Desenvolvimento Web II - Segurança em Projetos Web

Professor: Dr. William Simão de Deus

william.deus@ifpr.edu.br

Instituto Federal do Paraná (IFPR)
Campus Pinhais

Curso Superior em Gestão de Tecnologia da Informação – 2024.01
Processos e Técnicas de Pesquisa

Sumário

Introdução

- A segurança em projetos web é um tópico essencial
- Serve para evitar que os webapps (projetos web) fiquem vulneráveis aos ataques das mais diversas naturezas
- Ainda hoje, há muitos casos de ataques
- Exemplos: ataques de injeção de SQL, DDoS...

Recusa de serviço

Também chamados de DoS (denial of service)

- São predominantes e fáceis de serem executados
- Podem ocorrer por interesse em incomodar ou retaliar alguma ação
- Alguns ataques, no entanto, podem ser algo de porte maior e mais complexo...

Explorando fragilidades

- Ataques DoS podem explorar fragilidades de softwares com erros de programação
- Nesses casos, os atacantes buscam explorar fragilidades existentes nos softwares para obter acesso ao sistema ou negar o serviço aos usuários reais
- Exemplos: *Ping of death* (estouro de buffer), *dear drop* (informação mal formatada) e exaustão de recurso.

Degradação da rede

- Variação do ataque de exaustão de recurso
- Foca na estrutura da rede ao invés do software em si
- Exemplo: consumir a largura da banda de rede

Ataques de amplificação

- Forma de ataque na qual o invasor possui menos largura de banda do que o alvo/vítima
- Nesse caso, o invasor não conseguiria degradar a rede, por ter menos recursos disponíveis
- O invasor falsifica seu registro e envia uma solicitação para uma rede. A rede entende que deve amplificar seu poder, enviando centenas de respostas para o destino (alvo/vítima)

Ataques de fragmentação

- Ao invés de enviar uma grande solicitação, enviar diversos fragmentos de uma solicitação
- Colocar pacotes fora de ordem, com sobreposição ou reenvio do mesmo pacote
- Gerar um caos no alvo/vítima

Recusa de Serviço Distribuído

Também chamado de DDoS (distributed denial of service)

- Consiste em subjugar seu oponente com números absolutos

De forma resumida, há o invasor, os agentes e um alvo:

- Invasor: atacante
- Agentes: robôs ou zumbis. Muitas vezes, cúmpices inconscientes pois foram infectados por um código malicioso
- Alvo: vítima do ataque

Proteção

- Uso de softwares específicos
- Uso de técnicas sofisticadas (algoritmos de reconhecimento)
- Configurações gerais da rede e dos dispositivos
- Profissionais responsáveis pela segurança

Proteção

- Muitos ataques tem o foco de atingir algum ponto da rede ou do servidor
- Práticas ruins de programação podem contribuir e facilitar ataques
- Práticas ruins do dia a dia (instalação de softwares infectados)

- **Indiferença/emoção:** geralmente é um ataque sem objetivo
- **Curiosidade:** experimentações
- **Graffiti:** Pintar o nome por notoriedade e/ou desfigurar um site
- **Ponto de apoio:** comprometer sistemas e/ou ocultar rastros
- **Roubo de recursos ou informações:** Coletar elementos

Adivinhando senhas

Falhas consecutivas de login

- Um invasor pode explorar isso no sistema
- Identificar qual é a senha por força bruta
- Ou tentar derrubar o sistema por fazer diversas requisições inválidas

Cuidados

- Limitar o total de erros ao digitar a senha
- Bloquear o IP caso muitos erros sejam identificados

Cavalo de tróia

Executar uma aplicação maliciosa no computador

- E-mails
- Links suspeitos em redes sociais

Cuidados

- Evitar abrir links suspeitos
- Saber o que você está fazendo

- Tráfego de informação sensível (senhas, usuários, documentos)
- Armazenamento de dados sem criptografia
- Apresentação de informações/dados em requisições ou via URL
- Injeção de SQL

- Reduzir ao máximo o tráfego de dados sensíveis
- Evitar armazenar dados que não são necessários
- Evitar ao máximo expor dados/informações do projeto (tabelas e colunas do banco de dados, padrões de requisição, etc...)
- Adicionar camadas de proteção nos diferentes elementos do sistema

- Separar os dados do seu comando SQL
- Conhecer o seu sistema e as técnicas de invasão e de proteção
- https://www.php.net/manual/pt_BR/security.database.sql-injection.php

Referências

Este material é uma síntese e foi produzido com base nos livros

- Aprenda a Desenvolver e Construir Sites Seguros. Erik Schetina - Ken Green - Jacob Carlson. Campus.