Episode 2

Hacking Sunday

DESERIALIZATION

Twitter- @trouble1_raunak

LET'S FIRST TALK ABOUT WHAT IS THIS DESERILIZATION

LET'S FIRST UNDERSTAND WHAT IS SERILIZATION

THIS IS WHAT SERIALIZATION IS

It is the process of translating data structures or object state into bytes format that can be stored on disk or database or transmitted over the network.

AND THIS IS WHAT DESERIALIZATION IS

It is the opposite process, which means to, extract data structure or object from of bytes

LET ME GIVE YOU AN EXAMPLE

Zip and unzip

BUT HOW DESERIALIZATION IS VULNERABLE?

LET ME GIVE YOU AGAIN AN EXAMPLE

Suppose you are playing a game and you are stuck at somewhere level 5

So you have a saved game at level 5 and that file contains some info like your name, level, health, money etc.

And you change the file info by changing level 5 to level 6

And when you load the game with that respective file game starts from level 5 assuming you passed level 6

LET'S TALK IN CODING NOW

```php
<?php
class Place {

    public $one = "Bangladesh";
    public $two = "Rajasthan";
    public $three = "Delhi";

}

$obj=new Place;

$ser = serialize($obj);
echo $ser;
```

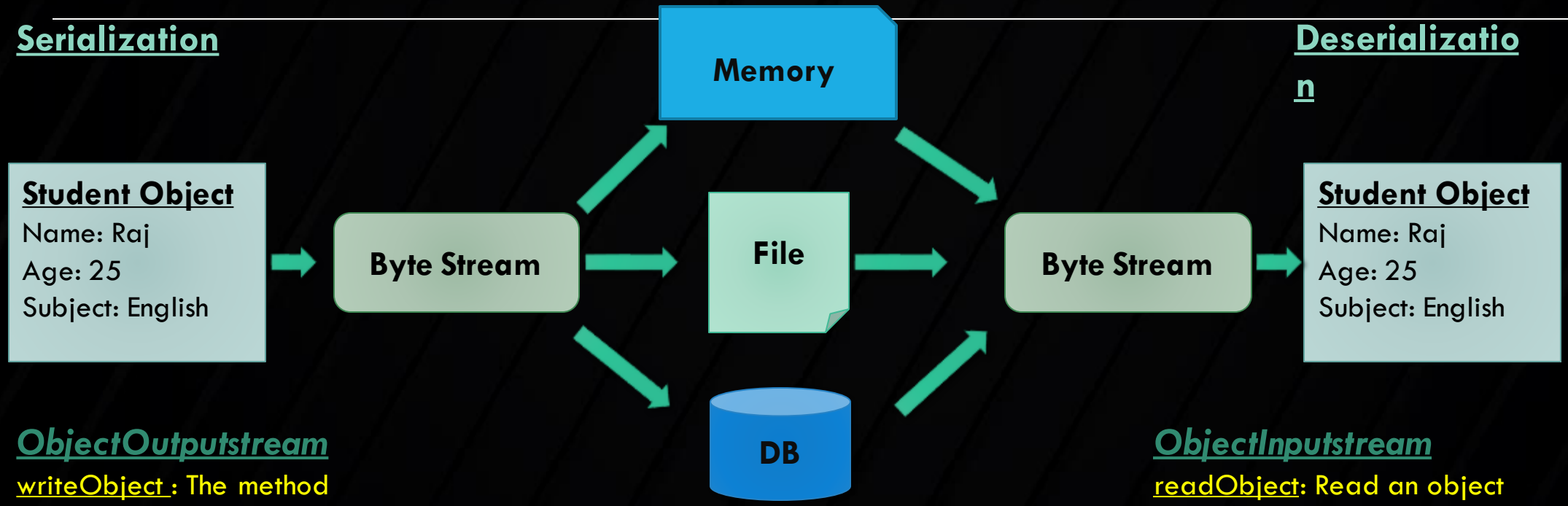
Reference to understand this serial values https://www.php.net/manual/en/function.serialize.php

```
O:5:"Place":3:{s:3:"one";s:10:"Bangladesh";s:3:"two";s:9:"Rajasthan";s:5:"three";s:5:"Delhi";}
```

SERIALIZATION IN JAVA

Serialization

Deserialization



ObjectOutputstream

writeObject : The method writeObject is used to write an object to the stream

ObjectInputstream

readObject: Read an object from the ObjectInputStream.

ReadObject it is the vulnerable method that leads to deserialization vulnerability

SERIALIZATION IN JAVA

```
@POST
public String renderUser(HttpServletRequest request) {
    ObjectInputStream ois = new ObjectInputStream(
        request.getInputStream());
User user = (User) ois.readObject();
return user.render();

}
```

Represents a web application with a classic Java deserialization vulnerability.

```
public class User implements Serializable {
    private String name;
    public String render() {
        return name;
    }
}
```

Implementation of the User class looks something like this.

```
public class ThumbnailUser extends User {
    private File thumbnail;
    public String render() {
        return Files.read  (thumbnail);
    }
}
```

Attacker changes the Type discriminator ***User*** to **ThumbnailUser.**
Then when the application calls render() on the object the contents of any file on the filesystem may be reflected to the attacker.

1 IMP THING U SHOULD KNOW

If you are able to find a deserialization in java application and if it has a vulnerable java library there are high chances you can use this to directly execute commands

LET'S CHECK OUT THOSE VULNERABLE JAVA LIBRARY

VULNERABLE JAVA LIBRARY

Commons collections

Spring Framework

Groovy

Apache Commons Fileupload<= 1.3.1

Spring1

Hibernate1

Jython1

HOW TO IDENTIFY JAVA SERIALIZED OBJECT

AC ED 00 05 in Hex

rO0 in Base64

Content-type header of an HTTP response set to application/x-java-serialized-object

LET'S CHECK OUT OWASP CHEAT SHEET

https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html

THANK YOU

Motivated by - @m0nkeyshell