01

Fazendo upload de arquivo

Transcrição

[00:00] Vamos voltar aqui para a nossa máquina do Kali Linux, a máquina do hacker, para tentar fazer mais alguns testes para encontrar vulnerabilidades aqui nessa aplicação da Alura shows. Então vamos voltar no Browser para nós podermos acessar a aplicação da Alura shows e como a aplicação da Alura Shows está rodando no Tomcat que está no Windows, nós temos que colocar o endereço IP da minha máquina do Windows, que no meu caso aqui é 19268121.100 e a porta de comunicação com o Tomcat é 8080.

[00:25] E aqui nós temos nossa aplicação da Alura shows. Então vamos tentar verificar novamente aquela parte de registro de usuário. Usuário, nós vamos na aba e nós clicamos na aba para registrar esse novo usuário e nós vamos registrar agora o usuário que é a Priscila.

[00:41] Então nós colocamos aqui o nome da Priscila, o e-mail da Priscila, priscila@gmail.com, e a senha da Priscila vai ser 1 2 3 4 5 6. E chega a hora da Priscila fazer o upload da imagem do perfil dela. A Priscila vai parar e vai pensar: será que a aplicação da Alura shows está fazendo alguma validação desse tipo de arquivo que nós estamos passando aqui? Ou será que a aplicação da Alura shows está aceitando qualquer tipo de arquivo?

[01:09] A Priscila vai querer fazer esse teste. Então qual que vai ser aqui a ideia da Priscila? Bom, essas imagens do que nós fazemos o upload do perfil vão ser passadas para o Tomcat e o Tomcat está rodando na nossa máquina do Windows.

[01:29] Então o que é que a Priscila vai tentar fazer? Ela vai querer verificar se de fato a aplicação da Alura shows está fazendo essa validação de que tipo de arquivo nós estamos passando e ela vai passar, na verdade, um arquivo como sendo a imagem do perfil dela que na verdade vai ser uma jsp com um código JAVA dentro para tentar remover um diretório presente aqui na nossa máquina do Windows.

[01:50] Vamos fazer esse teste inicialmente na nossa máquina do Windows, para ver como é que nós poderíamos fazer isso? Eu vou aqui clicar no explorador de arquivos e nós vamos aqui no nosso disco no C e nós vamos criar um novo diretório para nós podermos fazer esse teste, uma nova pasta.

[02:07] Eu vou clicar aqui, novo, para criar uma nova pasta e nós vamos criar essa nova pasta com o nome imagem falsa. Primeiro, vamos verificar aqui, com o prompt de comando, como é que nós poderíamos remover esse diretório que nós acabamos de criar.

[02:23] Então eu vou vir aqui e nós chamamos o prompt, é só colocar para baixo para nós podermos visualizar os dois ao mesmo tempo. Quando eu abro o prompt, nós entramos nesse nosso diretório, no nosso caso, o diretório Caelum. Então nós criamos essa pasta aqui no nosso disco C.

[02:41] O primeiro passo que nós temos que fazer é o quê? É mudar o diretório para ir aqui para o nosso disco C. Então eu coloco aqui na hora de mudar o diretório, change directory, e eu quero sair aqui e voltar para o C/ e eu tenho que escapar essa barra aqui com uma outra barra para dizer que nós queremos ir para esse caminho aqui.

[02:57] Então uma vez que nós estamos dentro desse nosso disco C, o que é que nós queremos fazer? Nós queremos remover esse diretório que nós acabamos de criar que recebe esse nome, imagem falsa. Então, além desse comando que nós estamos executando de mudar o diretório, nós queremos remover, então eu coloco duas vezes o & comercial, nós queremos remover um diretório, então nós colocamos aqui “rmdir” para remover o diretório chamado aqui de imagem falsa.

[03:24] Então vamos ficar vendo aqui. Nós temos aqui esse nosso diretório imagem falsa que nós acabamos de criar e eu vou rodar esse comando aqui no prompt. Vamos ver o que acontece. O diretório imagem falsa acabou de ser removido.

[03:36] O que nós vamos fazer agora? Nós vimos que esse comando funciona aqui no prompt, então agora nós vamos pedir para o nosso projector, estamos utilizando a linguagem Java, para tentar fazer essa mesma remoção, só que agora utilizando a linguagem Java.

[03:50] Eu vou criar novamente esse nosso diretório, só voltar para cá, e nós vamos criar novamente esse nosso diretório que nós vamos chamar de imagem falsa. Vamos voltar aqui no nosso projeto, no Eclipse, e eu vou fazer essa mesma execução agora com o código Java.

[04:06] Nós vamos aqui, vamos criar uma nova classe, nós vamos colocar essa classe dentro de um pacote aqui que nós vamos chamar de teste e o nome dessa nossa classe vai ser teste imagem falsa. Nós já podemos até marcar aqui para pegar o main para executar esse código. Eu já marco aqui, para vir no main, e finish.

[04:29] Nós já temos aqui essa nossa classe. Então aqui para podermos executar esse teste com a linguagem Java nós podemos utilizar da classe runtime. Então nós chamamos a classe runtime, eu venho aqui e peço para a classe runtime o método estático dela, que é o getRunTime, para que nós possamos executar esse comando.

[04:49] Eu chamo aqui o método Exec. E o que é que eu quero executar? Eu quero executar justamente esse comando que nós fizemos no prompt para poder deletar, para poder remover, esse diretório da nossa máquina.

[04:59] Como é que seria isso? O primeiro passo é nós pegarmos o prompt de comando. Então nós vamos aqui e colocamos “cmd.exe” e agora nós queremos o quê? Nós queremos executar o comando aqui no prompt. Então para dizer que eu quero executar um comando, nós colocamos aqui /c. O que nós queremos executar? Nós queremos executar esse comando aqui que nós fizemos.

[05:18] Eu vou copiar esse comando que nós já tentamos e vimos que funciona no terminal, no prompt, e agora nós vamos aqui e colamos esse nosso comando. Vou só colocar “Ctrl + S” e eu vou colocar “Ctrl + 1” e para ele colocar o try catch.

[05:38] Agora nós já fizemos essa nossa configuração. Vou só colocar aqui do lado e essa nossa classe teste imagem falsa e eu vou voltar para o explorador de arquivos para nós podermos ver se de fato ele vai ser removido.

[06:00] Eu vou vir aqui e nós vamos executar essa nossa classe com o objetivo de verificar se esse nosso diretório imagem falsa vai ser removido. Então eu vou vir aqui, eu vou colocar “F11”, eu vou colocar aqui Java application e vamos verificar. O nosso diretório imagem falsa deixou de existir.

[06:24] Então com isso o que que a Priscila vai fazer? Ela sabe que esse código JAVA já funcionou, não funcionou? Então dentro da jsp, como ela aprendeu aqui nos outros cursos da Alura, nós podemos ter os nossos scriptlets para rodar um código JAVA. Nós sabemos que não é boa prática fazer isso, mas para esse teste da Priscila, que ela quer comprometer a vulnerabilidade da segurança, é exatamente o que ela vai precisar.

[06:45] Ela vai vir aqui, ela copia esse código JAVA e ela vai voltar aqui para a máquina dela do Kali Linux e ela vai configurar uma jsp com esse código JAVA para remover esse diretório imagem falsa.

[07:00] Então vou só colocar a senha do Kali Linux e eu vou utilizar o Atom para poder fazer essa configuração dessa jsp. Então eu vou vir nas aplicações e eu vou pesquisar aqui pelo Atom, que é o editor de texto que eu vou usar, mas você pode ficar à vontade de usar o editor de texto de sua preferência.

[07:21] E aqui nós vamos criar essa nossa jsp. Então eu vou só esperar o Atom carregar, só vou esperar mais alguns segundos para o Atom carregar. Ele carregou. E aqui nós vamos criar esse nosso arquivo, que nós já vamos aproveitar,

vamos salvar esse arquivo, vamos como colocar no desktop mesmo. E nós vamos chamar ele de imagem falsa.jsp.

[07:50] Então para nós dizermos que é um código JAVA, para envolver com os scriptlets, o que é que nós temos que fazer? Nós temos que abrir a tag e nós temos que colocar a porcentagem. E nós colocamos o nosso código JAVA que nós já vimos que funciona que nós rodamos no eclipse, funcionou.

[08:09] Agora basta nós virmos aqui e fechar esse nosso scriptlet, também aqui com porcentagem e nós fechamos essa nossa tag. E nós temos que só fazer os imports do JAVA lang, do JAVA io, para nós podermos executar esse nosso código JAVA. Então para fazer esses devidos imports, nós colocamos aqui, abre a tag, nós colocamos aqui porcentagem @, nós colocamos aqui "<@page import = java.lang.*">.

[08:40] Nós vamos importar aqui também "<@page import = java.io.*". Nós colocamos ponto. O asterisco para importar tudo, porcentagem, e nós fechamos essa nossa tag dos imports.

[09:02] Então agora nós estamos o quê? Nós criamos esse nosso arquivo jsp com esse código JAVA dentro aqui das scriptlets com o objetivo o quê? De remover um diretório aqui nessa nossa máquina do Windows. Então eu vou só colocar "Ctrl + S" para salvar essa nossa jsp, e nós não podemos esquecer, que nós removemos a pasta, o diretório, aqui na nossa máquina do Windows.

[09:27] Eu vou só voltar ela, vamos só criar de novo, nova pasta, vamos colocar de novo imagem falsa aqui. Então nós estamos no C, aqui na nossa máquina do Windows, e nós temos esse diretório aqui, imagem falsa.

[09:39] Eu vou aqui na nossa máquina do Kali Linux e nós estamos nesse computador agora do Kali Linux, o computador que a Priscila está utilizando, e ela vai tentar agora fazer o upload desse arquivo jsp com esse código JAVA dentro e vamos ver se a aplicação aqui da Alura shows está preparada para isso.

[09:57] Eu vou vir aqui, coloco o endereço IP da máquina no Windows, dois pontos 8080/Alurashows, usuário, registrar, e nós colocamos aqui o nome da Priscila, o e-mail da Priscila é priscila@gmail.com, a senha da Priscila era 123456. E aí a Priscila vai fazer o quê? Ela vai fazer o upload desse arquivo jsp imagem falsa como se fosse a imagem do perfil dela.

[10:23] Então agora, eu vou até tentar colocar os dois aqui lado a lado, vamos ver se dá certo, para nós podermos ver se esse nosso diretório imagem falsa de fato vai ser removido. Então eu estou aqui no Kali Linux, no lado direito e aqui no lado esquerdo nós estamos na máquina do Windows no nosso disco C.

[10:43] Eu vou clicar aqui para registrar a Priscila e a nossa aplicação aceitou uma imagem jsp, a imagem falsa.jsp, olha só o que aconteceu aqui na nossa máquina do Windows? O diretório foi removido. Imagina só o estrago que isso não poderia ser? Nós poderíamos aqui, a nossa aplicação da Alura shows, não está fazendo nenhuma validação com esse tipo de arquivo que o usuário pode estar, que ele pode estar colocando como upload.

[11:11] E nós poderíamos sair removendo tudo que nós quiséssemos na máquina do Windows que é onde está rodando o nosso Tomcat. Olha só o problema que isso não poderia ser e a vulnerabilidade aqui que essa nossa aplicação da Alura shows não tem. Nós precisamos corrigir. Vamos ver como é que nós podemos corrigir isso na próxima etapa.