

Relatorio de falhas

emc.cpp

Uso de método indevido: 6 - gets();,

8 - vsprintf();,

10 - sprintf();,

Evite utilizar estes métodos para não ocorrer vazamentos de memória

Unsigned não tratado: usum4,

usum3,

Verifique se o valor recebido é positivo

Exe_1.java

Unboxing: n1,

n2,

n3,

n4,

doido,

n6,

n7,

O retorno das seguintes variáveis pode ser nulo, adicione clausulas throws ou bloco try catch para tratar exceções

Falhas de segurança de senha: 70 - jp5,

71 - jp5,

140 - jp,

59 - t.campo2().getText();,

118 - t.campo2().getText();,

PasswordField utilizando metodo .getText(), recomendado utilizar .getPassword()

Socket não possui criptografia: 43 - Socket s;,

Utilize criptografia SSL

Falhas variaveis final: 134 - public static int estatico = 0;,,

Declare esta variavel como final

Falhas de SQL: 119 - query = "select * from usuarios "+df,
120 - + "where nome = "+usuario;;

Evite concatenar valores diretamente na instrução SQL

Teste.java

Falhas variaveis final: 13 - public static int senha_teste;;

Declare esta variavel como final

Socket não possui criptografia: 50 - Socket s = new Socket("localhost", 5555);,

Utilize criptografia SSL

Falhas de segurança de senha: 31 - exe.noexe().getText();,
36 - campo().getText();,
34 - jpteste,
45 - js99,

PasswordField utilizando metodo .getText(), recomendado utilizar .getPassword()

Falhas de SQL: 32 - query = "insert into usuarios values("+usuario+"");,
42 - query = "select * from usuarios where nome = "+usuario;;

Evite concatenar valores diretamente na instrução SQL

Unboxing: n8,
n9,
b,

O retorno das seguintes variáveis pode ser nulo, adicione clausulas throws ou bloco try catch para tratar exceções

teste.php

Possível falha de Manipulação de URL: 14 - include(\$teste);,
30 - include(\$arquivo);//Incluioarquivo,

Verifique se há validação para estas variáveis

Falhas de SQL: 2 - \$query = 'select * from algumacoisa dsfs'.\$haha +,
3 - 'where nome = '.\$churros +,

4 - 'where nome = '.\$churros;;

Evite concatenar valores diretamente na instrução SQL

tt.php

Possível falha de Manipulação de URL: 0 falhas encontradas

Falhas de SQL: 2 - \$query = 'select * from algumacoisa dsfs'.\$haha +,

3 - 'where nome = '.\$qw +,

4 - 'where nome = '.\$chuquerwrros;;

Evite concatenar valores diretamente na instrução SQL