THE DEVELOPER'S CONFERENCE

Trilha – Software Security

Patrícia Magrin Leonardelli
Especialista de Segurança da Informação

THE DEVELOPER'S CONFERENCE

O papel de segurança da informação no processo de desenvolvimento de software

Patrícia Magrin Leonardelli
Novembro/2019

Dia a dia das equipes de desenvolvimento

THE DEVELOPER'S CONFERENCE

- Desenvolver softwares:
  - Estáveis;
  - Interface amigável;
  - Processamento escalável e rápido;
  - Intuitivos;
  - Dentre outros requisitos.
    - E além disso, entregar no menor tempo possível!

THE DEVELOPER'S CONFERENCE

No meio de tudo isso, vem aquele pessoal da segurança da informação.

THE DEVELOPER'S CONFERENCE

- Com o discurso que precisa incluir no processo:
  - Desenvolvimento seguro
  - Análise de vulnerabilidade
  - Análise de código
  - Autenticação em múltiplo fato
    - E por aí vai....

E no dia a dia ...

THE DEVELOPER'S CONFERENCE

- É necessário reduzir o tempo de novas versões e funcionalidades.
- Agilizar o desenvolvimento.
- Aumentar a estabilidade.

- Implantar um processo de auditoria do código e outras rotinas de segurança se torna bem difícil.
- Precisamos ser ágeis.

Além disso...

THE DEVELOPER'S CONFERENCE

- Implantar segurança no processo de desenvolvimento de software tem um custo:
  - Problemas com performance
  - Qualidade
  - Atraso na entrega
  - Dentre outros...

THE DEVELOPER'S CONFERENCE

E como resolver?

THE DEVELOPER'S CONFERENCE

- Implantar um ciclo de desenvolvimento de software seguro.
- Melhores práticas de segurança devem ser aplicadas em todo o ciclo de desenvolvimento.
- Não deixar a segurança para o final.

Automatizar rotinas para identificar vulnerabilidades

THE DEVELOPER'S CONFERENCE

CWE/SANS Top 25 Most Dangerous Software Errors

Brief Listing of the Top 25

This is a brief listing of the Top 25 items, using the general ranking.

NOTE: 16 other weaknesses were considered for inclusion in the Top 25, but their general scores were not high enough. They are listed in a separate "On the Cusp" page.

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66.0	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function

https://www.sans.org/top25-software-errors/#cat2

Implantar melhores práticas para correção de vulnerabilidades conhecidas

THE DEVELOPER'S CONFERENCE

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 - Injeção de Código	→	A1 - Injeção de Código
A2 - Quebra de Autenticação e Gerenciamento de Sessão	→	A2 - Quebra de Autenticação
A3 - Cross-Site Scripting (XSS)	↘	A3 - Exposição de Dados Sensíveis
A4 - referência Insegura e Direta a Objetos [Agrupada + A7]	U	A4 - Entidades Externas XML (XXL) [Nova]
A5 - Configuração Incorreta de Segurança	↘	A5 - Controle de Acesso Ineficiente [Agrupada]
A6 - Exposição de Dados Sensíveis	↗	A6 - Má Configuração de Segurança
A7 - Falta de Função para Controle do Nível de Acesso [Agrupada + A4]	U	A7 - Cross-Site Scripting (XSS)
A8 - Cross-Site Request Forgery (CSRF)	X	A8 - Desserialização Insegura [Nova]
A9 - Usar Componentes com Vulnerabilidades Conhecidas	→	A9 - Usar Componentes com Vulnerabilidades Conhecidas
A10 - Redirecionamentos e Encaminhamentos Inválidos	X	A10 - Registro e Monitoração Ineficientes [Nova]

https://www.owasp.org/index.php/Main_Page

Equipes de desenvolvimento

THE DEVELOPER'S CONFERENCE

- Capacitar as equipes para o desenvolvimento seguro de software.
- Efetuar regularmente atividades de revisão estática e dinâmica de código (Code Review).

Colaboração

THE DEVELOPER'S CONFERENCE

- Colaboração entre as áreas desde o início do projeto.
- É possível desenvolver soluções **mais seguras** a partir da troca de experiências entre os membros das equipes.

Monitoramento constante

THE DEVELOPER'S CONFERENCE

- Monitoramento contínuo assegura que potenciais violações ou problemas de segurança sejam notificados rapidamente, bem como isolados, desligados, prevenidos e corrigidos antes que aconteçam ou que sejam explorados.

THE DEVELOPER'S CONFERENCE

O que precisamos ter em mente?

- Ameaças e vulnerabilidades surgem todos os dias.
- Precisamos de colaboração e integração entre as equipes.
- Segurança da informação e equipes de desenvolvimento trabalhando juntas em prol do negócio.

Resumindo

THE DEVELOPER'S CONFERENCE

- Seguir boas práticas e frameworks de segurança.
- Monitorar e corrigir vulnerabilidades.
- Colaboração e integração entre as equipes.
- Capacitar equipes.

THE DEVELOPER'S CONFERENCE

Obrigada!

Contato:

Linkedin: Patrícia Magrin Leonardelli

E-mail: pati.leonardelli@gmail.com

THE DEVELOPER'S CONFERENCE