PADRÃO DE RESPOSTA – DISCURSIVA

CONCURSO PÚBLICO – CÂMARA MUNICIPAL DE BELO HORIZONTE/MG

CARGO: ANALISTA DE TECNOLOGIA DA INFORMAÇÃO – ÁREA DE DESENVOLVIMENTO DE SISTEMA

Questão 01

O SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) é um protocolo criptográfico utilizado para garantir a segurança da comunicação em redes, especialmente na *web*. Ele permite que um cliente e um servidor estabeleçam uma conexão segura, protegendo os dados transmitidos contra interceptação e adulteração por terceiros.

O SSL/TLS opera em camada de transporte, fornecendo segurança adicional sobre os protocolos de transporte, como TCP.

Para estabelecer uma conexão segura, o SSL/TLS realiza um processo de negociação de parâmetros de segurança, onde o cliente e o servidor concordam sobre os algoritmos de criptografia e outros parâmetros a serem utilizados na comunicação. Isso inclui a escolha de algoritmos de criptografia simétrica e assimétrica, bem como métodos de autenticação.

Após a negociação dos parâmetros de segurança, o SSL/TLS realiza um processo de estabelecimento de sessão, onde são trocadas chaves criptográficas para proteger a comunicação. O cliente e o servidor utilizam essas chaves para cifrar e decifrar os dados transmitidos, garantindo a confidencialidade e integridade da informação.

Fonte:

Stallings, William; **Criptografia e segurança de redes: princípios e práticas** / WilliamStallings; tradução Daniel Vieira; revisão técnica Paulo Sérgio LicciardiMesseder Barreto, Rafael Misoczki. 6. ed. São Paulo: PearsonEducation do Brasil, 2015.

Questão 02

Para garantir a segurança de um aplicativo *web*, é essencial compreender os principais conceitos relacionados a essa área. Isso inclui entender a importância da autenticação, autorização, criptografia, controle de acesso e validação de entrada de dados para proteger o sistema contra ameaças como ataques de injeção de código, *cross-site scripting* (XSS), *cross-site request forgery* (CSRF) e outros tipos de ataques comuns.

Além disso, é fundamental realizar uma análise de vulnerabilidades em aplicações *web* para identificar possíveis brechas de segurança. Isso pode ser feito utilizando ferramentas automatizadas, como *scanners* de vulnerabilidades, que ajudam a identificar vulnerabilidades conhecidas no código do aplicativo. Técnicas manuais de revisão de código também são importantes para identificar vulnerabilidades específicas que podem passar despercebidas pelos *scanners* automatizados.

No entanto, apenas identificar vulnerabilidades não é suficiente; é necessário explorar essas vulnerabilidades para entender seu impacto potencial no sistema e tomar medidas corretivas adequadas. Existem várias ferramentas e técnicas disponíveis para explorar vulnerabilidades em aplicativos *web*, incluindo ferramentas de *proxy*, *fuzzing*, manipulação de *cookies* e cabeçalhos HTTP, dentre outras.

Por fim, os testes de invasão em aplicativos *web* desempenham um papel crucial na avaliação da segurança do sistema. Esses testes simulam ataques reais contra o aplicativo para identificar e corrigir falhas de segurança antes que sejam exploradas por atacantes reais. Ao realizar testes de invasão regulares, é possível melhorar continuamente a segurança do aplicativo *web* e garantir a proteção dos dados confidenciais dos usuários e da organização.

Fontes:

- DUARTE, Luiz Otávio. **Segurança de Redes em Ambientes Cooperativos**. Rio de Janeiro: Ciência, Moderna, 2013.
- STALLINGS, William; **Criptografia e segurança de redes: princípios e práticas** / WilliamStallings; tradução Daniel Vieira; revisão técnica Paulo Sérgio LicciardiMesseder Barreto, Rafael Misoczki. 6. ed. São Paulo: PearsonEducation do Brasil, 2015.
- SINDRE, G. **Segurança de Redes em Ambientes Corporativos**. São Paulo: Pearson, 2014.
- TERADA, R. **Segurança de dados: criptografia em redes de computador**. ed. São Paulo: Editora Edgard Blucher, 2008.