Desenvolvimento Orientado por Testes (Test Driven Development)

É uma prática de desenvolvimento de software onde a codificação das funcionalidades começa a partir da escrita de testes unitários. Essa técnica foi criada por Kent Beck e é um dos pilares do XP (Extreme Programming).

O TDD consiste em um ciclo apelidado de Red, Green, Refactor.

1.RED - Fazer um teste para uma funcionalidade a qual queremos implementar.Ao executar esse teste ele deve falhar, pois ainda não temos a implementação.

2.GREEN - Depois que o nosso teste falhar resolvemos o que tem de ser resolvido no código.

3.REFACTOR - Analisar o código e procurar pontos a melhorar e aplicar boas práticas de programação eliminando redundâncias.

Os principais benefícios do TDD são -
Maior cobertura de testes unitários;
Testes são executados com maior frequência;
O código se torna mais limpo;

Exemplo:.

1. Criamos um sistema de CRUD de salgados onde consiste em adicionar um novo salgado, editar um salgado existente, deletar um salgado existente e mostrar o salgada no seu catálogo, dentro do nosso sistema.
2. Fazemos um teste unitário, onde o escopo é somente o pequeno sistema de cadastros de salgados, o teste é focado em fazer dar errado por exemplo cadastrar um salgado sem nome.
3. O teste tendo reportado um erro você reformula o seu código com base no seu teste anterior.
4. Por fim você analisar o código e procurar pontos a melhorar e aplicar boas práticas de programação eliminando redundâncias e melhorando o desempenho do sistema!

WannaCry ransomware 2017

WannaCry afetou o sistema operativo Microsoft Windows desatualizado. A sua difusão em larga escala iniciou-se em 2017 infectando mais de 230 mil sistemas, dentre operadoras de telecomunicações, empresas de transportes, organizações governamentais, bancos e universidades.

Para isso, ele criptografa arquivos importantes e impede que você os leia ou bloqueia o seu acesso ao computador para que você não consiga usá-lo.

A divulgação de exploits pelo grupo The Shadow Brokers a 14 de abril de 2017 levou ao lançamento de uma correção crítica pela Microsoft em maio de 2017. O ataque do ransomware WannaCry havia se espalhado através de uma campanha de phishing (uma campanha de phishing é quando os e-mails de spam com links ou anexos infectados servem de isca para os usuários fazerem download de malwares). No entanto, o EternalBlue foi o exploit que permitiu que o WannaCry se propagasse e se disseminasse, e o DoublePulsar foi o backdoor instalado nos computadores comprometidos (usado para executar o WannaCry).