

Guião de Demonstração

Instalação

1. Obter o código do repositório git da 3ª entrega
(<https://github.com/tecnico-distsys/T06-SD18Proj>)
2. Dentro da raiz do repositório correr **mvn clean install -DskipTests**

Demonstração

Execução Normal (S1) : Neste exemplo temos um utilizador bem intencionado, que activa a sua conta e usa o seu email para fazer os pedidos de levantamento e depósito de bina.

- Na diretoria **station-ws** fazer **mvn clean compile exec:java -Dws.i=1**, em **novos terminal**
- Na diretoria **binas-ws** fazer **mvn clean compile exec:java**, em **novos terminal**
- Na diretoria **binas-ws-cli** fazer **mvn test -Dtest=SecurityIT**, em **novos terminal**
- Observar o teste a correr e verificando no terminal do station-ws que existe na realidade uma alteração do saldo do utilizador e que a bina é libertada correctamente e retornada também.
- Observar nos terminais do binas-ws e binas-ws-cli a comunicação através dos handlers.

Ataque - email errado (S2) :Utilizador malicioso que se autentica com credenciais válidas, e-mail e password, mas ao enviar o pedido envia o email de outro utilizador, de modo a levantar uma bina sem perder créditos. (Esta alteração de email é feita através do handler EvilHandler):

- Aceder ao ficheiro **binas-ws-cli/src/jaxws/binas-ws-cli_handler-chain.xml** e descomentar o handler **example.ws.handler.EvilHandler**
- Na diretoria **station-ws** fazer **mvn clean compile exec:java -Dws.i=1**, em **novos terminal**
- Na diretoria **binas-ws** fazer **mvn clean compile exec:java**, em **novos terminal**
- Na diretoria **binas-ws-cli** fazer **mvn clean compile exec:java**, em **novos terminal**
- Observar que a execução falha, pois o servidor vê que o email do pedido não corresponde ao que foi enviado no ticket nem com o que vem no auth.
- Aceder ao ficheiro **binas-ws-cli/src/jaxws/binas-ws-cli_handler-chain.xml** e comentar o handler **example.ws.handler.EvilHandler**

Ataque - pedido alterada na rede (S3): Este teste simula o caso em que um utilizador malicioso executa um *man in the middle attack* e altera o pedido feito pelo cliente, sem alterar o auth ou o ticket.

- Aceder ao ficheiro `binas-ws/src/main/resources/binas-ws_handler-chain.xml` e descomentar o handler `example.ws.handler.EvilMacHandler`
- Na diretoria `station-ws` fazer `mvn clean compile exec:java -Dws.i=1`, em novo terminal
- Na diretoria `binas-ws` fazer `mvn clean compile exec:java`, em novo terminal
- Na diretoria `binas-ws-cli` fazer `mvn clean compile exec:java`, em novo terminal
- Observar que a execução falha, pois o servidor vê que o pedido recebido não corresponde ao pedido que foi usado para gerar o MAC, rejeitando assim o pedido em questão
- Aceder ao ficheiro `binas-ws/src/main/resources/binas-ws_handler-chain.xml` e comentar o handler `example.ws.handler.EvilMacHandler`