Conceitos de Segurança em Aplicações

Frameworks de Segurança

Prof. Roberto Padilha

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Segurança em Aplicações

Como funciona o seu ciclo de desenvolvimento de aplicações?

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Mindset para Segurança

- Não pode ser a última etapa
- Não pode ser reativa
- Deve fazer parte da visão de negócio
- Deve ser parte da concepção do software (análise de negócio, UX/UI)
- Deve levar em conta tecnologia e pessoas
- Deve estar enraizada na arquitetura da aplicação
- Deve fazer parte do dia-a-dia dos desenvolvedores
- Deve ser testada e monitorada

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Principais Desafios aos Desenvolvedores

- De acordo com OWASP Top 10 Security Risks *(Open Web Application Security Project)*, 5 dos principais desafios de segurança para os desenvolvedores:

1 | SQL Injection

2 | Falhas no controle de autenticação

3 | Exposição de dados sensíveis

4 | XXE
(XML External Entities)

5 | Falhas no controle de acesso

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Injection (1/2)

- Ocorre quando a aplicação recebe dados inválidos com o intuito de induzir a aplicação a executar algo diferente do que ela foi programada.

```
String query = ”select * from users where user_id = ‘” + usuario + ”’”;
```

- O usuário pode explorar esta estrutura informando, por exemplo:

```
’or’1’=’1
```

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Injection | Prevenção (2/2)

- Utilização de APIs seguras, como frameworks ORM (Hibernate, JPA)
- Validação de input no lado do servidor
- Utilize o nome de colunas em order by, group by, etc
- Separação entre os dados e a lógica da aplicação

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Falhas no Controle de Autenticação (1/2)

- Permite que se obtenha acesso a contas de usuário de um sistema.
- Ocorre devido a problemas de lógica de controle da aplicação, como:
  - Controle impróprio de sessão do usuário, por exemplo
  - Nomes de usuário e senha padrão
  - Páginas de administração padrão (www.site.com/**admin**)

- Pode ocorrer através de:
  - Ataques de força bruta
  - Política imprópria de recuperação de senha
  - Gravação de senhas sem criptografia
  - Exposição de session ID
  - Não invalidação de session ID

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Falhas no Controle de Autenticação | Prevenção (2/2)

- Implementação de *multi-factor authentication*
- Não utilizar senhas padrão em produção
- Implementação de uma política de senhas fortes
- Implementação de uma política constante de alteração e rotatividade de senhas
- Controle de tentativas de login e de limite de acessos à aplicação por IP
- Implementação de controles mais robustos de sessão do usuário através de tokens e critpografia (JWT, OAuth2)

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Exposição de Dados Sensíveis (1/2)

- Ocorre devido à gravação desprotegida de informações sensíveis aos usuários como:
  - Senhas
  - Números de contas
  - Números de cartões de crédito

- Pode ocorrer por causa de:
  - Dados gravados sem criptografia
  - Dados gravados criptografados, mas descriptografados em consultas
  - Não utilização de TLS (https)

Exposição de Dados Sensíveis | Prevenção (2/2)

- Proteção de dados cuja exposição possa causar danos ao negócio ou aos seus usuários
- Aplicar uma política de controle de acesso eficiente, baseada em papéis e responsabilidades
- Utilização de algoritmos de criptografia fortes
  - Evite Base64, MD5
  - Utilizar Bcrypt, Scrypt, PBKDF2, etc.
- Utilização de protocolos de segurança para transporte de dados (TLS)
- Desabilitar cache para conteúdo sensível

Prof. Roberto Padilha
robertocesardasilva@gmail.com

XXE (XML External Entities) (1/2)

- Ocorre em aplicações que aceitam entrada de dados em formato XML
- Alguns frameworks que aceitam JSON também tem suporte automático a XML

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<product>
        <id>123</id>
        <desc>&xxe;</desc>
        <value>233.12</value>
</product>
```

Prof. Roberto Padilha
robertocesardasilva@gmail.com

XXE (XML External Entities) | Prevenção (1/2)

- Utilização de formatos mais limpos como JSON
- Evite serialização de dados sensíveis
- Use verificações de dependências e validadores
- Desabilite processamento de entidades externas e processamento de DTD em parsers de XMl na aplicação
- Utilização de validação por XSD

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Falhas no Controle de Acesso (1/2)

- Ocorre quando um usuário consegue direta ou indiretamente acesso a partes de uma aplicação à qual seu papel não lhe dá direito.

- Pode ocorrer por causa de:
  - Muitos usuários com acesso ilimitado
  - Falta de “níveis” de administrador
  - Falta de validação de nível de acesso em todos os pontos da aplicação (front, back, db)
  - Falta de verificação de parâmetros de requisição
  - URLs padronizadas associadas à falha de validação no backend

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Falhas no Controle de Acesso | Prevenção (1/2)

- Realizar um controle eficiente de papéis
- Criar permissões específicas para as necessidades de cada usuário
- Remover acesso de usuários inativos
- Usar como política base a negação de acesso
- Minimize e controle o uso de CORS
- Desabilite listagem de diretórios na web
- Realize log e controle erros de tentativas de acesso
- Defina tempo de expiração para tokens de acesso

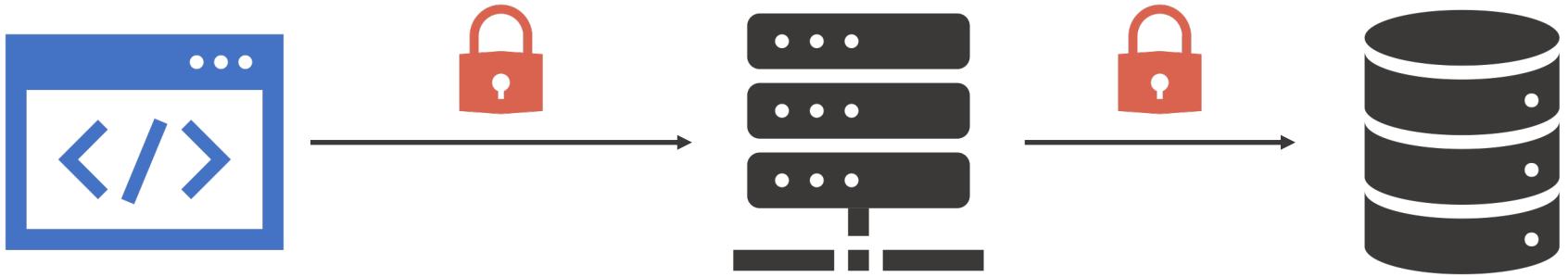
Prof. Roberto Padilha
robertocesardasilva@gmail.com

Impactos na Arquitetura de Aplicação

Qual o papel do desenvolvedor e arquiteto na prevenção destas ameaças?

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Cenários de Aplicação | Monolítico (1/2)



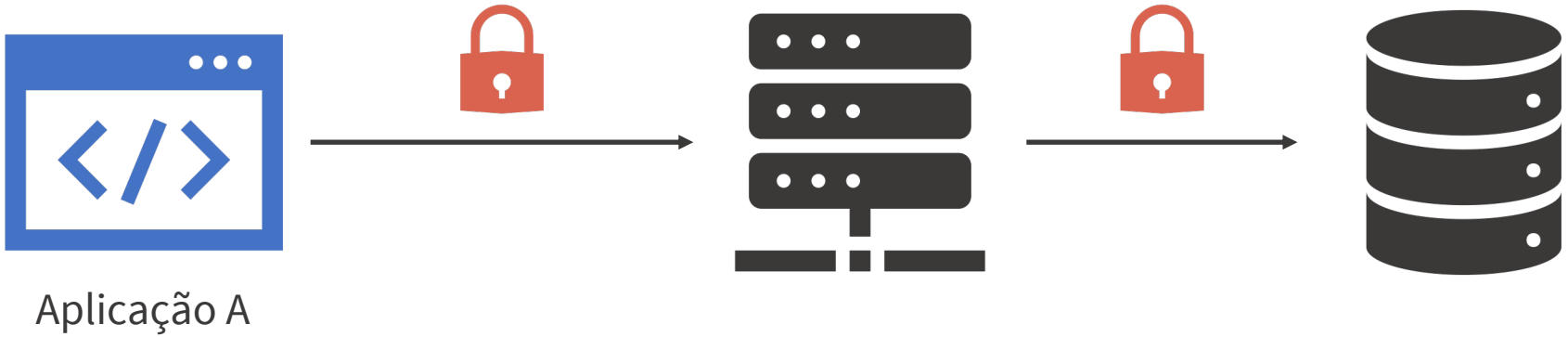
Prof. Roberto Padilha
robertocesardasilva@gmail.com

Cenários de Aplicação | Monolítico (2/2)

- Aplicação coleta credenciais, portanto pode vazá-las.
- Validação de credenciais em banco de dados.
- Implementação manual de todo o processo de acesso e suporte ao usuário
  - Lembrar login
  - Esqueci a senha
  - Confirmação de acesso
  - Bloqueio de acesso

Prof. Roberto Padilha
robertocesardasilva@gmail.com

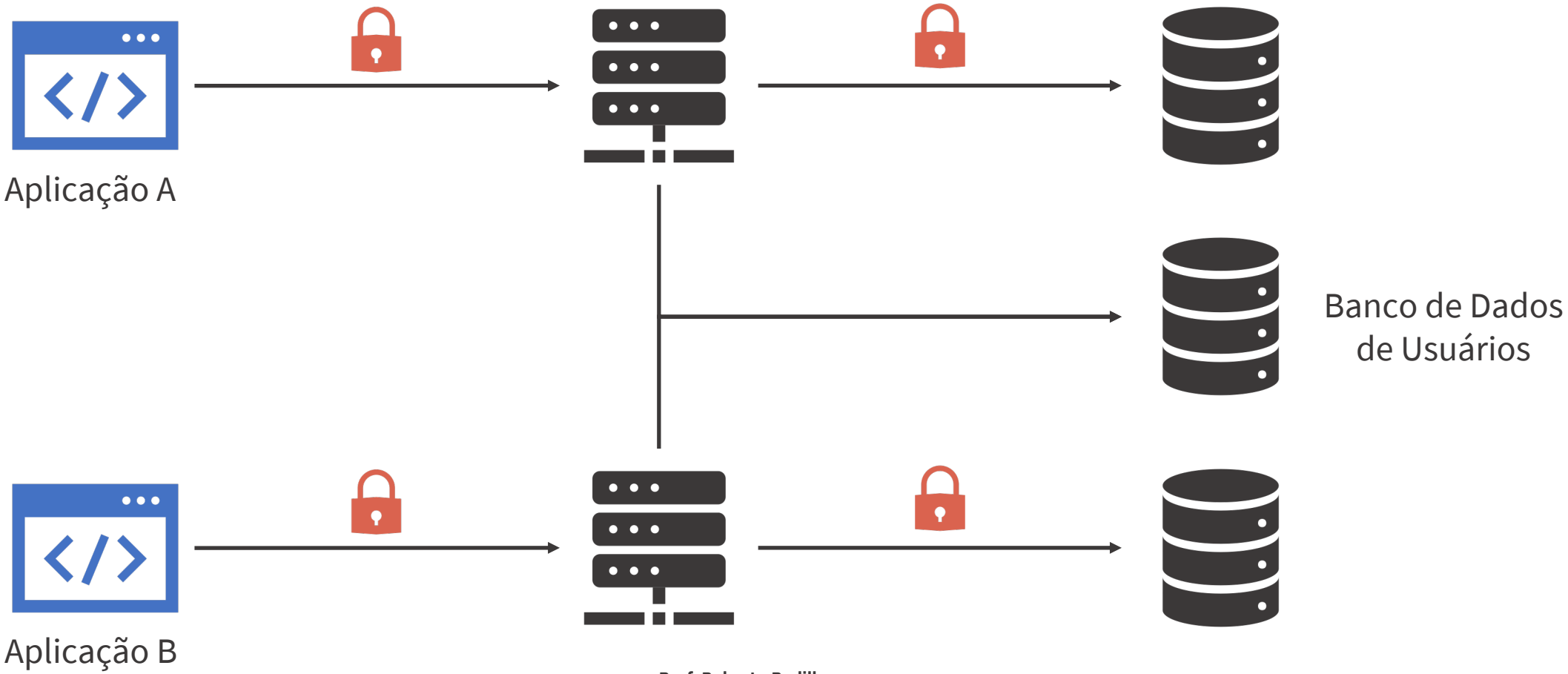
Cenários de Aplicação | Múltiplas Aplicações



Prof. Roberto Padilha
robertocesardasilva@gmail.com

Soluções de Arquitetura | Opção 1 (1/2)

- Centralização das credenciais do usuário:



Prof. Roberto Padilha
robertocesardasilva@gmail.com

Soluções de Arquitetura | Opção 1 (2/2)

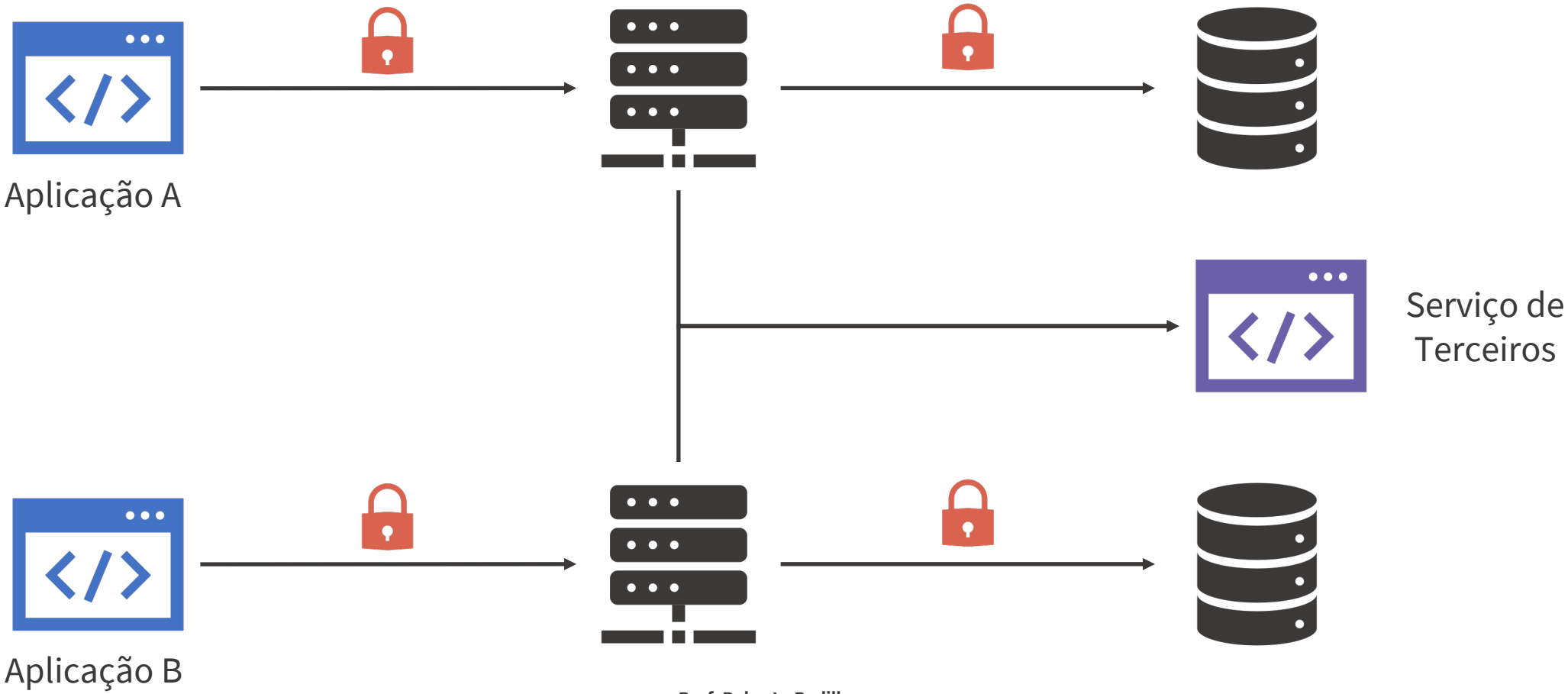
Desafios

- Aumentam as possibilidades de pontos de falha
- Replicação de lógica de acesso
- Controle de usuário e permissões descentralizado
- Replicação de falhas de segurança
- Retrabalho
- Ineficiência
- Grande impacto na implantação / alteração de políticas de segurança

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Soluções de Arquitetura | Opção 2 (1/2)

- Utilização de um serviço de autenticação de terceiros:



Prof. Roberto Padilha
robertocesardasilva@gmail.com

Soluções de Arquitetura | Opção 2 (2/2)

Desafios

- Dificuldade de integração do serviço na regra de negócio
- Armazenamento de dados do usuário no banco de dados da aplicação
- Integração de formatos
- Adequações de arquitetura

Prof. Roberto Padilha
robertocesardasilva@gmail.com

Conceitos de Segurança em Aplicações

Frameworks de Segurança

Prof. Roberto Padilha

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ