Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

SUPERIOR TRIBUNAL MILITAR (STM)

CARGO 3: ANALISTA JUDICIÁRIO – ÁREA: APOIO ESPECIALIZADO – ESPECIALIDADE: ANÁLISE DE SISTEMAS

Prova Discursiva

Aplicação: 01/06/2025

PADRÃO DE RESPOSTA DEFINITIVO

O modelo MVC (*model-view-controller*) é um padrão de arquitetura que separa a aplicação em três componentes principais: modelo, visão e controlador. O componente modelo representa os dados e a lógica ou as regras de negócio da aplicação. O componente visão refere-se à interface com o usuário e como será realizada essa interação. Por fim, o componente controlador realiza a intermediação das requisições. Esse tipo de modelo é muito utilizado em aplicações monolíticas. Já a arquitetura de microsserviços organiza a aplicação como um conjunto de serviços independentes, cada um executando uma funcionalidade específica e comunicando-se por meio de APIs. Ao contrário do MVC, que privilegia a separação interna da aplicação, os microsserviços distribuem funcionalidades em módulos autônomos, o que facilita a escalabilidade horizontal e a manutenção. Nota: embora tipicamente associado a aplicações monolíticas, o MVC também pode ser aplicado dentro de cada microsserviço individualmente.

Entre os riscos ou as vulnerabilidades que podem surgir em arquiteturas baseadas em *webservices*, dos quais o candidato deverá citar dois, destacam-se: (i) **ataques de injeção** (como SQL *Injection* ou XML *Injection*), que exploram falhas na validação de entrada para executar comandos maliciosos; (ii) **exposição de APIs sem autenticação ou controle de acesso**, o que permite o uso indevido por terceiros; (iii) **ataques de negação de serviço** (DoS), que podem comprometer a disponibilidade do serviço; ~~e~~ (iv) **falta de criptografia no tráfego de dados** (como ausência de HTTPS), o que facilita ataques de interceptação (*man-in-the-middle*)~~.~~; (v) vulnerabilidades relacionadas a falhas criptográficas; (vi) falhas de autenticação e autorização; (vii) manipulação de dados; (viii) Cross-Site Scripting (XSS); (ix) Cross-Site Request Forgery (CSRF); (x) Broken Access Control; e (xi) falta de criptografia dos dados em repouso e trânsito.

Entre os mecanismos ou testes específicos de segurança recomendados para aplicações que implementam *webservices*, dos quais o candidato deverá citar dois, destacam-se: (i) **autenticação baseada em *tokens***, como OAuth 2.0, SAML ou JWT, mecanismos que permitem que apenas usuários autenticados e autorizados acessem os *webservices*, o que reduz o risco de acesso não autorizado e vazamento de dados sensíveis; (ii) ***web application firewalls*** (WAFs), que atuam como barreiras de proteção, analisando requisições e bloqueando padrões conhecidos de ataques (por exemplo, *scripts* de injeção), de modo que contribuem para a mitigação de ameaças em tempo real; (iii) **escaneamento de vulnerabilidades com ferramentas como OWASP ZAP ou *burp suite***, que identificam automaticamente falhas conhecidas em APIs e serviços *web* e auxiliam na correção proativa antes que sejam exploradas por atacantes; (iv) **testes de penetração (*pentests*)**, que simulam ataques reais contra os sistemas e permitem avaliar a resiliência das defesas, identificar vulnerabilidades lógicas e validar a eficácia dos controles de segurança implantados~~.~~; (v) testes estáticos (SAST) e dinâmicos (DAST) de segurança de código; (vi) uso de Proxy Gateway para controle e proteção das requisições; (vii) validação rigorosa das entradas para prevenir vulnerabilidades como injeções; (viii) utilização de autenticação multifator (MFA) e autenticação unificada (SSO); (ix) estratégias de mitigação de ataques volumétricos (*rate limiting* e *circuit breakers*); (x) utilização de autenticação multifator (MFA) e autenticação unificada (SSO); e (xi) estratégias de mitigação de ataques volumétricos (*rate limiting* e *circuit breakers*).

QUESITOS AVALIADOS

QUESITO 2.1 Definição e comparação de MVC e microsserviços
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Apresentou corretamente apenas um dos aspectos a seguir, sem mencionar os demais: (i) definição de MVC; (ii) definição de microsserviços; (iii) breve comparação entre ambos.
Conceito 2 – Apresentou corretamente um dos aspectos precedentes, e apresentou outro de forma parcialmente correta.
Conceito 3 – Apresentou corretamente dois dos aspectos precedentes, apresentando o outro de forma parcialmente correta.
Conceito 4 – Apresentou corretamente os três aspectos precedentes.

QUESITO 2.2 Riscos ou vulnerabilidades em *webservices*
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Citou corretamente apenas um risco ou uma vulnerabilidade.
Conceito 2 – Citou corretamente dois riscos ou duas vulnerabilidades.

QUESITO 2.3 Mecanismos/testes de segurança e justificativa
Conceito 0 – Não abordou o quesito ou o fez de forma totalmente equivocada.
Conceito 1 – Citou corretamente apenas um mecanismo ou teste de segurança, mas não apresentou justificativa correta.
Conceito 2 – Citou justificadamente apenas um mecanismo ou um teste de segurança, ou citou, sem justificativa, dois mecanismos ou testes de segurança.
Conceito 3 – Citou justificadamente os dois mecanismos ou testes de segurança.