m3corp

VERACODE

Pipeline Scan

Guia de implementação

m3corp

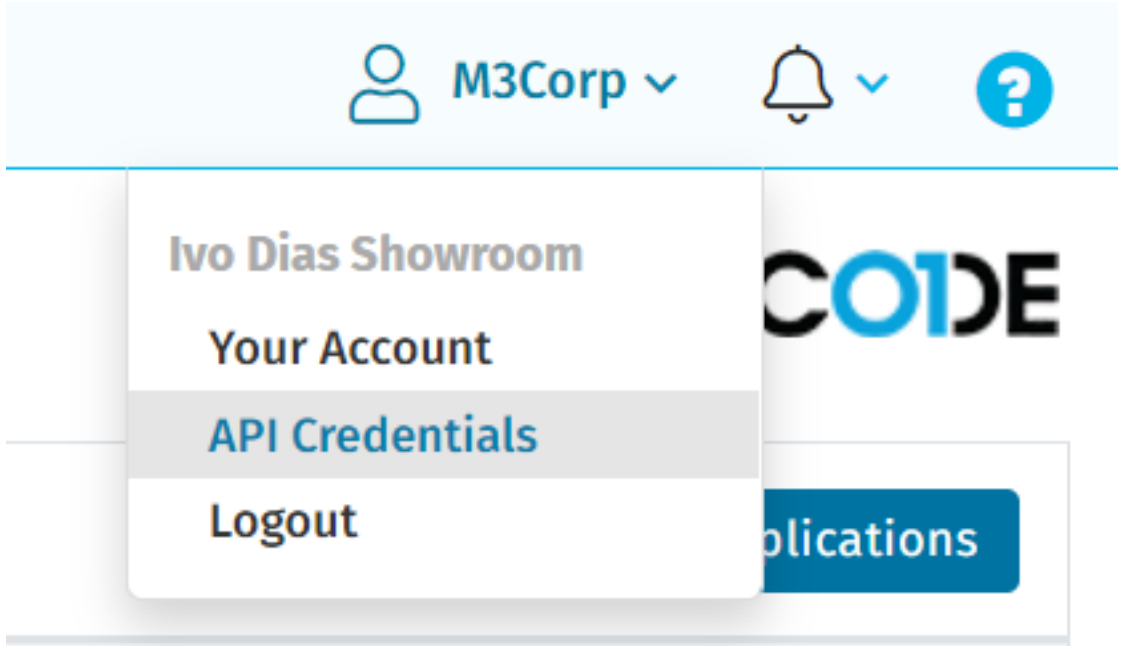
Considerações iniciais

- Para sistemas Mac e Linux, a implementação é a mesma devido ao processo ser feito utilizando Shell script
- Para sistemas Windows, utilizaremos comandos Powershell
- Precisamos ter o Java configurado, já que vamos utilizar um .jar para fazer os scans
- Esse processo pode ser feito em qualquer ferramenta de CI/CD que permita instalar o Java e rodar comandos Shell/Powershell
- O objetivo do material é mostrar como fazer as integrações, mas sem explicar muito sobre as ferramentas. Pode ficar tranquilo que também temos materiais explicando em detalhes cada uma delas.

VERACODE

Credenciais

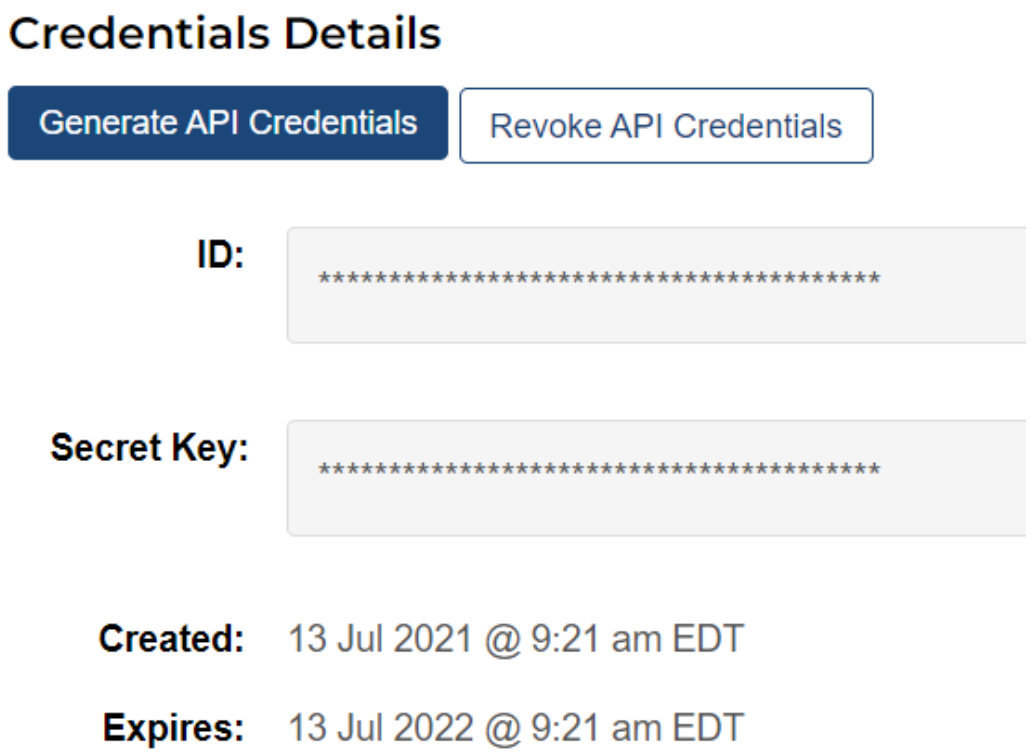
- Nosso primeiro passo é obter as credenciais no portal da Veracode
- O recomendo é a criação de um usuário API especifico para essas integrações
- Conforme a imagem ao lado, precisamos apenas clicar no nosso usuário no canto superior esquerdo e selecionamos a opção de credenciais



m3corp

Credenciais

- Vamos precisar do ID e da Secret Key para fazer as integrações
- Por padrão, essas credenciais duram 1 ano, mas conforme a imagem é possível revoga-las a qualquer momento



VERACODE

m3corp

Pipeline Scan

- Para utilizarmos o Pipeline Scan de forma simples, precisamos apenas fazer o download do script e utiliza-lo
- Caso você tenha um repositório de arquivos, pode fazer o download apenas uma vez e disponibiliza-lo para ser utilizado pelos scripts
- No próximo slide vamos ter um exemplo da implementação mais simples, mas você também consegue fazer customizações no scan, conforme parâmetros disponíveis na documentação
- O ponto mais interessante da ferramenta é o seu retorno completo no terminal, podendo inclusive trabalhar no tratamento dessa resposta para analises personalizadas

VERACODE

m3corp

Pipeline Scan – Linux e Mac

- Com essas três linhas de código, conseguimos fazer a configuração do script e fazer uma analise completa do projeto, com todos os benefícios de uma analise Veracode

```
# Pipeline Scan
curl -sSO https://downloads.veracode.com/securityscan/pipeline-scan-LATEST.zip
unzip pipeline-scan-LATEST.zip
java -jar pipeline-scan.jar -vid $veracodeID -vkey $veracodeAPIkey -f pacoteVeracode.zip
```

  - Na primeira linha fazemos o download do JAR e na segunda descompactamos ele
  - Na terceira fazemos a execução desse JAR passando como parâmetros as credenciais e o caminho do arquivo que queremos analisar

VERACODE

m3corp

Pipeline Scan - Windows

- No Windows fazemos o mesmo processo, só precisamos mudar a linguagem:

```
# Download e configuração
$urlDownload = "https://downloads.veracode.com/securityscan/pipeline-scan-LATEST.zip" # Define a url de download
$caminhoDownload = "$env:LOCALAPPDATA/VeracodePipeline.zip" # Define um caminho para o arquivo de download
Invoke-WebRequest -Uri "$urlDownload" -OutFile "$caminhoDownload" # Faz o download
Expand-Archive -Path "$caminhoDownload" # Descompacta o ZIP para uma pasta
# Uso
java -jar "pipeline-scan.jar" -vid $veracodeID -vkey $veracodeAPIkey -f $caminhoarquivo
```

  - Coloquei algumas linhas a mais só para uma melhor organização, mas podemos reduzir esse numero caso seja necessário

VERACODE

m3corp

Pipeline Scan – Dica de implementação

- Você pode deixar os agentes já baixados para que a equipe apenas utilize eles (isso vale para os outros também, como o API Wrapper)
- Vou exemplificar uma forma de fazer isso em Windows, mas nos outros sistemas é a mesma ideia:
  - Fazer o download para uma pasta do sistema e/ou compartilhada
  - Adicionar o caminho dela ao Path do sistema

```
# Configuracao
$pastaferramenta  = "$Env:Programfiles/Veracode/" # Define uma pasta onde vamos colocar a ferramenta
[Environment]::SetEnvironmentVariable("Path", $env:Path + ";$pastaferramenta") # Adiciona o caminho no Path do sistema

# Download e configuração: Pipeline Scan
$urlDownload = "https://downloads.veracode.com/securityscan/pipeline-scan-LATEST.zip" # Define a url de download
$caminhoDownload = "$env:LOCALAPPDATA/VeracodePipeline.zip" # Define um caminho para o arquivo de download
Invoke-WebRequest -Uri "$urlDownload" -OutFile "$caminhoDownload" # Faz o download
Expand-Archive -Path "$caminhoDownload" -DestinationPath "$pastaferramenta" # Descompacta o ZIP para uma pasta
Remove-Item "$caminhoDownload" # Remove o arquivo de download
```

- Com isso vamos conseguir acessar o agente de qualquer ponto do sistema e em qualquer script ou terminal, sem a necessidade de um novo download
- Para evitar versões defasadas, podemos ter uma rotina de execução desse script de configuração (por exemplo, uma vez por semana)

VERACODE

m3corp

Pipeline Scan

- É assim que vemos os resultados no terminal

```
====================
Analysis Successful.
====================

==================
Analyzed 3 modules.
==================
JS files within 398.zip
PHP files within 398.zip
Python files within 398.zip

====================
Analyzed 101 issues.
====================
-----------------------------------
Found 9 issues of Very High severity.
-----------------------------------
CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'): 1/s/vulnerabilities/view_help.php:15
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/medium.php:19
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/medium.php:23
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/low.php:10
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/low.php:14
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/impossible.php:22
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/impossible.php:26
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/high.php:26
CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'): 1/s/vulnerabilities/exec/source/high.php:30
```

VERACODE

m3corp

Pipeline Scan

- Se ativamos a descrição das falhas, podemos ver assim:

```
CWE-209: Information Exposure Through an Error Message: 1/s/external/phpids/0.6/lib/ids/caching/dat
Details: <span> The application calls the !operator_phpexit() function, which may expose informatic
CWE-209: Information Exposure Through an Error Message: 1/s/external/phpids/0.6/lib/ids/caching/dat
Details: <span> The application calls the !operator_phpexit() function, which may expose informatic
CWE-209: Information Exposure Through an Error Message: 1/s/external/phpids/0.6/lib/ids/caching/dat
Details: <span> The application calls the !operator_phpexit() function, which may expose informatic
CWE-209: Information Exposure Through an Error Message: 1/s/external/phpids/0.6/docs/examples/examp
Details: <span> The application calls the !php_standard_ns.printf() function, which may expose infc
CWE-209: Information Exposure Through an Error Message: 1/s/dvwa/includes/dvwaphpids.inc.php:97
Details: <span> The application calls the !php_standard_ns.printf() function, which may expose infc
----------------------------------------
Skipping 8 issues of Informational severity.
----------------------------------------

========================
FAILURE: Found 93 issues!
========================
```

VERACODE

m3corp

Conclusão

- Como vimos nesse material, mesmo a forma “difícil” de implementar Veracode é muito simples e propicia uma grande liberdade para sua equipe definir como e onde quer trabalhar
- Nossas ferramentas são desenhadas para uma utilização simples, mas sempre pensando em maximizar os resultados. Mesmo com uma ou duas linhas de código, vai conseguir uma analise completa do seu projeto, com a menor taxa de falsos positivos do mercado e de forma simultânea, sem precisar em se preocupar com infraestrutura, já que todos os scans são feitos em nossa nuvem

VERACODE


m3corp
Entre em contato com a nossa equipe para mais detalhes:
vendas@m3corp.com.br
SECURING THE SOFTWARE
THAT POWERS YOUR WORLD
VERACODE