

Roteiros Atividades 01 e 02 de ASTE

Credenciais de acesso

Máquina Virtual

- Usuário: ubuntu
- Senha: Acadi-TI

Jenkins

- Usuário: ubuntu
- Senha: Acadi-TI

Atividade 01 - Projeto Freestyle - vulnado-demo (1. Construção de Esteira FreeStyle no Jenkins)

A partir da máquina virtual disponibilizada no drive da Acadi-TI e execute os passos a seguir:

1. Neste momento, iremos criar um pipeline simples do tipo **Freestyle**. Para isto, na página inicial do **Jenkins**, clique em **Nova tarefa**.



Agora no campo **nome de item** digite **vulnado-demo**, em seguida clique na opção **Construir um projeto de software de estilo livre (2)** e por último clique no botão **Tudo certo**.

Entre com um nome de item

1 vulnado-demo
» Campo requerido

2 **Construir um projeto de software de estilo livre.**
Esta é a central de funcionalidades do Jenkins. Ela construirá seu projeto e você pode combinar qualquer SCM com qualquer sistema de construção, e ele até mesmo pode ser usado para outras tarefas diferentes de construções de *software*.

Construir um projeto maven
Construir um projeto maven. Jenkins tira vantagem de seus arquivos POM e reduz drasticamente a configuração. Ainda é um trabalho em progresso, mas disposto a aceitar feedback.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

3 **Construir projeto de múltiplas configurações**
Tudo certo
Ado para projetos que necessitam de grande número de diferentes configurações, como teste em múltiplos ambientes, builds de formas específicas, etc.

Em seguida acesse o projeto vulnado no github:

<https://github.com/ScaleSec/vulnado>

Clicar em **Code (1)** e em seguida clicar no botão **Copy url to clipboard (2)**.

ScaleSec / vulnado (Public)

Notifications Fork 449

<> Code Issues 3 Pull requests 9 Actions Projects Security Insights

master 5 Branches 0 Tags

Go to file

1 Code

Clone

HTTPS GitHub CLI

2 <https://github.com/ScaleSec/vulnado.git>

Clone using the web URL

Download ZIP

Purposely vulnerable Java app to help lead secure coding work

Readme

New license

Activity

Custom properties

145 stars

18 watching

Desça a página e no campo **Gerenciamento de código fonte** selecione a opção **Git (1)**. Em seguida no campo **Repository URL (2)** insira o repositório que acabamos de copiar.

Configurar

Geral

Gerenciamento de código fonte

Gatilho de disparo para construções

Ambiente de construção

Passos de construção

Ações de pós-construção

Gerenciamento de código fonte

☐ Nenhum☒ Git ?

Repositories ?

Repository URL ?

https://github.com/ScaleSec/vulnado.git

Please enter Git repository.

Credentials ?

- none -

Desça mais a página até encontrar o campo **Branch Specifier (blank for 'any')**. Devemos nos certificar que neste campo esteja especificado o valor ***/master**

Branches to build ?

Branch Specifier (blank for 'any') ?

*/master

Add Branch

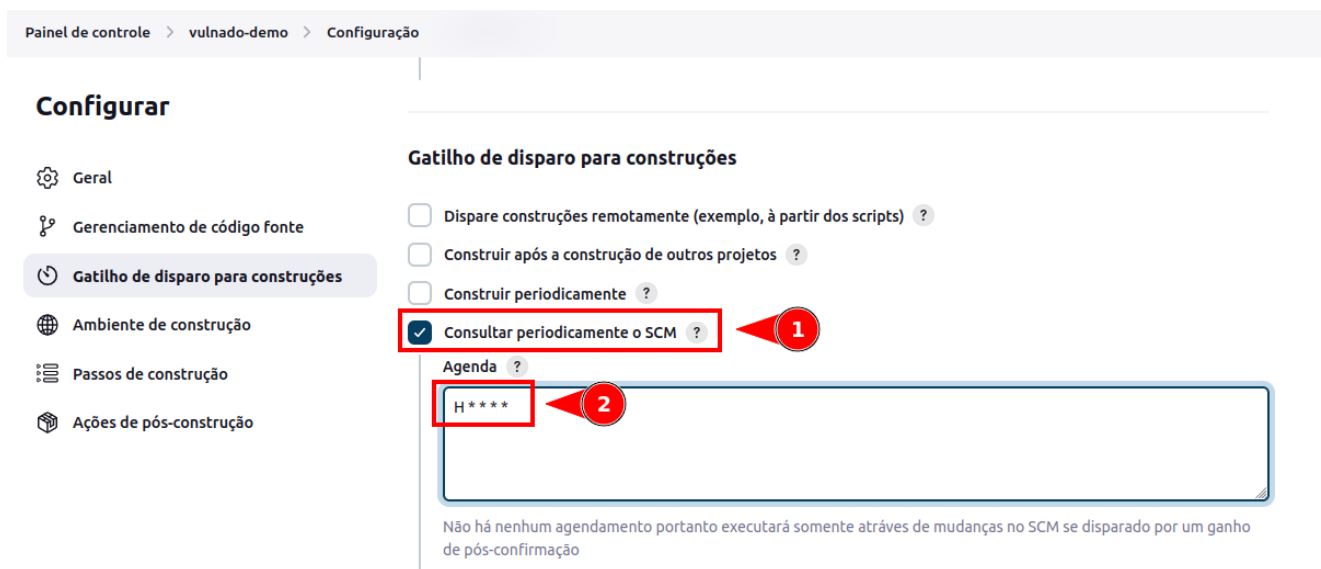
Navegar no repositório ?

(Auto)

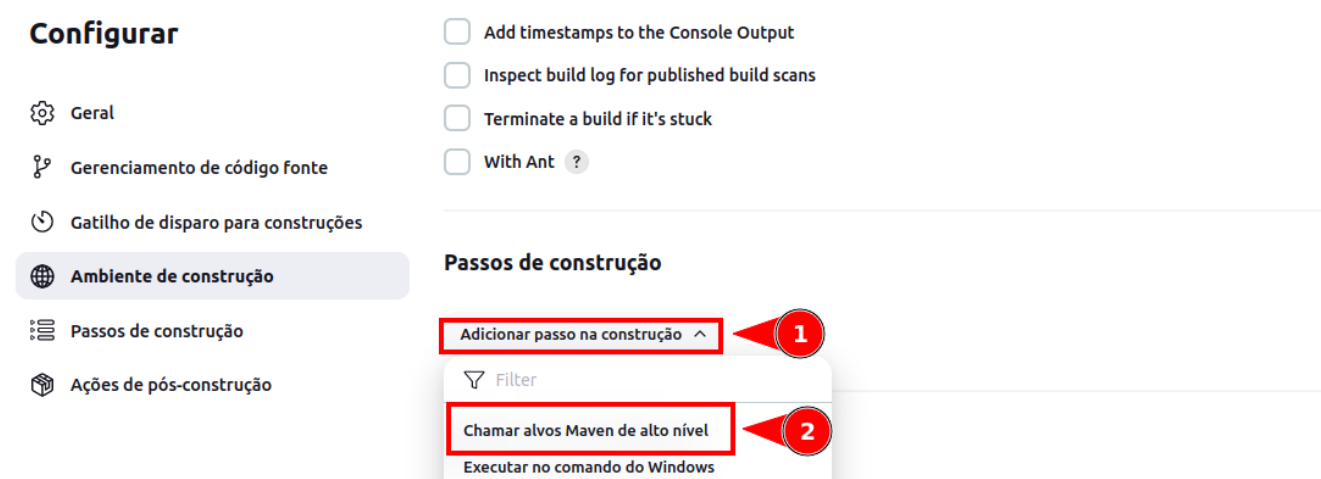
Additional Behaviours

Adicionar ▾

Desça mais um pouco na página e no campo **Gatilho de disparo para construções** marque a opção **Consultar periodicamente o SCM (1)**. Em seguida no campo **Schedule** digite ***H * * ***



Na etapa **Passos de construção** clique na opção **Adicionar passo na construção** (1) e em seguida clique na opção **Chamar alvos Maven de alto nível** (2).



Clique na caixa de seleção abaixo do campo **Versão do Maven** e selecione a opção **Install From Apache** (1). No campo **Goals** digite **compile** (2). Este campo é case *sensitive*, ou seja, se colocar letras em maiúsculo poderá dar erro. Por último clique no botão **Salvar** (3).

Configurar

- Geral
- Gerenciamento de código fonte
- Gatilho de disparo para construções
- Ambiente de construção
- Passos de construção**
- Ações de pós-construção

Passos de construção

Chamar alvos Maven de alto nível ?

Versão do Maven

Install From Apache

Goals

compile

Avançado

Adicionar passo na construção

Ações de pós-construção

Adicionar ação de pós-construção

3

Salvar

Aplicar

Agora clique em **Construir agora**.

Painel de controle > vulnado-demo >

Situação

Alterações

Workspace

Construir agora

Configurar

Excluir Projeto

Git Sondagem de registro de atividades

Renomear

vulnado-demo

Links permanentes

Podemos ver que foi buildado com sucesso.

► Construir agora

⚙ Configurar

🗑 Excluir Projeto

📄 Git Sondagem de registro de atividades

✎ Renomear


Links permanentes

 **Histórico de construções** Tendência ▼


✓ #1 6 de fev de 2024 16:43

 [Atom feed para todos](#)  [Atom feed por falhas](#)






Agora clique na build de número 1.

 **Histórico de construções** Tendência ▼

✓ #1 6 de fev de 2024 16:43

 [Atom feed para todos](#)  [Atom feed por falhas](#)

Aqui você poderá ver a data e horário da build além de informações sobre o repositório utilizado. Agora clique na opção **Alterações**.

 **Jenkins**     ubuntu ▼

Painel de controle > vulnado-demo > #1

📄 Estado pessoal

</> Alterações


📄 Saída do console

📄 Editar informações de compilação


🗑 Apagar a construção {0}

🔗 Git Build Data

✓ #1 (6 de fev de 2024 16:43:37)

 Adicionar descrição

Iniciado pelo(a) usuário(a) **ubuntu**

 **Revision:** 53336e14a40a0b25acdb8edd8b65a813e5f61bda
Repository: <https://github.com/ScaleSec/vulnado.git>
• refs/remotes/origin/master

Deixar essa construção como perma

Iniciado 1 min 9 seg atrás
Levou **19 seg**

Agora clique em **Saída do console** para que possamos ver mais informações.

Estado pessoal

✓ #1 (6 de fev de 2024 16:43:37)

Deixar essa construção como permanente

</> Alterações

Saída do console

✍ Editar informações de compilação

🗑 Apagar a construção {0}

🔗 Git Build Data

✎ Adicionar descrição

Iniciado 2 min 7 seg atrás
Levou 19 seg

</> No changes.

🕒 Iniciado pelo(a) usuário(a) **ubuntu**git
Revision: 53336e14a40a0b25acdb8edd8b65a813e5f61bda
Repository: <https://github.com/ScaleSec/vulnado.git>
• refs/remotes/origin/master

Aqui você poderá visualizar as informações do processo de build.

Estado pessoal

✓ Saída do console

</> Alterações

Saída do console

📄 Exibir como texto puro

✍ Editar informações de compilação

🗑 Apagar a construção {0}

🔗 Git Build Data

Ignorando 23 KB.. [Ver log completo](#)Downloading from central: <https://repo.maven.apache.org/maven2/org/springframework/spring-web/5.1.4.RELEASE/spring-web-5.1.4.RELEASE.pom>
Progress (1): 12 kBDownloaded from central: <https://repo.maven.apache.org/maven2/org/springframework/spring-web/5.1.4.RELEASE/spring-web-5.1.4.RELEASE.pom> (12 kB at 476 kB/s)Downloading from central: <https://repo.maven.apache.org/maven2/com/fasterxml/jackson/core/jackson-databind/2.9.8/jackson-databind-2.9.8.pom>
Progress (1): 6.3 kBDownloaded from central: <https://repo.maven.apache.org/maven2/com/fasterxml/jackson/core/jackson-databind/2.9.8/jackson-databind-2.9.8.pom> (6.3 kB at 191 kB/s)Downloading from central: <https://repo.maven.apache.org/maven2/com/fasterxml/jackson/jackson-base/2.9.8/jackson-base-2.9.8.pom>
Progress (1): 5.5 kB

Desça até o final e verá informações sobre o status de build, data, horário e também o tempo que esse processo levou para ser realizado.

```
[INFO] -----  
[INFO] BUILD SUCCESS  
[INFO] -----  
[INFO] Total time: 13.662 s  
[INFO] Finished at: 2024-02-06T16:43:56-03:00  
[INFO] -----  
Finished: SUCCESS
```

Atividade 02 - Construção de Pipeline no Jenkins via HoruSec

Clique no botão **Nova tarefa**.

Painel de controle >

+ Novo tarefa

Usuários

Histórico de compilações

Gerenciar Jenkins

Minhas visões

Tudo

+

S	W	Nome ↓	Último sucesso	Última falha	Última duração
✓	☀	vulnado-demo	3 min 24 seg #1	N/D	19 seg

Fila de construções

Nenhuma construção na fila.

Estado do executor de construções

1 Parado

2 Parado

Ícone: P M G

Icon legend

Atom feed para todos

Atom feed para falhas

Atom feed para apenas

No campo **Entre com um nome de item** digite **"VULNADO (Pipeline)"** (2). Em seguida selecione a opção **Pipeline (2)** e por último clique no botão **Tudo certo**.

Painel de controle > Tudo >

1

Entre com um nome de item

VULNADO (Pipeline)

» Campo requerido

2

Construir um projeto de software de estilo livre.

Esta é a central de funcionalidades do Jenkins. Ela construirá seu projeto e você pode combinar qualquer SCM com qualquer sistema de construção, e ele até mesmo pode ser usado para outras tarefas diferentes de construções de *software*.

Construir um projeto maven

Construir um projeto maven. Jenkins tira vantagem de seus arquivos POM e reduz drasticamente a configuração. Ainda é um trabalho em progresso, mas disposto a aceitar feedback.

Pipeline

Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

3

Construir projeto de múltiplas configurações

do para projetos que necessitam de grande número de diferentes configurações, como teste em múltiplos ambientes, builds de formas específicas, etc.

Tudo certo

Agora clique em **Pipeline**.

Painel de controle > VULNADO (Pipeline) > Configuração

Configurar

Geral

Advanced Project Options

Pipeline

Geral

Habilitado ☒

Descrição

HTML escapado [Visualizar](#)

☐ Descartar construções antigas ?

☐ Do not allow concurrent builds

No campo **Script** será onde iremos inserir o nosso script com instruções da build do nosso projeto.

Painel de controle > VULNADO (Pipeline) > Configuração

Configurar

Geral

Advanced Project Options

Pipeline

Pipeline

Definition

Pipeline script

Script ?

1

try sample Pipeline... ▾

☒ Use Groovy Sandbox ?

[Pipeline Syntax](#)

Salvar Aplicar

Colar o seguinte código no campo **Script**.

```
pipeline {
    agent any
    stages {
        stage('PASSO 1: Coleta do Projeto do repositório GIT')
    }
    steps{
        git 'https://github.com/ScaleSec/vulnado'
    }
    stage('PASSO 2: Analise de Segurança SAST via
```

```

Horusec') {
    steps {
        sh 'horusec start -p="." --disable-
docker="true" --information-severity="true" -log-level="debug"
> SAST.log'
    }
}
stage('PASSO 3: Apresentação de Relatório de
Resultados') {
    steps {
        sh 'cat SAST.log'
    }
}
}
}
}

```

Após colar o código acima clique no botão **Salvar**.

Painel de controle > VULNADO (Pipeline) > Configuração

Configurar

- Geral
- Advanced Project Options
- Pipeline**

Pipeline

Definition

Pipeline script

Script ?

```

3 agent any
4 stages {
5   stage('PASSO 1: Coleta do Projeto do repositório GIT'){
6     steps{
7       git 'https://github.com/ScaleSec/vulnado'
8     }
9   }
10  stage('PASSO 2: Analise de Segurança SAST via Horusec'){
11    steps{
12      sh 'horusec start -p="." --disable-docker="true" --information-severity="true" -log-level="debug" > SAST.log'
13    }
14  }
15  stage('PASSO 3: Apresentação de Relatório de Resultados'){
16    steps{
17      sh 'cat SAST.log'
18    }
19  }
20 }
21 }

```

try sample Pipeline...

☒ Use Groovy Sandbox ?

[Pipeline Syntax](#)

Salvar Aplicar

Agora clique no botão **Construir agora**.

Painel de controle > VULNADO (Pipeline) >

Status

</> Changes

▶ Construir agora

⚙️ Configurar

🗑️ Excluir Pipeline

🔍 Full Stage View

✎ Renomear

VULNADO (Pipeline)

✎ Adicionar descrição

Desabilitar projeto

Stage View

No data available. This Pipeline has not yet run.

Com isso podemos ver que a build foi executada com sucesso.

Painel de controle > VULNADO (Pipeline) >

Status

</> Changes

▶ Construir agora

⚙️ Configurar

🗑️ Excluir Pipeline

🔍 Full Stage View

✎ Renomear

🔗 Pipeline Syntax

VULNADO (Pipeline)

✎ Adicionar descrição

Desabilitar projeto

Stage View

Average stage times:
(Average full run time: ~5s)

	PASSO 1: Coleta do Projeto do repositório GIT	PASSO 2: Análise de Segurança SAST via Horusec	PASSO 3: Apresentação de Relatório de Resultados
#1	795ms	3s	424ms

fev. 06 16:59 No Changes

Links permanentes

Histórico de construções **Tendência** ▾

🔍 Filtro de construções... /

✅ #1 6 de fev de 2024 16:59

📡 Atom feed para todos

📡 Atom feed por falhas

Para visualizar os logs, passe a seta por cima do quadrado verde referente ao PASSO 3 (1) e em seguida clique no botão Logs (2).

🗑️ Excluir Pipeline

🔍 Full Stage View

✎ Renomear

🔗 Pipeline Syntax

Stage View

Average stage times:
(Average full run time: ~5s)

	PASSO 1: Coleta do Projeto do repositório GIT	PASSO 2: Análise de Segurança SAST via Horusec	PASSO 3: Apresentação de Relatório de Resultados
#1	795ms	3s	424ms

fev. 06 16:59 No Changes

Links permanentes

Histórico de construções **Tendência** ▾

🔍 Filtro de construções... /

✅ #1 6 de fev de 2024 16:59

📡 Atom feed para todos

📡 Atom feed por falhas

📊 Logs

Com isso pudemos ver os logs da nossa build. Juntamente com as vulnerabilidades encontradas.

Stage Logs (PASSO 3: Apresentação de Relatório de Resultados)

Shell Script – cat SAST.log (self time 310ms)

c269d4fe13b89ea9ff06fe729061

Details: (1/1) * Possible vulnerability detected: Unchecked Class Instantiation when providing Plugin Classes

CVE-2022-21724 pgjdbc instantiates plugin instances based on class names provided via authenticationPluginClassName, sslhostnameverifier, socketFactory, sslfactory, sslpasswordcallback connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. The first impacted version is REL9.4.1208 (it introduced socketFactory connection property) until 42.3.1. Please update to fixed versions ^42.2.25 or ^42.3.2. For more information checkout the CVE-2022-21724 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21724>) advisory.

=====

Language: Java

Severity: HIGH

Line: 31

Column: 6

SecurityTool: HorusecEngine

Confidence: LOW

File: /var/lib/jenkins/workspace/VULNADO (Pipeline)/src/main/java/com/scalesec/vulnado/Comment.java

Code: } catch (Exception e) {

RuleID: HS-JAVA-63

Histórico de construções **Tendência**

Filtro de construções...

#1

6 de fev de 2024 16:59

Average stage times:
(Average full run time: ~5s)

795ms

3s

424ms

#1

fev.06
16:59

No
Changes

795ms

3s

424ms