**Tipos de Ataques a aplicações web**

As aplicações web são frequentemente alvo de diversos tipos de ataques maliciosos devido às vulnerabilidades presentes em suas estruturas. Algumas das principais formas de ataques incluem:

**SQL Injection**

Consiste na inserção de comandos SQL maliciosos através de campos de entrada de dados, permitindo manipulação do banco de dados da aplicação.

**CSRF (Cross-site request forgery)**

Envolve a falsificação de solicitações entre sites, onde comandos não autorizados são transmitidos a partir de um usuário com acesso legítimo, explorando a autenticação da sessão.

**XSS (Cross-site scripting)**

Permite a injeção de código malicioso no navegador do usuário através de campos de entrada não validados, possibilitando o roubo de cookies, tokens e dados de acesso.

**Broken Authentication**

Ocorre quando o sistema falha em utilizar métodos confiáveis de autenticação e armazenamento de informações do usuário, facilitando ataques de força bruta.

**Sensitive Data Exposure**

Envolve a exposição inadequada de informações transmitidas por APIs, permitindo que invasores as explorem para obter dados sensíveis.

**XXE (XML External Entities)**

Específico de sistemas que trabalham com XML, onde invasores podem injetar códigos maliciosos em documentos XML para exploração.

**Broken Access Control**

Falha que permite a usuários não autorizados acessar informações restritas do sistema, geralmente devido a falhas na validação de permissões.

**Security Misconfiguration**

Ocorre devido a configurações incorretas de segurança, como informações abertas na nuvem ou headers HTTP mal configurados.

**Insecure Deserialization**

Vulnerabilidade explorada para execução remota de códigos maliciosos ou escalonamento de privilégios.

**Using Components with Known Vulnerabilities**

Refere-se ao risco de utilizar bibliotecas ou componentes com falhas conhecidas, tornando a aplicação vulnerável a exploits.

**Insufficient Logging & Monitoring**

Falha na implementação de registros de atividades e monitoramento em tempo real, dificultando a detenção de atividades suspeitas e ataques.

É crucial que os desenvolvedores estejam cientes dessas vulnerabilidades e implementem medidas de segurança adequadas para proteger suas aplicações web contra esses tipos de ataques.

**Camadas e Mecanismos de Segurança**

A estratégia de segurança em camadas é crucial para proteger sistemas e dados contra-ataques cibernéticos, consistindo na implementação de várias etapas de proteção. Essa abordagem visa tornar os ataques mais difíceis e demorados, desestimulando os criminosos. Ela vai além da proteção tradicional de antivírus, oferecendo benefícios como proteção contra malwares, phishing e vazamentos, segurança proativa e facilidade de implementação.

**Oque é estratégia de segurança em camadas**

São barreiras que são impostas em cada camada de informação de modo a torna o ataque cibernético mais trabalhoso e demorado tendo como abjectivo principal desestimular a acção pela a dificuldade imposta. Ela concentra não só os antivírus mais também um serie de ferramentas que aprimoram a protecção e afastam os perigos dos ataques digitais.

**Benefícios da protecção em camadas:**

* Protecção contra malwares, phishings, vazamentos e outros ciberataques;
* Segurança proativa;
* Facilidade de implementação;
* Protecção multicamadas.

**As principais camadas dessa estratégia incluem:**

**Firewall:** Filtra o tráfego de rede e bloqueia acessos suspeitos.

**Proteção de Dados:** Prioriza a segurança das informações corporativas, permitindo a recuperação em caso de perda física.

**Rede:** Protege contra falhas na firewall, neutralizando ameaças que ultrapassam outras camadas.

**DNS**: Funciona como uma agenda para proteger informações na busca por sites.

**Backup:** Essencial como medida de rotina para recuperação de dados em caso de perdas.

**Quais as melhores práticas de segurança da informação?**

As melhores práticas de segurança da informação incluem prevenção de falhas, atualização contínua de sistemas de proteção, identificação de vulnerabilidades e implementação de consultoria especializada.

Além disso, é importante investir em segurança de e-mails, já que muitas comunicações e acordos corporativos ocorrem por meio desse canal. Proteger os e-mails impede a interceptação criminosa, roubo de identidades virtuais e recebimento de spams, melhorando a confidencialidade e produtividade da empresa. O gestor de TI deve priorizar a segurança dos dados corporativos e conhecer os conceitos para uma boa implementação das camadas de segurança da informação.