



OWASP Top 10



Open Web Application Security Project

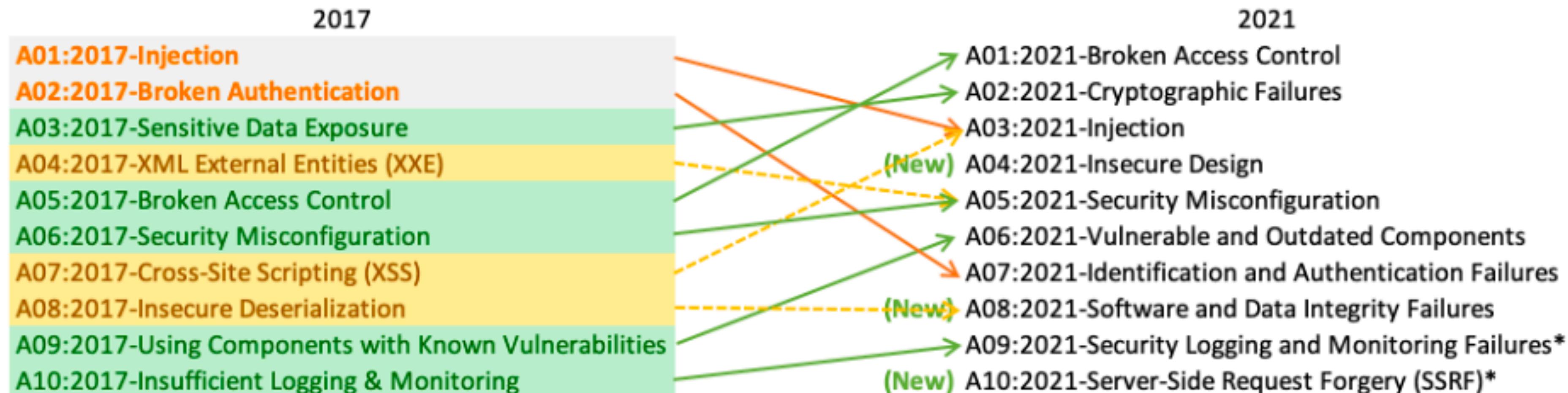


Entidade sem fins lucrativos e com
reconhecimento internacional que atua com foco
na colaboração para o fortalecimento da
segurança de softwares em todo o mundo.



OWASP Top 10

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



* From the Survey

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-  **A06 - Vulnerable and Outdated Components**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

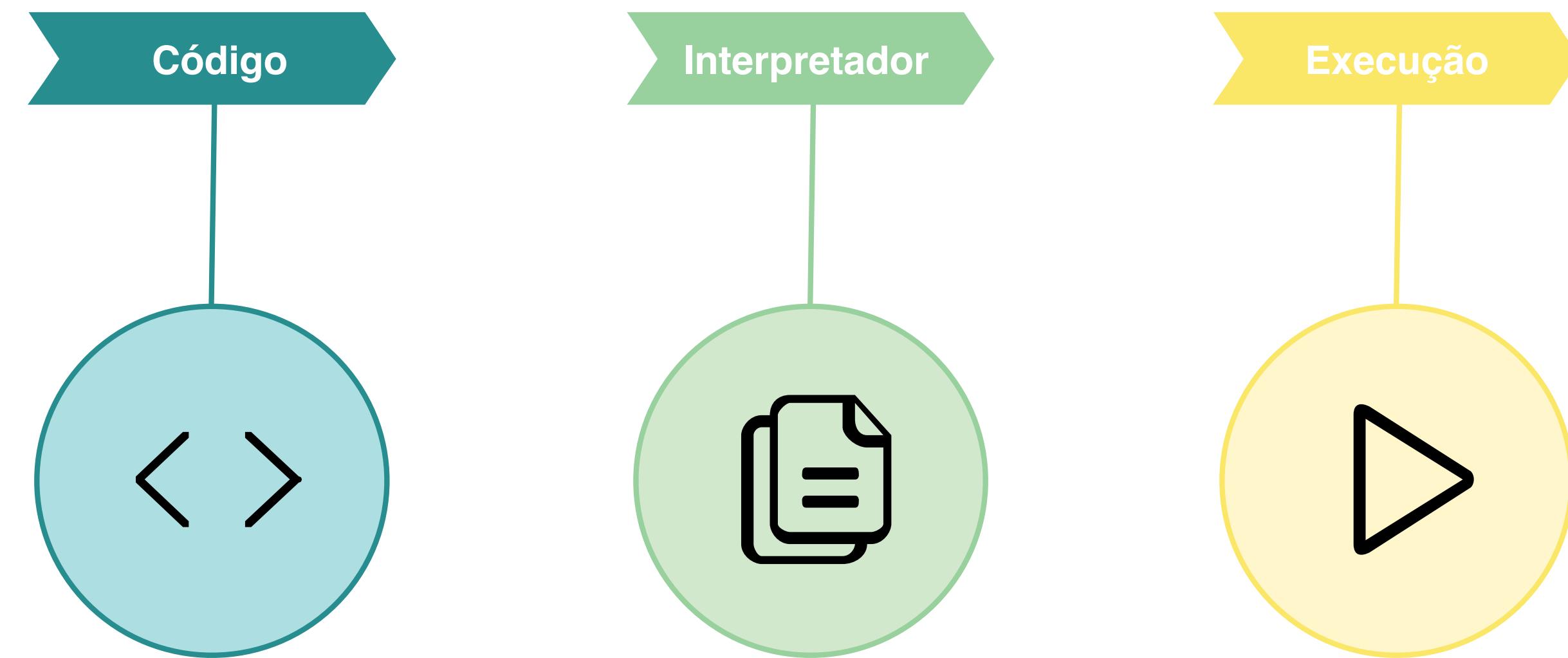


Utilizar criptografia reconhecidamente eficiente para proteger os seus dados sensíveis



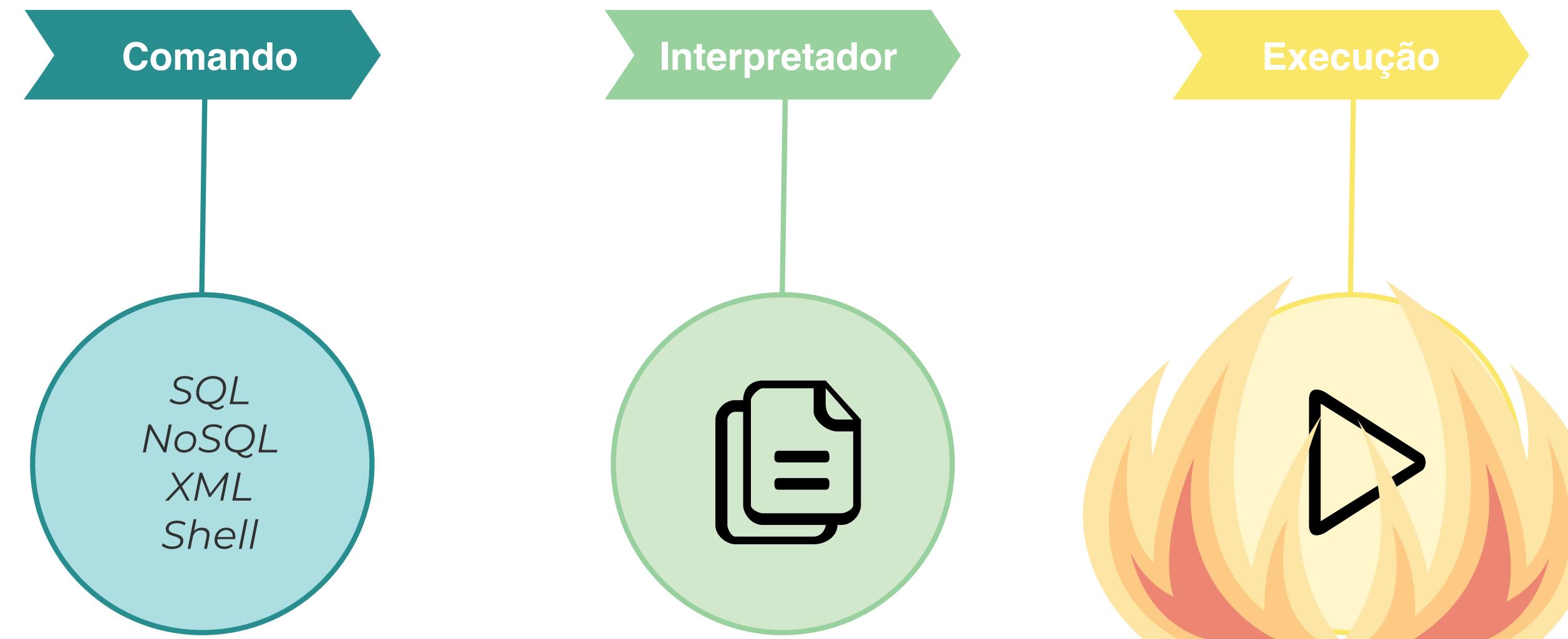
A03 - Injection

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 analizar 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 - Software and Data Integrity 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

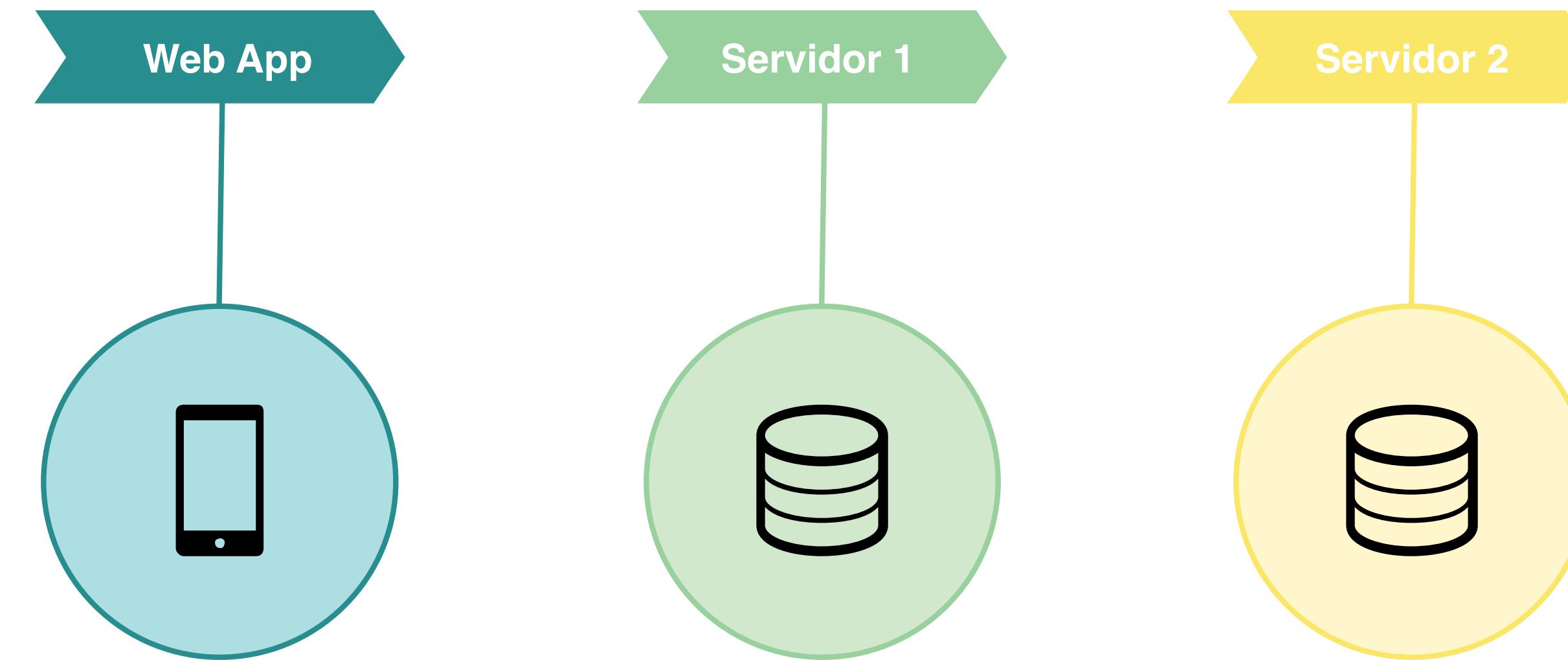
- ◆ Sem logs e monitoramento, as brechas não podem ser detectadas
- ◆ Ataques avançam em etapas
 - ◆ Exemplo de passos de um atacante:
 1. Rouba seu carro
 2. Encontra documentos com o seu endereço
 3. Usa o controle do portão para acessar a garagem
 4. Na garagem encontra as chaves da casa
 5. E assim 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)



A10 - Server-side Request Forgery (SSRF)

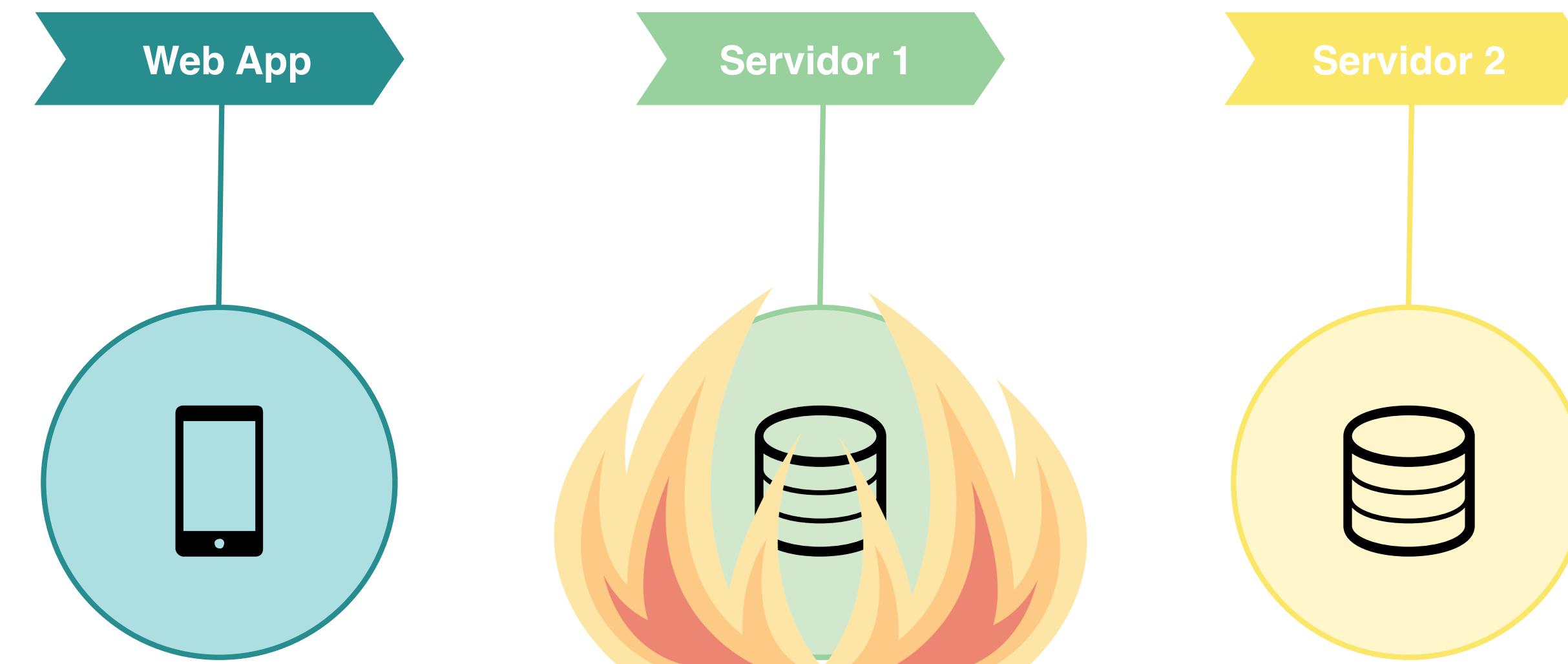
Falsificação de Requisição do lado do Servidor



<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/>





OWASP Top 10

