Validação e Sanitização de Entrada de Dados

Descrição: Trate todo dado recebido do usuário como potencialmente perigoso; sempre valide e sanitize antes de usá-lo.

Aplicação: Limite a sanitização às funções que recebem dados diretamente do usuário.

Uso Preciso de Sanitização

Descrição: Evite o excesso de sanitização em funções internas para evitar redundância e melhorar a eficiência do código.

Aplicação: Aplique sanitização com precisão, priorizando pontos onde o usuário interage diretamente.

SSH e Segurança de Rede

Descrição: Conheça a capacidade do SSH para manter uma conexão segura e, quando necessário, configurar túnel seguro e reenvio de portas.

Aplicação: Use SSH para garantir conexões seguras e explore opções como tunneling e port forwarding com consciência.

Exposição e Controle de Firewall e Proxy

Descrição: Controle o acesso a portas e conexões externas com a configuração de firewall e regras de proxy bem definidas.

Aplicação: Siga o princípio do “privilégio mínimo”, permitindo apenas o essencial para reduzir a superfície de ataque.

Atualização Contínua de Ferramentas e Conhecimento

Descrição: Entenda profundamente as ferramentas de segurança que utiliza, buscando sempre atualizar e aprimorar conhecimentos.

Aplicação: Estude as ferramentas que você usa, como SSH e firewalls, para entender como protegê-las.

Desconfiança Construtiva com Usuários

Descrição: Assuma que todo usuário pode ser uma potencial ameaça para o sistema.

Aplicação: Configure verificações rigorosas, tratativas seguras e monitoramento contínuo em pontos onde há entrada de dados de usuários.