Na aula de Hoje – Segurança de Aplicação

* O contexto da segurança da aplicação
* O WASP Top 10 Most Critical Web App Security Risks
  + Estudo sobre os riscos
  + O papel do desenvolvedor.
* Orientação para o projeto sobre Hardening do B. D.

Segurança de aplicação

1. 1º Segurança no perímetro, Firewall, IDS.
   1. Segurança do aplicativo Web
   2. O aplicativo pode ser um meio para o ataque já que os dados estão armazenados no B. D.
   3. Não há Segurança no B. D. sem compreender como as vulnerabilidades do app podem afetar o B. D.
2. Segurança no BD pelo Dev: - O B. D. é parte do app, extensão do código, gerido e controlado pelo app – Acesso completo a todos os objetos do B. D.
   1. Segurança do B. D. pelo DBA: - O App é um ponto de atenção – Violação da segurança no app expõe o B. D.
   2. Modelo de Autenticação e autorização
3. Vulnerabilidade senha B. D. em arquivo de configuração
   1. DBA deve entender sobre o ambiente do app
   2. Muitos exemplos do ambiente de produção
   3. Configurações padrões dos frameworks de desenvolvimento
4. Questão Como Enfrentar as Vulnerabilidades ?
   1. Criar relatórios com nomes de usuários do B. D., endereço IP e quais app acessam o B. D.
      1. Usar ferramentas do tipo who – what , when-where
      2. Como as senhas estão armazenadas no app?
         1. Use relatório como uma linha base.
         2. Procure por novos pontos de acesso
            1. Pode ser um app que legitimamente está acessando o B. D.
            2. Pode ser um ataque Hacker

Utiliza-se uma máquina diferente para execução de Scripts

* + - 1. Bloquear acessos de um IP que não está na linha base
         1. Usar um firewall padrão ou firewall SQL
  1. Autenticação via S. O.
     1. Usar LDAP evitar manter senhas em arquivos de configuração
  2. Ofuscar o código da app
     1. Técnica usada em Java e .NET
     2. Transforma pseudocódigo em formato que torna a engenharia reversa difícil.
     3. Existe utilitários para isso.