escola britânica de artes criativas & tecnologia

Engenheiro de Qualidade de Software

Testes de Segurança

Introdução a Testes de Segurança

Você sabia?

+612%
Tentativas de fraudes digitais em serviços financeiros

+135%
Fraudes na indústria de games

R$ 2.7 bilhões
Estimativa de prejuízo com fraudes financeiras

+223.000.000
Brasileiros com dados vazados (fotos, endereços, documentos e renda)

+1.566%
Pessoas se passando por outras

12:00 às 00:00
Horário com maior incidência de golpes.

Fonte Dados: https://newsroom.transunion.com.br/um-ano-apos-a-pandemia-tentativas-de-fraude-digital-aumentam-no-brasil-segundo-estudos-da-transunionq4/


Motivos de Invasões
CURIOSIDADE & DESAFIO
TRABALHO
CIÚMES
ROUBO & ESPIONAGEM
IDEOLOGIA

Principais tipos de Ataque

- **Cavalo de Tróia:** Malware que opera com "autorização" do usuário.
- **Força Bruta:** Furto de senhas através de diversas tentativas de combinações de usuário e senha.
- **Phishing:** Geralmente aplicado via e-mail, usuários são enganados para revelarem informações sigilosas.
- **DDoS (Distributed Denial of Service):** Ataque de negação de serviços que sobrecarrega as atividades computacionais, provocando lentidão e tornando o sistema sob ataque indisponível.
- **Port Scanning:** Usa malwares que faz em uma busca pelo servidor na tentativa de encontrar alguma vulnerabilidade.
- **Ransomware:** "Sequestrador Virtual" que bloqueia o acesso a todos os dados, liberados mediante pagamento por criptomoeda.
- **Engenharia Social:** Induzir usuários desavisados a compartilhar dados pessoais (utilizados para identificar senhas de acesso), infectar seus computadores com malware ou abrir links para sites infectados.

Testes de Segurança

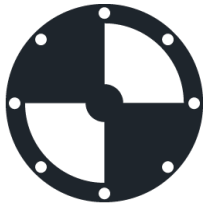
É um tipo de Teste de Software **não funcional**, que busca identificar vulnerabilidades em um sistema para evitar ataques maliciosos de intrusos.

Busca as lacunas e fraquezas possíveis do sistema de software que podem resultar em vazamentos de dados e invasão.

Parte do ciclo de desenvolvimento de um software, especialmente em ambientes ágeis que implementam a cultura DevSecOps

Como se preparar?

Blue Team



Time que aprimora a defesa:

Avalia a segurança de rede e identifica possíveis vulnerabilidades. Seu foco é em detecção de ameaças e resposta de incidentes, ou seja, seu principal objetivo é aplicar estratégias de defesa e manter a segurança dos sistemas e aplicações.

Red Team

Time de ataque:

Tem como função a realização de testes de penetração. Imita ataques do mundo real, fazendo uso de todas as etapas e habilidades que um invasor usaria para, assim, identificar falhas e ameaças à segurança.


Princípios de Testes de Segurança
DISPONIBILIDADE
Garantia de que um serviço ou sistema está funcional e disponível e está fazendo o que se espera.
INTEGRIDADE
Garantia de que os dados ou resultados são consistentes e precisos em todas as plataformas.
AUTENTICAÇÃO
Consiste em confirmar a identidade de uma pessoa / sistema, tentando acessar um recurso protegido em outro sistema.
AUTORIZAÇÃO
É o processo de definir as funções que um cliente* tem permissão para realizar ações em um recurso protegido residente em um servidor.
CONFIDENCIALIDADE
É um processo de segurança que protege os dados do mundo externo por meio de criptografia / hash etc.
NÃO REPÚDIO
Garantia de que uma mensagem transmitida foi enviada e recebida pela pessoa que afirma ter enviado e recebido a mensagem.

Estratégias

VARREDURA DE VULNERABILIDADE

Feito por meio de ferramentas de software automatizadas para varrer um sistema contra vulnerabilidades conhecidas.

VARREDURA DE SEGURANÇA

Identificação de fraquezas da rede e do sistema por meio de ferramentas manuais e automatizadas e fornece soluções para reduzir esses riscos.

TESTE DE PENETRAÇÃO

Análise de um determinado sistema / serviço / aplicativo para verificar possíveis vulnerabilidades por meio da simulação de uma tentativa de hacking.

AVALIAÇÃO DE RISCO

Análise de riscos de segurança e classificação dos mesmos em Baixo, Médio e Alto. Este teste recomenda controles e medidas para reduzir o risco.

AUDITORIA DE SEGURANÇA

Inspeção interna de Aplicativos / Sistemas / Serviços para incidentes de violação de segurança.

HACKER ÉTICO

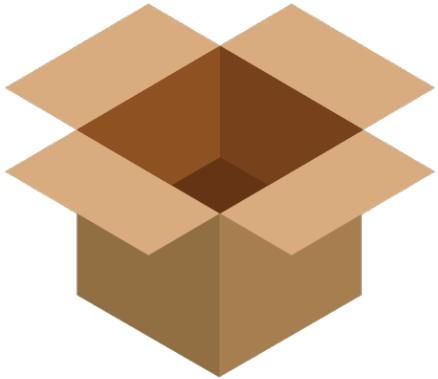
Hackear os sistemas de software de uma empresa com a intenção de expor falhas de segurança no sistema

Tipos de Análise

DAST
Dynamic Application Security Testing

Examina uma aplicação em tempo de execução para encontrar vulnerabilidades que um invasor potencial pode explorar.

SAST
Static Application Security Testing



Examina o código em busca de falhas e pontos fracos de software, como injeção de SQL, XML, JSON, registro e monitoramento insuficientes.

Plano de Testes

- Descrição do seu objetivo e alvos
- Massa de dados de teste utilizados para reproduzir os "ataques"
- Ferramentas de teste necessárias para executar os testes
- Análise dos resultados e criação de caso de testes com o vetor de ataque (passo a passo detalhado para reproduzir como o ataque ocorreu)

Mantenha-se atualizado

- Painel de Incidentes Cibernéticos 2022: https://www.securityreport.com.br/email/InfoSR2022_.html
- Relatório de Brechas Verizon: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/
- Mapa de ataques FortiGuard: https://www.fortiguard.com/threat-research/map
- Mapa de ataques Kaspersky: https://cybermap.kaspersky.com/
- Mapa de ataques Sonic Wall: https://attackmap.sonicwall.com/live-attack-map/

Referências

- https://newsroom.transunion.com.br/um-ano-apos-a-pandemia-tentativas-de-fraude-digitalaumentam-no-brasil-segundo-estudos-da-transunionq4/
- https://www.securityreport.com.br/destaques/cenario-de-ameacas-ciberneticas-e-critico-nobrasil/#.Yi33GhDMIZG
- https://backupgarantido.com.br/blog/tipos-de-ataque-hacker/
- https://blog.konduto.com/pt/2021/07/censo-da-fraude-2021-como-e-o-comportamento-do-fraudadorno-brasil/
- https://g1.globo.com/economia/noticia/2021/06/24/cresce-no-de-consumidores-vitimas-de-fraudesfinanceiras-no-brasil-veja-ranking-das-mais-recorrentes.ghtml
- https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2021/07/06/tentativas-defraudes-digitais-em-servicos-financeiros-crescem-612percent-no-brasil-em-2021.ghtml
- https://medium.com/it-security-best-practices-methodologies-loopholes/security-testing-basicsthat-you-should-know-999f02084dc3

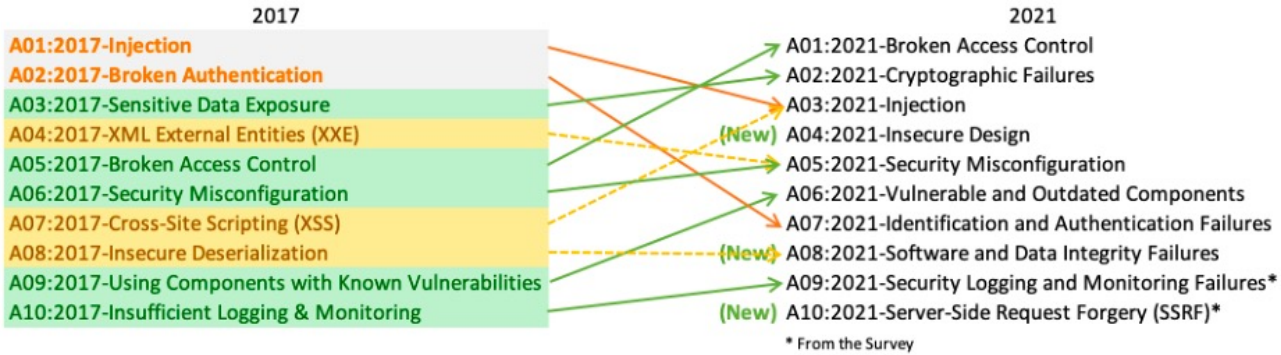
OWASP Top 10

Open Web Application Security Project

Entidade sem fins lucrativos e com reconhecimento internacional que atua com foco na colaboração para o fortalecimento da segurança de softwares em todo o mundo.

OWASP Top 10

- Primeira versão em 2003
- Inicialmente focado nas principais brechas de segurança
- Na ultima versão focada nos principais riscos à segurança



OWASP Top 10 - 2021

A01 - Broken Access Control

A02 - Cryptographic Failures

A03 - Injection

A04 - Insecure Design A05 - Security Misconfiguration

A06 - Vulnerable and Outdated Components

A07 - Identification and Authentication Failures

A08 - Software and Data Integrity Failures

A09 - Security Logging and Monitoring Failures

A10 - Server-side Request Forgery (SSRF)

A01 - Broken Access Control ✦

Quebra de Controle de Acesso

- Quebra de permissões de acesso à informações
- Acesso indevido à informações de outros usuários
- Escalar privilégios para ter acesso à informações de outros usuários

http://meusite.com.br/myInfo?account=ernesto ✓

http://meusite.com.br/myInfo?account=fabio ✗

http://meusite.com.br/admin/appInfo ✗

A02 - Cryptographic Failures

Falhas de Criptografia

- Dados em trânsito e armazenados devem ser protegidos
- Senhas, cartões, informações pessoais, informações sobre saúde e informações corporativas devem ter proteção extra

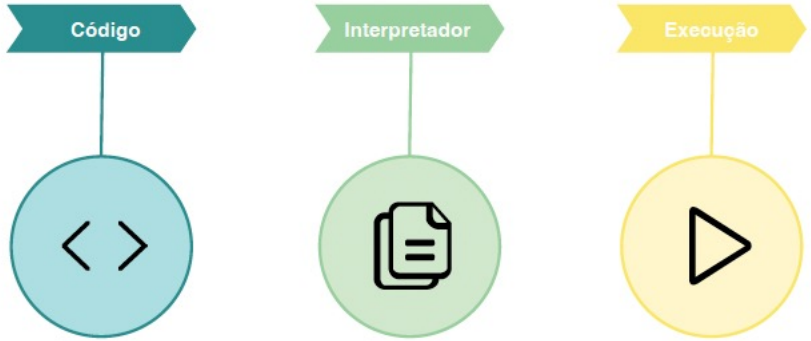
Utilizar criptografia facilmente quebrável para proteger os seus dados sensíveis ✗

Não utilizar criptografia para proteger seus dados sensíveis ✗

Utilizar criptografia reconhecidamente eficiente para proteger os seus dados sensíveis ✓

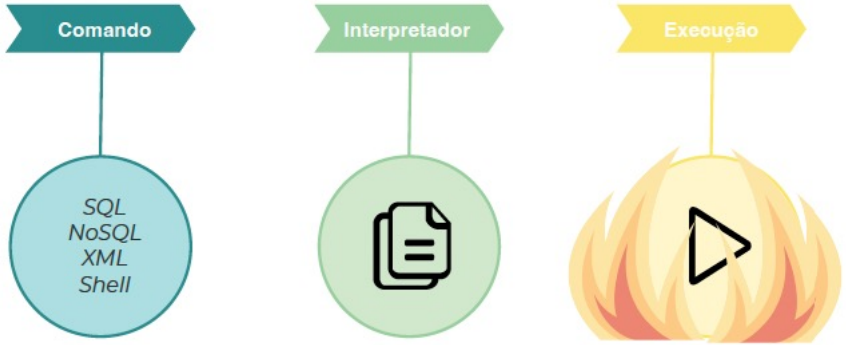
A03 - Injection

Injeção



A03 - Injection

Injeção



A04 – Insecure Design

Design Inseguro

- Riscos ao projetar aplicações e arquiteturas inseguras
- Sem pensar em segurança

Incluir as mensagens de erro que vêm do framework utilizado	✗
Repassar as mensagens de erro técnicas da API ao usuário	✗
Pensar na melhor forma de exibir mensagens de erro para o usuário	✓

A05 – Security Misconfiguration

Configuração Incorreta de Segurança

- Falhas de configuração em ferramentas e ambientes
- Senhas de acesso fracas
- Senhas padrão

Alterar a senha padrão para outra senha conhecida por todos da equipe	✗
Manter as senhas padrão das ferramentas em ambientes de teste	✗
Controle de acesso individual para todas as ferramentas, utilizando regras de senha fortes	✓

A06 – Vulnerable and Outdated Components

Componentes Vulneráveis e Desatualizados

- Uso de ferramentas desatualizadas
- Uso de bibliotecas sem analisar o seu conteúdo e riscos à segurança
- Sistema operacional sem atualizações de segurança
- Vulnerável a ataques de "Dia Zero"

Não avaliar riscos ao utilizar ferramentas ou bibliotecas ✗

Manter todas as suas bibliotecas e ferramentas atualizadas ✓

Manter o Sistema Operacional com todas as atualizações de segurança ✓

A07 – Identification and Authentication Failures

Falhas de Identificação e Autenticação

- Validação e Verificação de Identidade
- Controle de Sessão
- Problemas frequentes em fluxos de recuperação de senha

Utilizar recuperação de senha com perguntas secretas e respostas fixas	✗
Não implementar duplo fator de autenticação (2FA)	✗
Manter sessão do usuário sempre ativa para facilitar o acesso	✗
Verificar se o usuário passou por todas as etapas antes de executar a recuperação de senha	✓

A08 – Identification and Authentication Failures

Falha de Integridade de Software de Dados

- Uso de ferramentas inseguras no processo de Integração Contínua
- Componentes desatualizados
- Sem validações de segurança no processo de integração contínua

Incluir mudanças no software automaticamente em PRD sem validações de segurança ✗

Utilizar ferramentas de segurança e testes automatizados dentro do pipeline ✓

A09 – Security Logging and Monitoring Failures

Falha de Segurança em Logs e Monitoramento

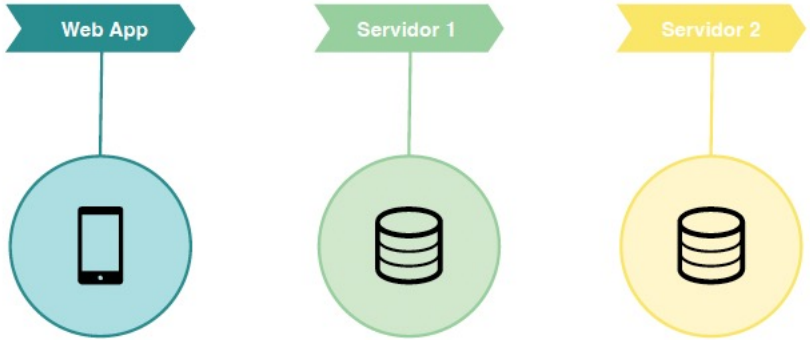
- Sem logs e monitoramento, as brechas não podem ser detectadas
- Ataques avançam em etapas
- Exemplo de passos de um atacante: 1. Rouba seu carro 2. Encontra documentos com o seu endereço 3. Usa o controle do portão para acessar a garagem 4. Na garagem encontra as chaves da casa 5. E assim por diante...
- Se você não possuir um sistema de monitoramento e alerta, nada será detectado e o ataque prosseguirá, indo cada vez mais longe e causando mais estragos.

Logs com identificação dos autores de cada ação (quem baixou um arquivo, tentativas de autenticação, logins de locais inesperados, e assim por diante) ✓

escola britânica de artes criativas & tecnologia

A10 – Server-side Request Forgery (SSRF)

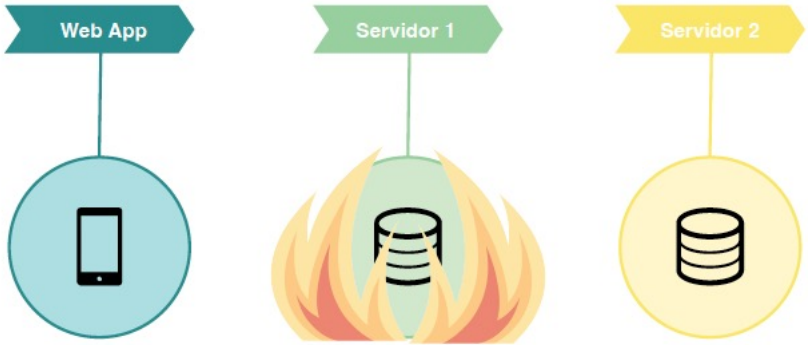
Falsificação de Requisição do lado do Servidor



https://minhalojasegura.com.br/?url=produtos.minhalojasegura.com.br/1002223

A10 – Server-side Request Forgery (SSRF)

Falsificação de Requisição do lado do Servidor



https://minhalojasegura.com.br/?url=file:///etc/passwd

https://minhalojasegura.com.br/?url=arquivomuitogrande.png

Referências

- https://owasp.org/www-project-top-ten/

SQL Injection

Referências

- Repositório: https://github.com/EBAC-QE/ebac-injection-testing

NoSQL Injection

Referências

- Repositório: https://github.com/EBAC-QE/ebac-injection-testing

Command Injection

Referências

- Repositório: https://github.com/EBAC-QE/ebac-injection-testing
- Serviço de emails QA Team - https://qa.team/