de conhecimento atual do profissional de segurança da informação e o nível de oportunidades encontradas hoje no mercado do trabalho.

Atualmente, nota-se no cenário da Segurança da informação a necessidade de mais profissionais nessa podemos destacar algumas categorias:

- Aqueles que possuem contato direto com a rede de uma organização e os recursos tecnológicos que a compõem, identificação de vulnerabilidades, possíveis ameaças e maneiras de mitigá-las, os chamados *Ethical Hackers*, que possuem as mesmas habilidades que possíveis atacantes e as utilizam em prol da organização. Nas organizações, é comum vermos a divisão desses profissionais em duas equipes:
    - *Red team* – Responsável por identificar as vulnerabilidades em uma rede de computadores e como estas podem ser exploradas. Essa equipe possui a visão mais parecida com a visão de um atacante.

    - *Blue team* – Responsável por mitigar as ameaças encontradas pelo *Red team*. São os responsáveis pela defesa da rede corporativa.

    - Aqueles que atuam na área de GRC (Governança, Risco e *Compliance* – também identificada como Conformidade). Esses profissionais são responsáveis pela aplicação e monitoramento de regras, leis, políticas e afins dentro de uma organização. Para melhor entendimento, podemos fazer uma analogia e dizer que esses profissionais são os “advogados” do setor de TI de uma organização. Em empresas grandes, é comum ver também a área de Governança Corporativa, que tem a mesma finalidade, abrangendo a corporação como um todo.

Para ambas as funções, é comum que uma empresa terceirize a mão de obra, contratando empresas de consultoria de Segurança da Informação, que possuem uma visão mais direcionadas sobre as regras e normas que devem ser seguidas para que a empresa contratante tenha suas atividades regularizadas e documentadas, em conformidade com normas impostas por órgãos regulamentadores e leis de seu segmento de atuação.

Sendo assim é importante também avaliar a intenção de investimento financeiro por parte das empresas no profissional contratado para alcançar o nível técnico desejado pela empresa.

No entanto um profissional que adquire certificações na área de segurança da informação se destaca sendo bem-visto no mundo do trabalho, pois com essas certificações informa à empresa que o profissional tem o conhecimento apropriado e está habilitado a proteger seus dados sigilosos com segurança.

7. REFERÊNCIAS

ABREU, K. C. K. História e usos da internet. Biblioteca on-line de Ciências da Comunicação. Universidade da Beira Interior. Covilhã, 2009.

ALMEIDA, I. Primeiro site da história estreava há 30 anos — e ele ainda está no ar. Yahoo Esportes. 2021. Disponível em: < https://esportes.yahoo.com/noticias/primeiro-da-hist%C3%B3ria-estreava-h%C3%A1-125300418.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABRVqyhDohyUX8fuJJqKBnxNl4ajLLIk5LYXhgvMLLV41_lqwWwF5618cjAnDnDlAx6n02b383DZ0TaxWGg_h6I-m_snvLwUBITgvInbEBrzHxLwJVGaH2pzSJvDhLJ6lb7gZI2VBNohdIb25KR_m9giJI3ghw2jqTmagTOqSI8v>. Acesso em: 18 de nov. 2021.

CONVERSE, T.; PARK, J. PHP: a bíblia. [S.l.]: Gulf Professional Publishing, 2003.

DIAS, C. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Axcel, 2000.

FOLHA DE SÃO PAULO. Internet foi criada em 1969 com o nome de "Arpanet" nos EUA. FOLHA DE SÃO PAULO. 2001. Disponível em: < https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml>. Acesso em: 19 de nov. 2021.

FIA, F. Segurança da informação. FIA. 2008. Disponível em: < https://fia.com.br/blog/seguranca-da-informacao/>. Acesso em: 19 de nov. 2021.

GUPTA, M. et al. Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. Decision Support Systems, 2004. No prelo.

OFICINA, R. Segurança da informação, conceitos e mecanismos. Oficina da Net. 2008. Disponível em: < https://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos>. Acesso em: 18 de nov. 2021.

ROSSETTI, A. G.; MORALES, A. B. T. O papel da tecnologia da informação na gestão do conhecimento. Ciência da Informação, SciELO Brasil, v. 36, n. 1, p. 124–135, 2007.

SÊMOLA, M. Gestão da Segurança da Informação - Uma Visão Executiva - 2 ed. São Paulo: Elsevier, 2014.

STONEBURNER, Gary. Underlying Technical Models for Information Technology Security. NIST Special Publication 800-33, 2001.

SHIREY, R. RFC 2828 - Internet Security Glossary. 2000. Disponível em: https://www.ietf.org/rfc/rfc2828.txt. Acesso em: 4 fev. 2021.

WINDER, DAVEY. Classificado: As 100 piores senhas do mundo. Forbes. 2019. Disponível em: < https://www.forbes.com/sites/daveywinder/2019/12/14/ranked-the-worlds-100-worst-passwords/>. Acesso em: 18 de nov. 2021.