JOAO VITOR PEREZ SARAIVA

Resumo

Uma pesquisa sobre a segurança na web com conceitos, ferramentas, praticas pra segurança e tendencias para a melhora na segurança

SeguRANÇA NA WEB

Sumário

[Segurança na Web 2](#_Toc160031338)

[Conceitos- 2](#_Toc160031339)

[Práticas Recomendadas- 5](#_Toc160031340)

[Ferramentas- 6](#_Toc160031341)

[Tendencias- 8](#_Toc160031342)

[Referencias: 9](#_Toc160031343)

# Segurança na Web

## Conceitos-

Segurança da Internet é um termo que descreve a segurança de atividades e transações feitas na Web. Trata-se de um componente particular de ideias maiores, como segurança virtual e segurança do computador, envolvendo tópicos que incluem segurança do navegador, comportamento on-line e segurança de rede.



As vulnerabilidades das aplicações web permitem que fatores maliciosos tenham controle não autorizado sobre o código-fonte, manipulem informações privadas.

Tendo certos erros nas aplicações web que fazem o “hacker” ter acesso indevido na mesma.

**Ataque de Preenchimento de Credenciais**

Os hackers usam nomes de usuários, e-mails e senhas de lixeiras públicas da dark web para invadir e assumir as contas dos usuários. Os dados ilegais podem conter milhões de nomes de usuários e combinações de senhas, devido aos anos de violações de dados em diversos sites.

**O que é Segurança Web?**

Como uma área de cibersegurança, a segurança web se concentra em proteger sites, aplicativos baseados na internet e serviços online contra uma variedade de ataques maliciosos. Deste modo, ela serve para garantir o bom funcionamento e desempenho dos sites.

**Injeção de SQL**

Este tipo de falha permite que um cibercriminoso adultere uma consulta no banco de dados da aplicação através da injeção de um código. Na maioria dos ataques, os hackers conseguem acessar dados protegidos de usuários ou até mesmo da aplicação, como senhas, informações de cartão de crédito e cookies.

**Phishing**

É um ataque virtual envolvendo e-mails enganosos. Os hackers tentam enganar os remetentes dos e-mails para que acreditem que uma mensagem é genuína e relevante, uma solicitação do seu banco ou uma nota de um colega de trabalho, por exemplo, de forma que cliquem em um link ou abram um anexo. O objetivo é enganar as pessoas para que entreguem informações pessoais ou baixem malware.



**Hackeamento e acesso remoto**

Os hackers estão sempre procurando explorar uma rede privada ou vulnerabilidades do sistema, de forma que possam roubar informações e dados confidenciais. A tecnologia de acesso remoto dá a eles outro alvo a ser explorado. Os softwares de acesso remoto permitem que os usuários acessem e controlem um computador remotamente e, desde a pandemia, com mais pessoas trabalhando remotamente, sua utilização aumentou.

**Malware**

Malware é a combinação dos termos "malicious" (malicioso) e "software". É um termo amplo relacionado a vírus, worms, cavalos de Troia e outros programas danosos que os hackers usam para causar estragos e roubar informações confidenciais. Qualquer software criado para danificar um computador, servidor ou rede pode ser descrito como malware.

**Ransomware**

é um tipo de malware que impede você de usar o seu computador ou acessar arquivos específicos no seu computador se um resgate não for pago. Geralmente, ele é distribuído como um cavalo de Troia, ou seja, malware disfarçado de software legítimo. Após instalado, ele bloqueia a tela do seu sistema ou alguns arquivos até que você pague.

## Práticas Recomendadas-

As práticas recomendadas pra se navegar na web são diversas geralmente é envolvida para as pessoas:

**Verifique se os sites são seguros**

Verifique se os sites que você acessa têm um certificado SSL e usam o protocolo de segurança“https”, que é criptografado (o "http" não é). Essa é apenas uma etapa que pode ajudar a evitar golpes como o spoofing.

**Instale as atualizações de software mais recentes**

Cibercriminosos estão constantemente encontrando novos vetores de ataque. As atualizações de software mais recentes para seu dispositivo e aplicativos ajudam a corrigir riscos e vulnerabilidades de segurança.

**Faça backup de seus dados**

No caso de um ataque de malware ou falha do dispositivo, talvez seja necessário formatar o aparelho. O backup dos seus dados em um dispositivo de armazenamento externo e na nuvem pode ser um salva-vidas.

**Cuidado com o que você publica**

As informações que você compartilha online podem ser usadas contra você ou permitir que alguém roube sua identidade. Mantenha-se em segurança na internet ocultando detalhes importantes sobre você.

**Use a 2FA**

Com a autenticação de dois fatores (2FA), você usa dois métodos para acessar uma conta. Se sua senha for roubada, sua conta protegida por 2FA permanecerá segura e privada.

**Use um antivírus confiável**

Usar antivírus modernos, que são atualizados para proteger os usuários contra as ameaças mais recentes.

**Evite anexos ou links suspeitos**

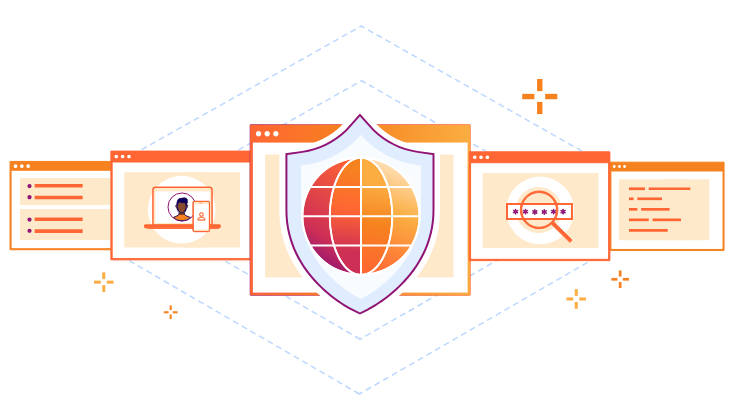
Links e anexos não seguros podem levar ao roubo de dados ou infecções por malwares. E-mails falsos ou sites maliciosos podem parecer muito convincentes.

## Ferramentas-

Uma solução de segurança para aplicações web protege as empresas de ataques que visam tirar proveito das vulnerabilidades de código presentes em uma aplicação.

**Cloudflare**

Com a interface intuitiva da Cloudflare, os usuários podem identificar e analisar rapidamente os riscos de segurança, bloqueando quaisquer possíveis ameaças cibernéticas.



Suas regras personalizadas de proteção firewall protegem seu site e APIs contra o tráfego malicioso, enquanto o log de atividades o ajudará a ajustar as configurações de segurança.

Impeça o uso de credenciais roubadas ou expostas que possam permitir o acesso de invasores à sua conta. Os serviços da Cloudflare também incluem um firewall para as aplicações web e proteção contra DDoS.

**StackHawk**

A StackHawk analisa seus aplicativos, serviços e APIs em busca de falhas de segurança no código ou em componentes de código aberto. Ela é muito eficiente na localização e correção dos erros, permitindo que os desenvolvedores da sua equipe repliquem o problema que provocou uma vulnerabilidade apenas copiando um comando cURL.

**Barracuda**

A Barracuda Cloud Application Protection protege suas aplicações de várias ameaças combinando recursos WAF completos com serviços e soluções de segurança avançados. Além de proteger as aplicações da web, a Barracuda também oferece soluções para proteger seu serviço de email com domínio, dados e rede.

## Tendencias-

A segurança da informação é uma preocupação cada vez maior para indivíduos e organizações. À medida que a tecnologia se torna mais complexa e os ataques cibernéticos se tornam mais sofisticados, é importante estar ciente das tendências que estão moldando o futuro da segurança da informação.

Essas tendências podem ter um impacto significativo em nosso dia a dia, afetando a maneira como as pessoas trabalham, se comunicam e se divertem.

**IA generativa democratizada**

A Inteligência Artificial (IA) tem desempenhado um papel cada vez mais crucial na segurança da informação, e a tendência para 2024 é a democratização da IA generativa.

A capacidade de gerar conteúdo de maneira autônoma e inovadora oferece oportunidades significativas para melhorar a segurança cibernética.

**Segurança Adaptável**

O mundo digital está em constante mudança, e as empresas precisam de uma abordagem de segurança que possa se adaptar a essas mudanças. A segurança adaptável é uma abordagem que usa inteligência artificial e machine learning para identificar e responder às ameaças em tempo real.

**Governança de dados**

A governança de dados é o processo de garantir que os dados sejam gerenciados de forma segura e eficiente. Essa é uma área importante de segurança da informação, pois os dados são um ativo valioso para as organizações.

## Referencias:

INTELIGÊNCIA SOFTWALL. **5 Tendências de Segurança da Informação para 2024**. Disponível em: <https://www.softwall.com.br/blog/5-tendencias-seguranca-da-informacao-2024/>. Acesso em: 28 fev. 2024.

‌

KASPERSKY. **Segurança da Internet: o que é e como você pode se proteger on-line?** Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-internet-security>. Acesso em: 28 fev. 2024.

‌

VIDANYA, B. **Segurança Web: O que é, Como Funciona e Quais os Melhores Serviços**. Disponível em: <https://www.hostinger.com.br/tutoriais/seguranca-web>. Acesso em: 28 fev. 2024.

‌

DEEPAN GHIMIRAY. **Principais dicas de segurança na internet para todos**. Disponível em: <https://www.avast.com/pt-br/c-internet-safety-tips>. Acesso em: 28 fev. 2024.

‌