

# THE DEVELOPER'S CONFERENCE

## **Trilha: Software Security**

**André Barreto**

Especialista em Segurança Cibernética

# Yellow Team



THE  
DEVELOPER'S  
CONFERENCE

A equipe de segurança

composta por **desenvolvedores**

# Propósito da palestra



THE  
DEVELOPER'S  
CONFERENCE

Mostrar que a segurança não é responsabilidade de apenas uma área, a “área de segurança”.

Ela é responsabilidade de todos!

A segurança deve estar presente em todas as áreas e níveis de uma empresa, deve estar na tecnologia, nos processos e, principalmente, na conscientização das pessoas, que precisam ter um olhar detalhista, analítico, crítico e prudente diante das mais diversas situações do dia a dia.

Vamos ver que os “construtores” dos sistemas são essenciais não apenas para desenvolver soluções e funcionalidades criativas, que irão tornar as empresas competitivas e diferenciadas.

Eles são fundamentais para que o negócio se mantenha seguro, confiável e com credibilidade em um mercado cada vez mais competitivo e exigente.

# Sobre a palestra



- Analisaremos vulnerabilidades que dificilmente são identificadas por “áreas de segurança” tradicionais.
- Veremos como as áreas de desenvolvimento têm papel fundamental para manter a segurança, confiabilidade e credibilidade de um negócio.
- Vamos entender como as áreas de desenvolvimento e áreas de segurança podem interagir e contribuir uma com a outra, trazendo benefícios para ambas, para o negócio e para os clientes.

# História da segurança cibernética



THE  
DEVELOPER'S  
CONFERENCE

No princípio: Redes para comunicação militar

Internet, a rede mundial de computadores

Grandes empresas conectadas, firewalls mantidos por “gurus de conhecimento supremo”

E-commerce

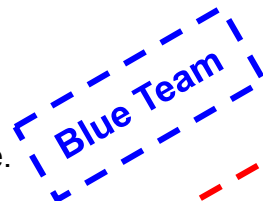
Médias empresas conectadas, mais opções de firewalls mantidos por “seres de conhecimento raro”

WEB 2.0, dinâmica, troca de informações e colaboração

Pequenas empresas e pessoas conectadas.

Firewalls já não eram mais suficientes. Anti-vírus, anti-spam, controle de acesso.

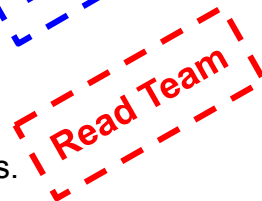
Não bastava um “ser iluminado” para cuidar da segurança, era preciso uma equipe.



Falsificações, fraudes, roubo de informações, exploração de falhas em sistemas.

Já não bastava uma equipe de segurança defensiva (Blue Team).

Era preciso se antecipar, localizar as falhas e corrigi-las antes que fossem exploradas.



## **Pilares da Segurança: 3 bases**

(CID) Confidencialidade, Integridade e Disponibilidade

(PPT) Pessoas, Processos e Tecnologia

# Yellow Team

Quantas pessoas na área de segurança?

- Blue Team
- Red Team

E na área de desenvolvimento?

- Desenvolvedores
- Engenheiros de software
- Arquitetos de sistema e soluções



THE  
DEVELOPER'S  
CONFERENCE





# THE DEVELOPER'S CONFERENCE



## BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics



## RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



## YELLOW TEAM

- Software Builders
- Application Developers
- Software Engineers
- System Architects

# Requisitos vs Vulnerabilidades



THE  
DEVELOPER'S  
CONFERENCE

Se “debug” é o processo de identificar e remover “bugs”, então programar é o processo de inseri-los.

- Requisitos funcionais
- Requisitos não funcionais

- Vulnerabilidades funcionais
- Vulnerabilidades não funcionais

O óbvio precisa ser dito.

O “óbvio” nem sempre é observado e muito menos seguido.



# Vulnerabilidades funcionais (regras de negócio)



THE  
DEVELOPER'S  
CONFERENCE

- Não enviar para o front-end informações que o usuário não tem permissão para ver. Não basta esconder a informação no front;
- Valide o acesso às funcionalidades no backend. Não ter a opção no “menu do front” não basta;
- Valide no backend se o usuário está consultando informações que ele deveria ter acesso. Confiar na identificação do usuário enviado pelo front não basta. O mesmo se aplica a outras identificações;
- Valide no backend se o usuário está usando recursos que pertençam a ele (cupons, moedas);
- Cuidado com “caminhos secundários” que dêem acesso às informações sem as mesmas validações feitas nos “caminhos oficiais”;
- Cuidado com exposições “desnecessárias” da documentação completa dos recursos das suas APIs;
- Você **realmente** precisa saber a senha do usuário?  
Avaliar a necessidade de armazenar e até de transmitir via rede a senha real do usuário, ainda que por meio criptografado.

# Vulnerabilidades não funcionais



THE  
DEVELOPER'S  
CONFERENCE

2011 - Sony (37k)  
2012 - Yahoo (500k)  
2020 - Catho (1,2m)  
2021 - Liker (465k)

- Não armazenar as senhas e chaves de forma aberta;
- Não trafegar credenciais e outros dados sensíveis de forma aberta (header);
- Não fazer integrações que trafegam dados sensíveis de forma aberta;
- Não ignorar erros de certificados em comunicações SSL/TLS
- Aumentar o tempo de retorno para erros de autenticação;
- Definir restrições de palavras de fácil associação e sequências numéricas nas senhas (tdc@123);
- Definir restrições de certas datas nas senhas (tdc@2022);
- Restringir o uso do "username" na senha (andre@2022);
- Aplicar um algoritmo de similaridade com a senha(s) anterior(es) (tdc@2021 -> tdc@2022).

# Vulnerabilidades não funcionais



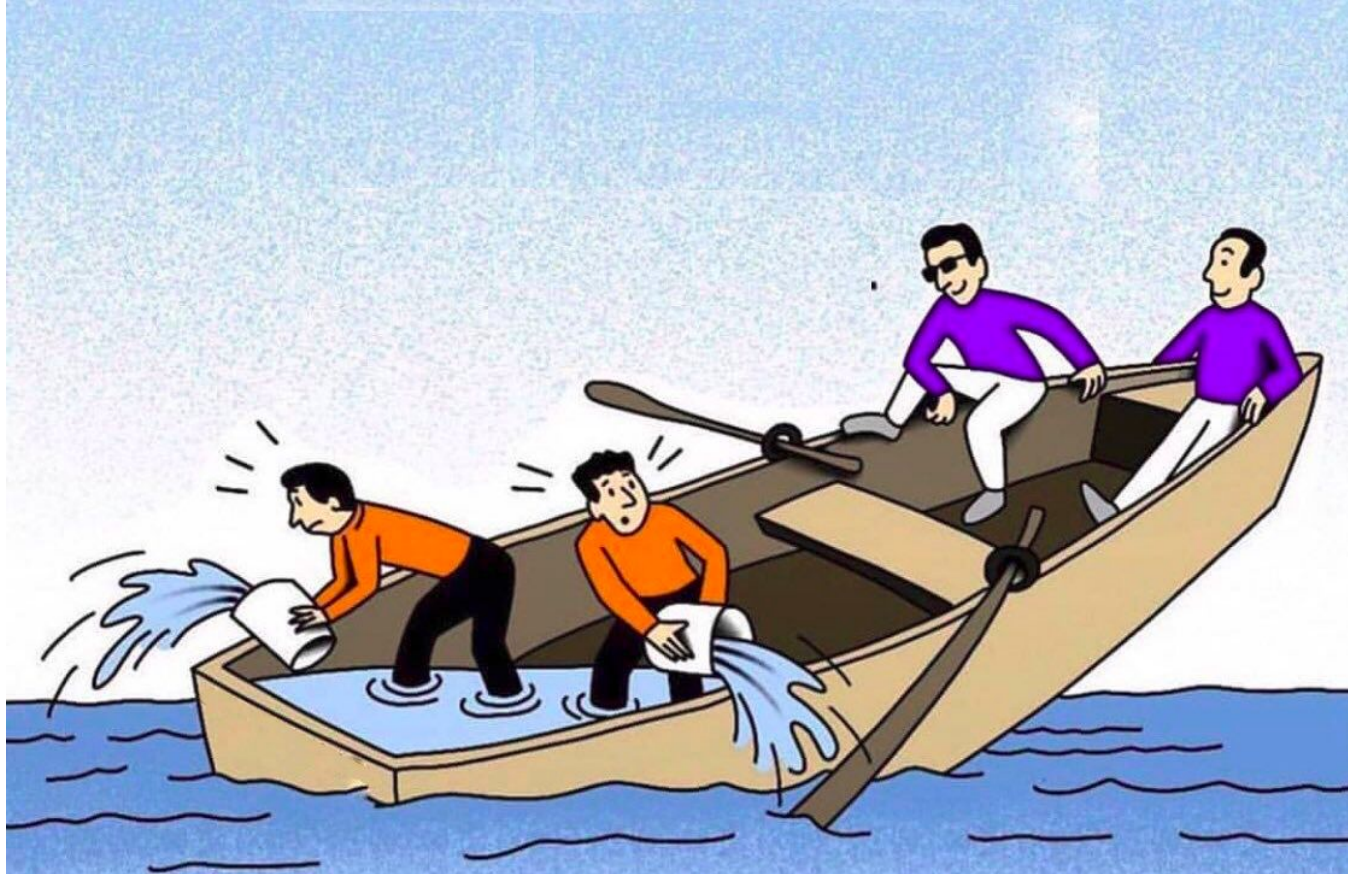
THE  
DEVELOPER'S  
CONFERENCE

- Não dar dicas se “o usuário não existe” ou “a senha está incorreta” (enumeração de usuários);
- Cuidado com mensagens de aviso para o usuário durante a autenticação (“usuário bloqueado”, “senha expirada”, etc).  
Se for necessário informar algo, faça somente após validação com sucesso das credenciais;
- Avaliar a possibilidade de associar um “token ao usuário” ao invés de um “usuário ao token”.  
(Reduz sessão "esquecidas" e, principalmente, evita compartilhamento de credenciais);
- Avaliar o famoso bloqueio do usuário após X tentativas de login incorretas (DoS).

# Equipe de segurança (somente Blue e Red)



THE  
DEVELOPER'S  
CONFERENCE



- Dinamismo do mercado
- Concorrência
- Regulamentações
- Regras de negócio
- Crises
- Quebra de barreiras geográficas

Não basta os 15m<sup>2</sup> do barco "seguros", aquela brecha de 1cm<sup>2</sup> pode nos fazer afundar.

# Segurança



THE  
DEVELOPER'S  
CONFERENCE



# The InfoSec colour wheel

blending **developers** with **red** and **blue** security teams



Red, Blue and Yellow are our Primary Colours.  
Combine two of them and you get Secondary Colours.



## THE DEVELOPER'S CONFERENCE

Cores primárias:

- Blue
- Red
- Yellow

Cores secundárias:

- Purple
- Green
- Orange



# Exemplos de integração entre times



THE  
DEVELOPER'S  
CONFERENCE

- Aumentar o tempo de retorno para erros de autenticação (força bruta); ●
- Não apresentar comportamento diferente quando apenas a senha estiver errada e quando o usuário não existir (enumeração de usuários); ●
- Se existir uma opção de “Esqueci minha senha”, não apresentar comportamento diferente quando o usuário não existir (enumeração de usuários); ●
- Ajustar códigos de retorno HTTP.  
Isso pode ser trabalhado junto ao Blue Team em sistemas de análise de acessos:
  - 400 - Identificar requisições com erros estruturais (bad request); ●
  - 401 - Usar nas falhas de autenticação; ●
  - 403 - Usar quando se tenta acessar um recurso ao qual não se tem permissão; ●
  - 404 - Se possível não usar dentro da aplicação, avaliar o uso do 204. Blue Team pode usar o 404 para localizar tentativas de enumeração de arquivos e diretórios. ●
- Se retornar 200 na falha de autenticação, então possuir diversas mensagens de erro de login, com diferentes frequências, tendo algumas com percentual bem baixo (enumeração de usuários). ●



# Segurança de perímetro sem um Yellow team



THE  
DEVELOPER'S  
CONFERENCE



## Um forte portão de entrada

- Firewall NGFW
- IDS/IPS
- WAF
- SIEM
- Sistema de segurança com AI



# Mensagens finais



THE  
DEVELOPER'S  
CONFERENCE



# Mensagens finais



THE  
DEVELOPER'S  
CONFERENCE

“Se quisermos sobreviver nessa nova era digital, onde os crimes são cibernéticos, precisamos aprender a lidar com as novas “trancas” e “cadeados” que a evolução tecnológica nos exige.”

André Barreto

# Mensagens finais



THE  
DEVELOPER'S  
CONFERENCE

“Está em cada um de nós a capacidade e a responsabilidade de proteger não apenas uma empresa, mas de proteger a cada pessoa que usa, depende e confia em nossos sistemas e em nosso trabalho.”

André Barreto

# We are the YELLOW TEAM!



THE  
DEVELOPER'S  
CONFERENCE

