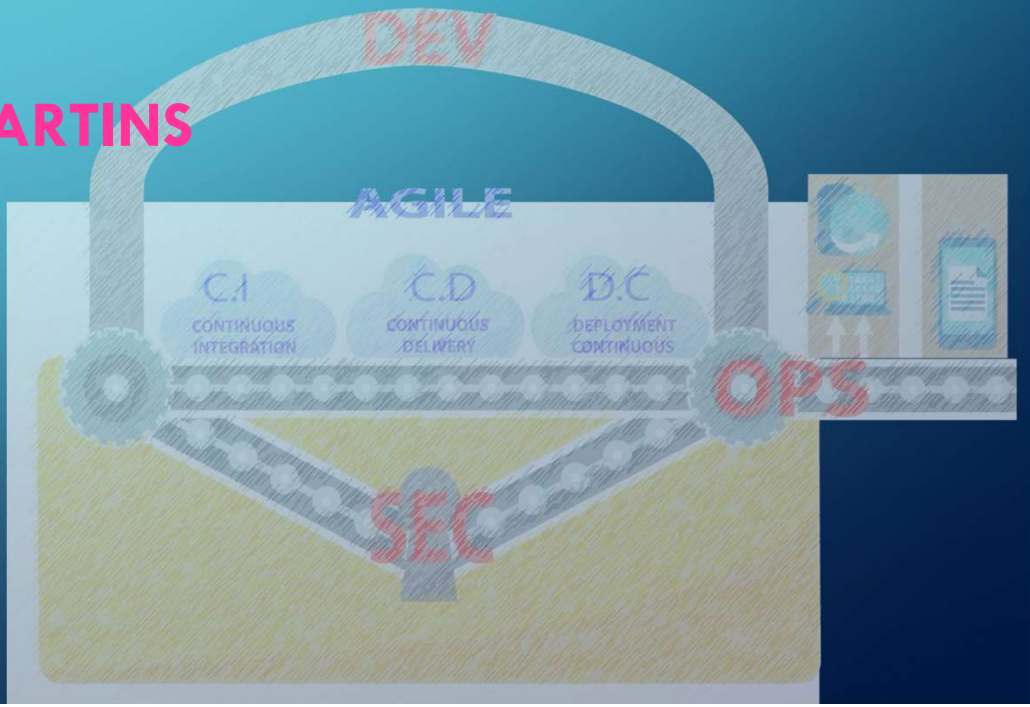
TESTES DE SEGURANÇA NO CICLO DE VIDA DE DESENVOLVIMENTO DE SOFTWARE: PLANEJANDO, CRIANDO E EXECUTANDO TESTES DE SEGURANÇA UTILIZANDO KALI LINUX

FACILITADORA: ALESSANDRA MARTINS



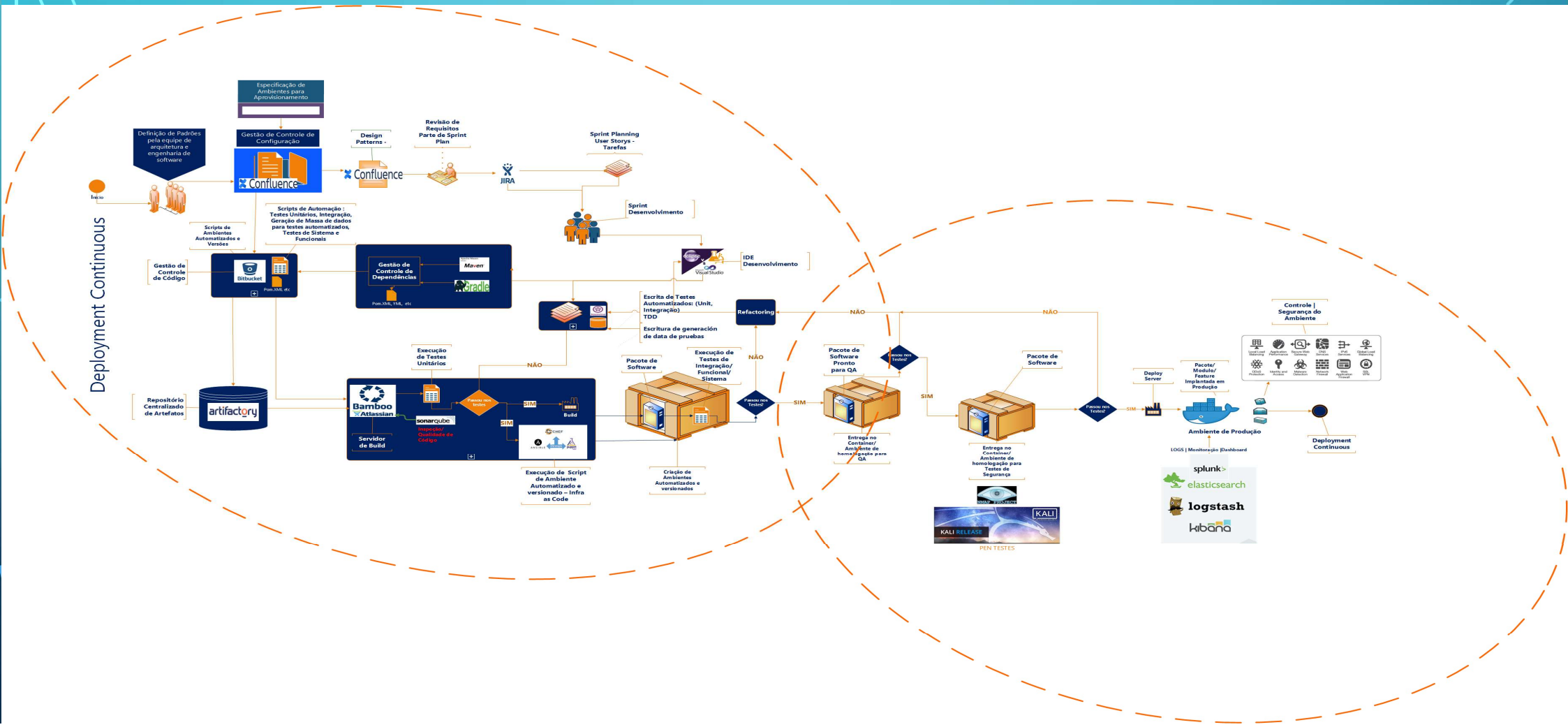
Femme it
O JEITO FEMININO DE FALAR DE TI

AGENDA:


Como Planejar os Testes de Segurança?
Por Onde Começar?
O Que Descrever?
Quais Ferramentas ?
Como Documentar ?
Executando e Guardando Evidências
Referências

COMO PLANEJAR?

UMA ABORDAGEM: DEVSECOPS
APROXIMAÇÃO ENTRE TESTES E SEGURANÇA



COMO PLANEJAR?

UMA VISÃO: QUALIDADE DE SOFTWARE ALINHADA A SEGURANÇA

Pilares da Segurança da Informação

Integridade - ausência de alterações não autorizadas a um sistema, a uma ou mais informações;

Disponibilidade - a informação é acessível por usuários autorizados sempre que a solicitarem, está disponível;

Confidencialidade – diz respeito à ausência de divulgação não autorizada de informação, somente usuários autorizados podem visualizar uma informação;

Autenticidade - que diz respeito à origem do sistema ou informação fornecido, se são ou não genuínos.

Princípios de Teste e Qualidade de Software

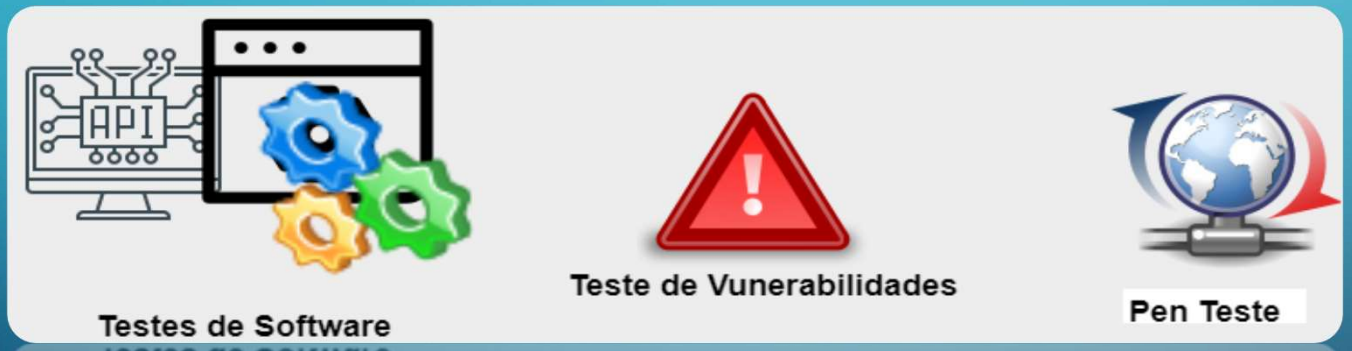
1. Teste Demonstra a Presença de Defeitos
2. Teste Exaustivo é impossível
3. Testes dependem do contexto
4. A ilusão da ausência de erros
5. Teste Antecipado
6. Agrupamento de defeitos
7. Paradoxo do Pesticida

COMO PLANEJAR?

CONTEXTO: INSERINDO TESTES DE SEGURANÇA NO CICLO DE VIDA DE DESENVOLVIMENTO DE UMA APLICAÇÃO

A parte mais visível do teste é a execução

O Teste de Segurança tem como meta garantir que o funcionamento da aplicação se comporta adequadamente mediante as mais diversas tentativas ilegais de acesso, visando possíveis vulnerabilidades. Para isso, testa se todos os mecanismos de proteção embutidos na aplicação de fato a protegerão de acessos indevidos.



POR ONDE COMEÇAR ?

O PAPEL DO QA E ALGUMAS COISAS MAIS

QA não é Analista de SegurançaMas pode ser Capacitado

- Arquitetura de Teste –
- Framework e Ferramentas
- Automação de Testes com Scripts
- Execução de Casos e Cenários de Testes Automatizados e Manuais

Perfil/ Papel do QA:

Cenários de Teste – US- Comportamento e Workflow

Análise de Protótipos

Teste Manual

Revisão de Requisitos

Teste Exploratório

Casos de Teste

POR ONDE COMEÇAR ?

PRÁTICAS & PROCESSOS ENVOLVIDOS

Dimensões de Teste: Confiança, Funcionalidade e Performance;

Processos de Teste:

Verificação: Nós Construímos Corretamente o Sistema?

Validação: Nós Construímos o Sistema Correto?

Processo de Segurança:

Nós Construímos o sistema pensando na Segurança?

Nós validamos a segurança construída para o sistema?

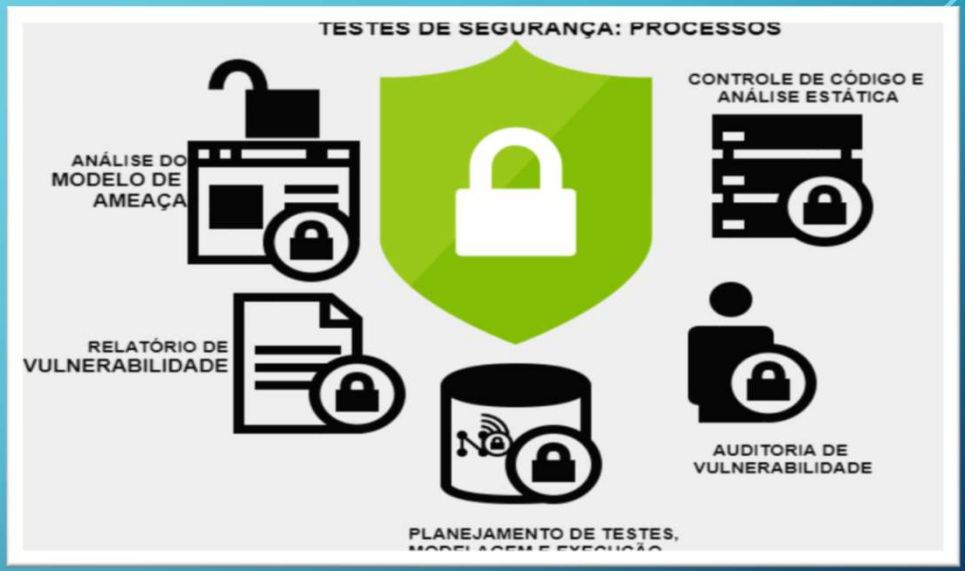
POR ONDE COMEÇAR ?

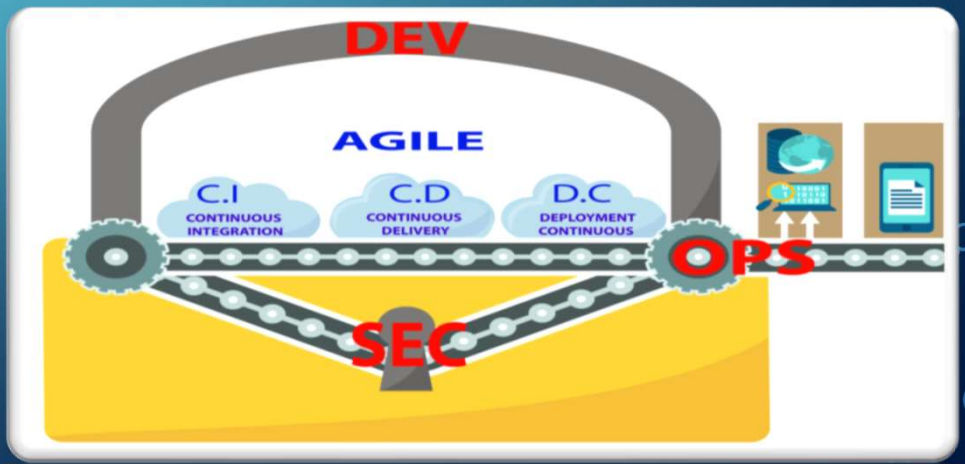
PRÁTICAS & PROCESSOS ENVOLVIDOS

A validação de segurança pode ser realizada em duas fases:

Estática - tenta localizar falhas inseridas durante o desenvolvimento do projeto, como um estado não-alcançável ou possíveis erros humanos introduzidos no código. Nesse caso são utilizados métodos de análise estática (ex.: inspeção de código, analisadores de vulnerabilidade estáticos), ou prova de teorema, os quais não necessitam executar o sistema.

Dinâmica - se foca na verificação da implementação durante sua execução, verificar o sistema exercitando seu código, onde entradas reais são fornecidas para verificar os mecanismos de segurança.

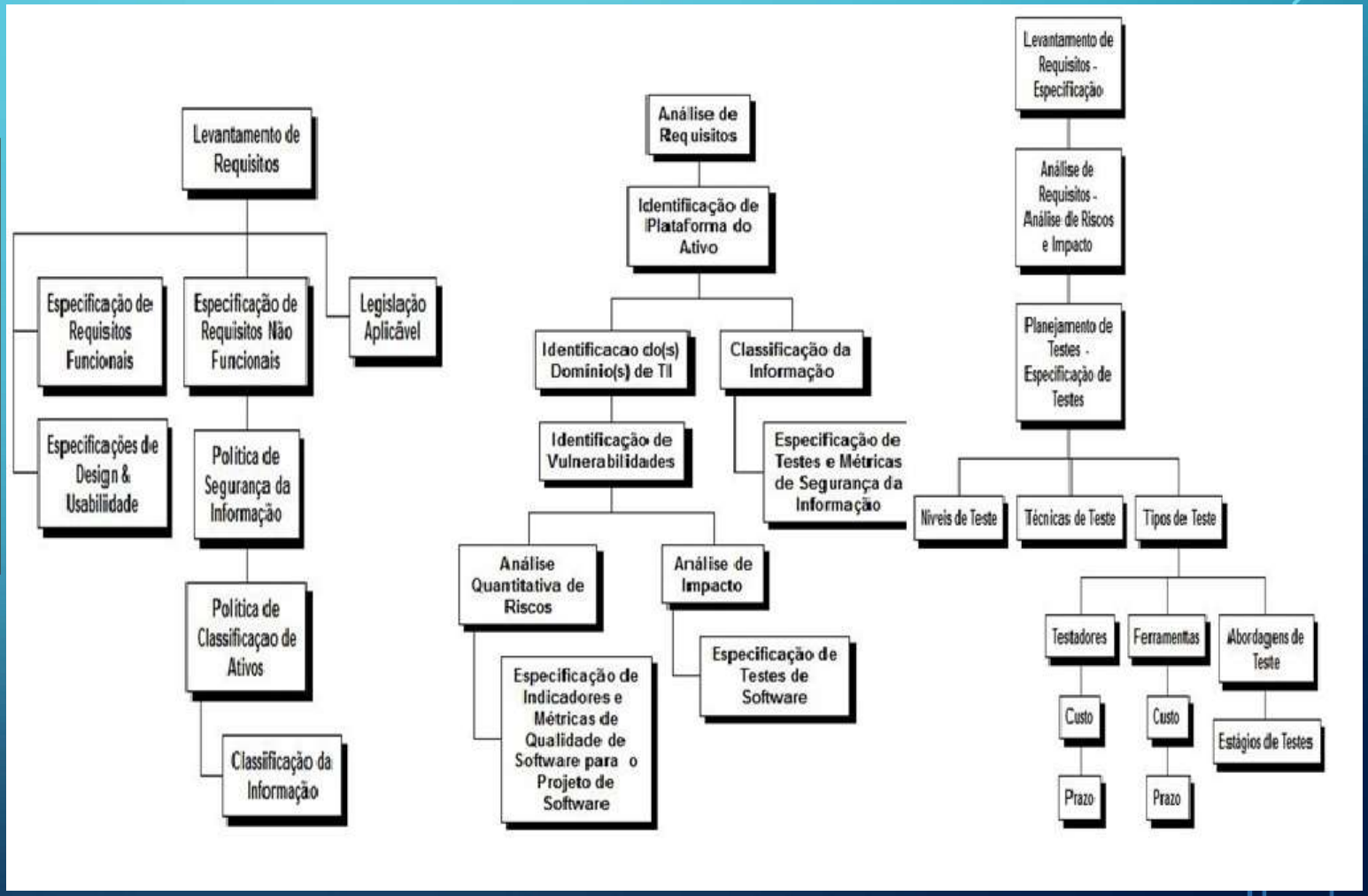




POR ONDE COMEÇAR ?

PRÁTICAS & PROCESSOS ENVOLVIDOS

	Processo de Modelagem de Ameaças
1	Identificar Ativos valiosos que devem ser protegidos
2	Criar uma visão geral da Arquitetura
3	Decompor a Arquitetura da Aplicação para criar camadas e perfis segurança
4	Identificar Ameaças
5	Documentar Ameaças
6	Classificar Ameaças



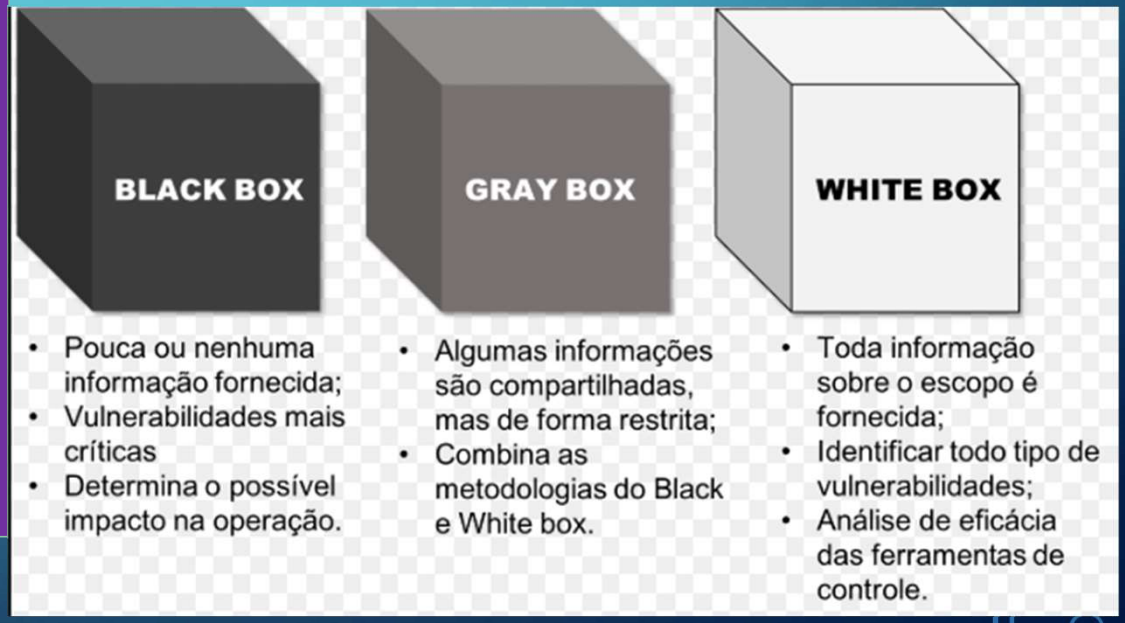
POR ONDE COMEÇAR ?

HABILIDADES E OUTROS ENVOLVIDOS

Fuzzy -> Técnica para Injeção de falhasEscalável funciona com qualquer linguagemVersátil Host ou Rede

Especialista/ Analista de Segurança da Informação

- Capacidade Técnica - uso de Ferramentas;
- Conhecimentos de Segurança para Testar o Software;
- Análise de Vulnerabilidades;
- Modelagem de Cenários e Ameaças para Testes;
- Conhecimentos de Auditoria,
- Monitoria



O QUE DESCREVER?

Plano de Testes, Casos/ Cenários de Testes/ Scripts de Testes/ Relatórios de Testes

Mapeamento da Aplicação - Projeto Exemplo

Cookies (Quebra de Autenticação; CSRF)	Campos de Upload (Injeção; XSS)	Campos de Pesquisa (Injeção, Configuração Incorreta de Segurança - Autocomplete)	Campos de Texto (XSS, Injeção-Fuzz; Configuração Incorreta de Segurança - Autocomplete)	Parâmetros na URL (Referência Insegura; CSRF)	URL para fora do domínio (Redirecionamento e Encaminhamento Inválido; CSRF)	Login (Configuração Incorreta de Segurança; Quebra de Autenticação; Falta de Função para Controle do Nível de Acesso)	Url (Configuração Incorreta de Segurança; Falta de Função para Controle do Nível de Acesso; Referência Insegura e Direta a Objetos)	Usuário Autenticado (Exposição de Dados Sensíveis)	Validar Componente
									X

O QUE DESCREVER?

Análise ou Pentest?

Análise de Vulnerabilidades

Indica possíveis vulnerabilidades em sua rede, sem necessariamente explorá-las. Muitas avaliações usam uma ferramenta de scan para identificar possíveis brechas em sistemas e políticas de segurança. Então, a ferramenta classifica por nível de impacto as vulnerabilidades encontradas em seu ambiente.

Pentest

Consiste em uma avaliação mais extensiva, mais recomendada para organizações que já possuem uma postura de segurança madura. O objetivo do teste de penetração é identificar exploits dentro da rede ou aplicativos que tentam obter acesso a dados sensíveis. Com o pentest, também é possível mostrar o impacto financeiro de possíveis exploits em seu ambiente.

O QUE DESCREVER?

Matriz de Rastreabilidade

Ameaças	Técnicas	Objetivos de Teste	Status	Observação
INJEÇÃO	Malicious File Execution	Em campos de Upload, verifique se a aplicação aceita arquivos não permitidos. Ex: XML, html e etc.	Não Executado	
	SQL Injection - Manual	Em campos de Pesquisa, execute testes manuais de SQL Injection.	Não Executado	
	SQL Injection - Automatizado	Execute a ferramenta SQL Inject Me na aplicação.	Não Executado	
		Execute a ferramenta de pentest SQL Map na aplicação.	Não Executado	
	Fuzz Automatizado	Execute a ferramenta de pentest Owasp Zap (no modo Fuzz Categories e Buffer Overflows and Format String Errors) na aplicação.	Não Executado	
	Fuzz Manual	Em campos de Texto e Pesquisa, execute testes manuais fuzzing na aplicação.	Não Executado	
QUEBRA DE AUTENTICAÇÃO E GERENCIAMENTO DE SESSÃO	Bypass vertical acess	Usuários de privilégios diferentes, verifique se os usuários podem acessar dados para os quais o seu tipo de usuário tem permissão. (Acesso	Não Executado	
	Bypass horizontal acess	Usuários de privilégios diferentes, verifique se os usuários podem acessar modificar dados para os quais o seu tipo de usuário tem permissão.	Não Executado	
	Password reset	Tela de login, verifique se o número de tentativas de login na aplicação é ilimitado.	Não Executado	
	Logout Application	Aplicação com "Logout", verificar se é possível acessar a aplicação ao clicar no botão "Voltar".	Não Executado	
	Renew cookies	Páginas que usam cookies, verifique se é possível renovar os cookies de sessão.	Não Executado	
ROSS SITE SCRIPTING - XS	Xss - Text field	Em campos de Texto e Pesquisa, execute scripts de XSS.	Não Executado	
	Xss - URL	Na URL da aplicação, execute scripts de XSS.	Não Executado	
PROTEÇÃO DE ATAQUES INSUFICIENTES	Insecure Direct Object References	Validar código de erro não tratados nas páginas. (Usar Owasp Zap no modo Spider e Active Scan)	Não Executado	
		Na URL da aplicação, verifique se é possível obter acesso através de Ids e funcionalidades.	Não Executado	
		Execute a ferramenta de pentest (Nikto).	Não Executado	
FALTA DE CONFIGURAÇÃO DE SEGURANÇA	Forbidden url	Verifique na aplicação se é possível acessar url "proíbidas" com referências expostas para atacantes (arquivo, código, diretório e etc.)	Não Executado	
	Autocomplete	Verifique se o autocomplete para campo de texto está habilitado.	Não Executado	
	Entry application points	Verifique se é possível extrair informações com os códigos de status HTTP da aplicação.	Não Executado	
	Entry application points - Login	Verifique se combinações diferentes na tentativa de login disponibilizam informações para o atacante.	Não Executado	
EXPOSIÇÃO DE DADOS SENSÍVEIS	Sensitive Data	Validar se aplicação utiliza criptografia e verificar o certificado.	Não Executado	
REQUISIÇÃO REMOTA FORJADA (CSRF)	Cross-Site Request Forgery (CSRF)	Execução da ferramenta Owasp Zap para validar todas as requisições na aplicação para evitar requisições falsas. Observe também se na aplicação é possível obter informações utilizando engenharia social.	Não Executado	
COMPONENTES COM VULNERABILIDADES CONHECIDAS	Components with Known Vulnerabilities	Verifique se os componentes utilizados possuem vulnerabildiades conhecidas expostas e já utilziadas, um ataque pode causar sérias perdas de dados ou o comprometimento do servidor.	Não Executado	
API's SUBPROTEGIDAS	UNDERPROTECTED API	UTILIZAÇÃO DE API'S SEM CRIPTOGRAFIA, FALTA DE FILA E MAPEAMENTO DE MICROSERVIÇOS, PODENDO CAUSAR PERDAS OU TROCA DE INFORMAÇÕES		
	Unvalidated redirects	Validar todos redirecionamentos que encaminham usuários para outras página na aplicação e fora da aplicação para determinar a página de destino.	Não Executado	
QUEBRA DE CONTROLE DE	Missing Function Leval Acess Control	Falta de niveis de controle de Acesso, nivéis de permissões e controle de acesso não definidos, permitindo a escalada de privilegios, comprometendo a integridade das infromações.	Bloqueado	

O QUE DESCREVER?

Casos de Testes

Feature: Alteração de Dados do Perfil de Usuario Logada
Pré-Condições:
Estar utilizando o Browser Chrome para acessar a página
www.onomedapagina.com.br/login/função
Estar logado no sistema, e clicar na edição de perfil

Descrição:
@Cenário 1: @Funcional @Segurança -> Tags
Dado(Given) que eu abro meu perfil no Twitter após fazer o login
E (And) realizo uma atualização do meu perfil informando um telefone
Quando (When) executar a ação Salvar
Então (Then) espero o receber a mensagem para confirmar a ação inserindo minha senha
E (And) quando a senha informada é corretada a ação é salva e uma mensagem confirma a ação

Palavras Chaves (Keywords): Cenário(s) estão relacionados com a funcionalidade Login Seguro e o(s) Caso(s) de testes abc123.

Versão: Versão que esta associado e foi executado o caso de teste (release ou snapshot) 1.0.X.

Resultados Esperados: Critérios de Aceitação Cumpridos com a Execução do Cenário(s) de teste passando, sim ou não?

O QUE DESCREVER?

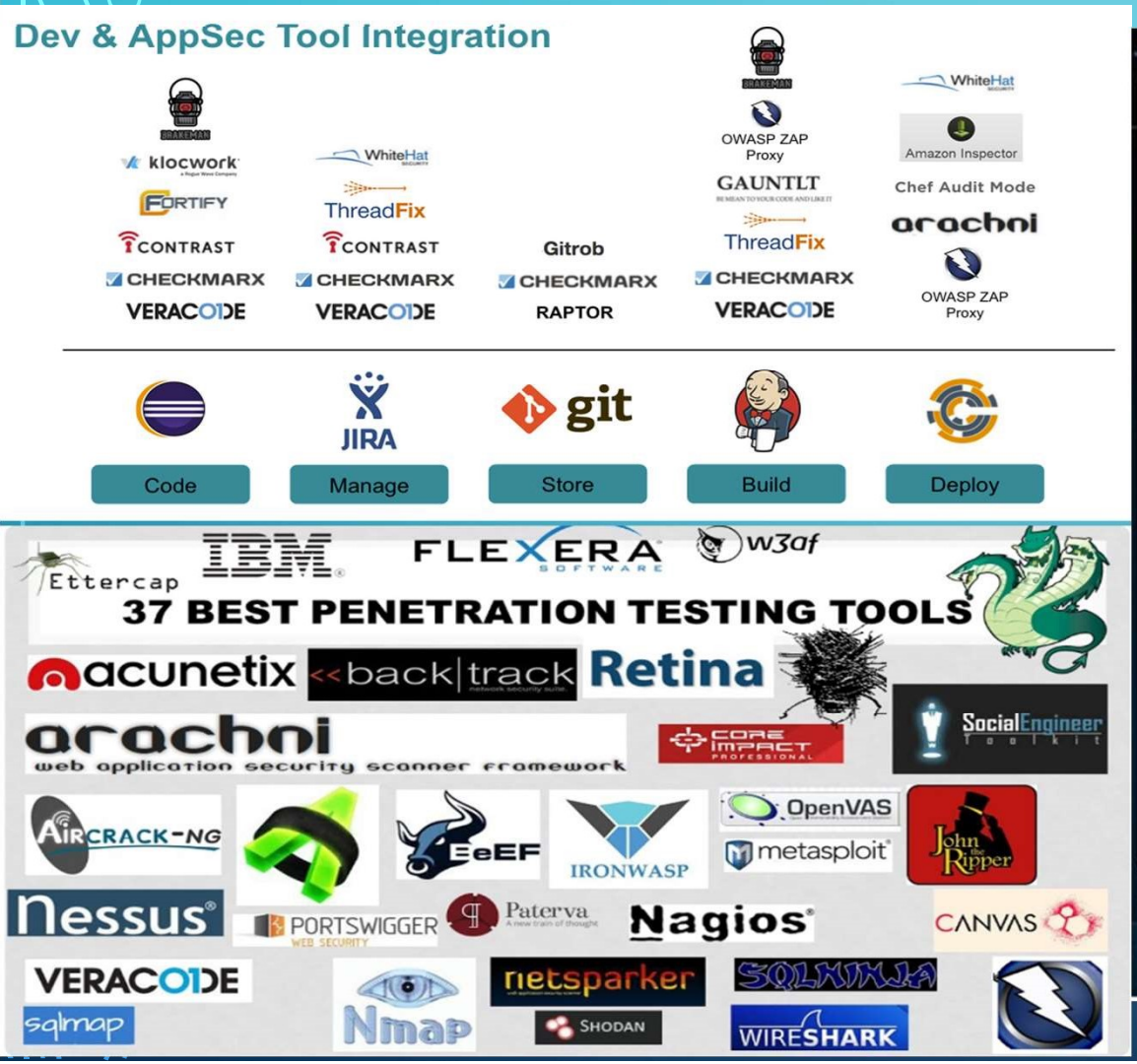
Scripts de Testes

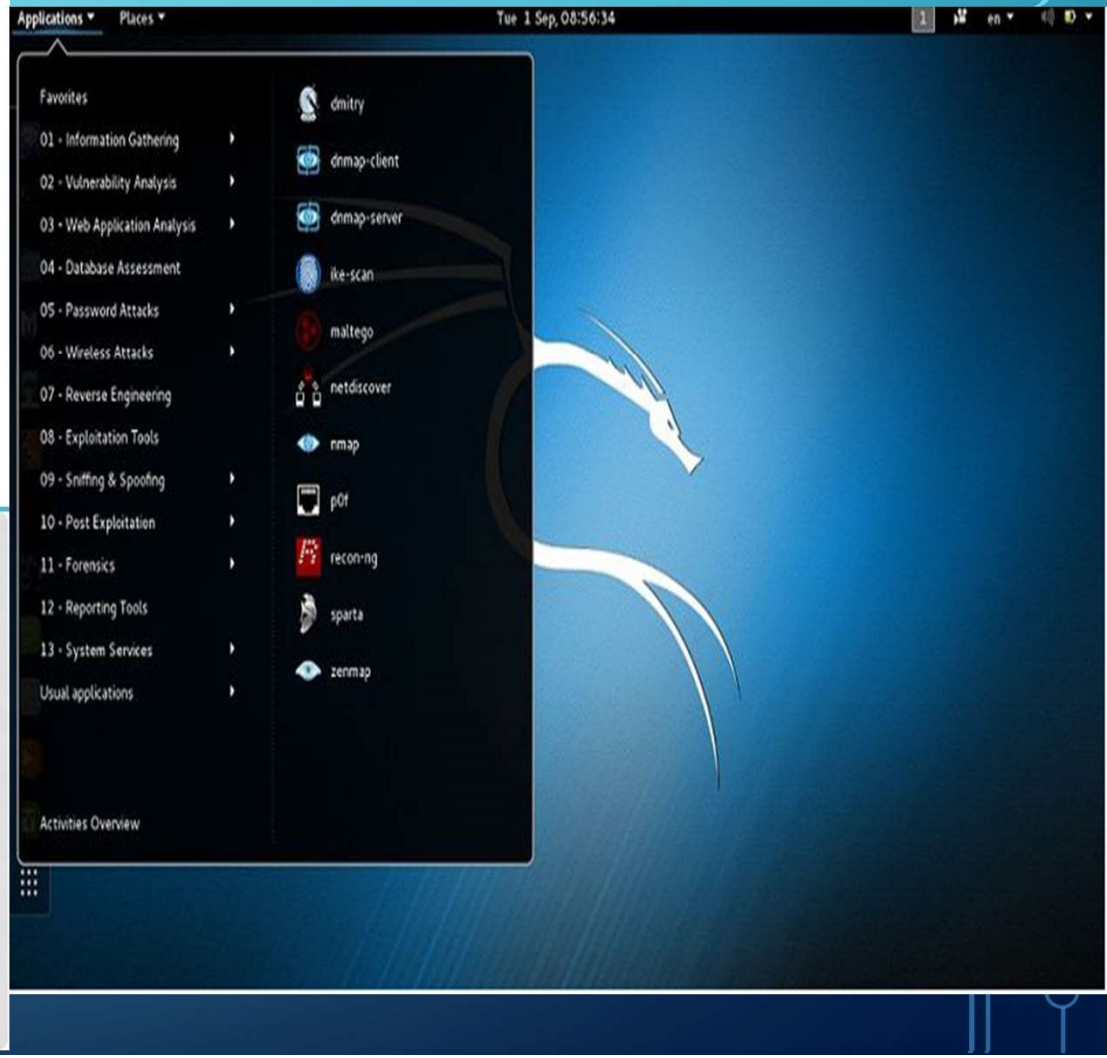
```
package com.example.tests;

public class UntitledTestCase {
private Selenium selenium;

 @Before public void setUp() throws Exception {  WebDriver driver = new
FirefoxDriver();  String baseUrl = "https://www.katalon.com/";
selenium = new WebDriverBackedSelenium(driver, baseUrl);
}
@Test
public void testUntitledTestCase() throws Exception {
selenium.open("https://twitter.com/");
selenium.type("name=session[username_or_email]", "@Xxx_Xx);
selenium.click("id=save_password");
selenium.click("id=user-dropdown-toggle");
selenium.click("xpath=(.//*[normalize-space(text()) and normalize-
space(.)='Teclas de atalho'])[1]/following::button[1]");  selenium.close();
}
@After
public void tearDown() throws Exception {  selenium.stop(); }
```

```
curl -X POST "https://api-
hml.gs1br.org/oauth/access-token" -H "accept:
application/json" -H "Authorization: Basic
NWU1ODYxM2UtMmU5YS0zOGVmLWJkNjktNjJ
kYzU0OTNhZDIwOjhlNGQ2ZTQ4LTUwMWMtM
2VkZC05NjgxLTUwYmYyZDBjYjQ5Mw==" -H
"Content-Type: application/json" -d "{
\"grant_type\": \"password\", \"username\":
\"123abc@gmail.com\", \"password\":
\"G$@2018\", \"cpfCnpj\":
\"007007160218\"}"
```

QUAIS FERRAMENTAS?

Quais Ferramentas o QA pode escolher?





COMO DOCUMENTAR?

O que de fato importa para registrar?

Check- List de Requisitos Não Funcionais;

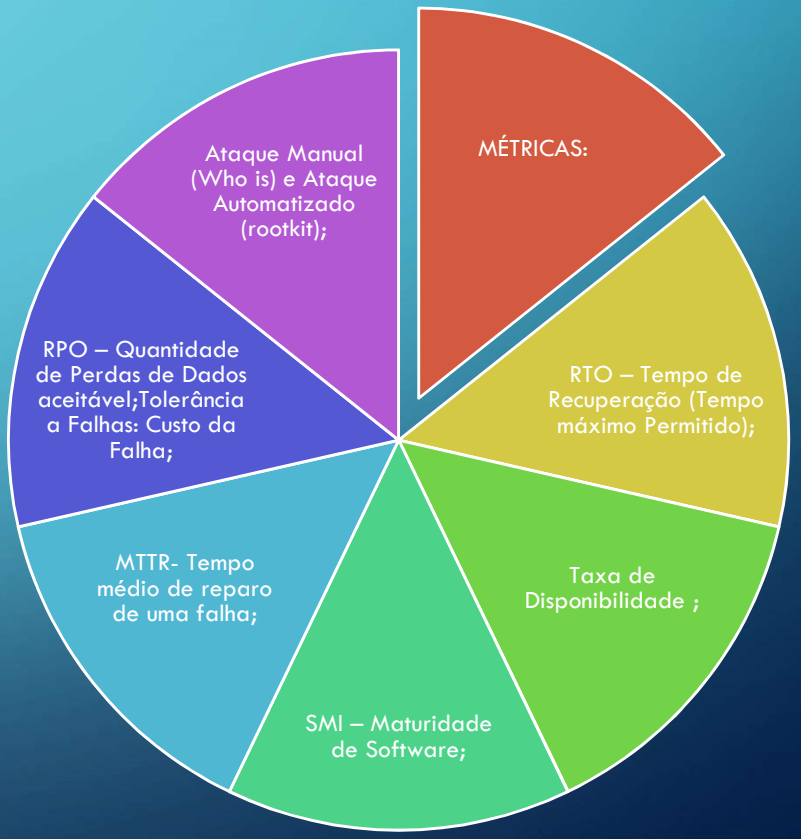
Modelagem de Ameaças;

Scripts para cenários de testes que podem ser automatizados com geração de relatórios

Definição das Ferramentas que serão utilizadas para execução de testes específicos de segurança conforme o domínio da aplicação e ameaças modeladas, que possibilitem a geração de relatórios

EXECUTANDO E GUARDANDO EVIDÊNCIAS DOS TESTES DE SEGURANÇA DURANTE O CICLO DE VIDA DA APLICAÇÃO

- CONTROLE DE HISTORICO DE TESTES EXECUTADOS COM FALHA;
- CONTROLE DE RELATORIOS DE TESTES EXECUTADOS ;
- EXTRAÇÃO DE MÉTRICAS APARTIR DOS RESULTADOS DO TESTES EXECUTADOS;
- MONITORAMENTO DO CICLO VIDA DA APLICAÇÃO VS EVOLUÇÃO DE PROBLEMAS;
- HISTOGRAMA DE FALHAS;
- CONTROLE DE MUDANÇAS VS RELATORIO DE FALHAS PÓS MUDANÇAS;
- GESTÃO DE CONFIGURAÇÃO ATUALIZADA CONFORME CICLO DE VIDA DA APLICAÇÃO



< REFERÊNCIAS:>

COSTA, I; NETO, M; COSTA NETO, P; JUNIOR, J. et al. Qualidade em Tecnologia da Informação. São Paulo: Editora Atlas, 2013. CORREIA, M. Segurança no Software. Lisboa: Editora, 2010. FONTES, E..et al. Políticas e Normas para Segurança da Informação. Rio de Janeiro: Editora Brasport, 2012. LYRA, M. et al. Segurança e Auditoria em Sistemas de Informação. Rio de Janeiro: Editora Ciência Moderna, 2008MIGUEL, A. Gestão de Projectos de Software. Lisboa: Editora QFCA, 2010.RIOS, E; MOREIRA, T. et al. Teste de Software. Rio de Janeiro: Alta Books, 2013. C. 2010. SOLOMON, M.G; KIM, D.et at. Fundamentos de Segurança de Sistemas de Informação. Rio de Janeiro: Editora LTC, 2014.PADUA, W. A. et al. Engenharia de Software Fundamentos, Métodos e Padrões. Rio de Janeiro: Editora LT
https://cipher.com/br/2018/03/13/diferenca-entre-analise-de-vulnerabilidade-e-teste-de-penetracao/https://pt.slideshare.net/JulianoPadilha1/engenharia-de-software-ii-teste-de-seguranca-de-softwarehttps://blog.conviso.com.br/tag/testes-de-seguranca/https://www.cigniti.com/security-testing/https://pt.wikipedia.org/wiki/Ficheiro:%D9%83%D8%A7%D9%84%D9%8A_%D9%84%D9%8A%D9%86%D9%83%D8%B3.pnghttps://pt.wikipedia.org/wiki/Teste_de_seguran%C3%A7ahttps://pt.wikipedia.org/wiki/Kali_Linuxhttps://www.google.com.br/search?q=security+testing+tools&tbm=isch&tbs=rimg:CTx_1PvjxCHzRIjhfhkB-2XWXgUKD20_1IZv8jr7NSG4abVXX_1THw6ngP-DmVUPRj1kq5tQcajQ-M9CczfWFb1U3QVkSoSCV-GQH7ZdZeBEUHQvxzS0fU1KhIJQoPbT8hm_1yMRULmrug4MQ7kqEgmvs1IbhptVdRExQrvwCzK_16SoSCf9MfDqeA_14OETz_1QgqimTbjKhIJZVQ9GPWSrm0Rw0SgIPmvAElqEgIBxqND4z0JzBHEvIIW0FU-UCoSCd9YVvVTdBWREdbDWtQFYz4p&tbo=u&sa=X&ved=2ahUKEwju2qTFnMbeAhVLI5AKHe_4A1UQ9C96BAgBEBs&biw=1366&bih=577&dpr=1#imgrc=TbTxR_jKmy7eFM: