10 - Module - Serialization

Serialization: storing objects in a sequence of bytes in a reversible way to either transport the data to another program or store it in the pc
Serialization = pickle = marshalling

Note: that serialization might not only be present on the web application layer.

Serialization in Java

Understanding the process

-> Firstly we will create a serialized object to understand the process. we need **javac** to compile the source code.

-> Notice that the file name should be the same as the name of the class inside that file; this is a common practice when
coding in Java.

14- 29

-> The file begins with the `ac ed 00 05` bytes, which is a standard java serialized format signature

-> As java serialized data is in binary format, when used in web applications, it is often encoded using Base64 in order to mitigate non-ASCII bytes. So look for string that begins with `rO0AB`

30-31 not understood!!!!!
gadgets: https://frohoff.github.io/appseccali-marshalling-pickles/

ysoserial tool to perform exploitation of insecure java deserialization vulnerabilities by generating java deserialization payloads

> `java -jar ysoserial..jar CommonCollections1 "whoami"`

The command above generates a serialized payload.

Burpsuit plugings: **Java Deserialization Scanner** & **Freddy, Deserialization Bug Finder**

(29-87 read from the slides)

---

exploiting Java Deserialization Resources:

https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet https://github.com/Coalfire-Research/java-deserialization-exploits

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Insecure Deserialization/Java.md

https://nickbloor.co.uk/2017/08/13/attacking-java-deserialization/

Serialization in PHP

87-106

abusing control over PHP serialized objects is also called „**PHP Object Injection**”
-> It is like Java deserialization, when the user has control over a PHP serialized object that is being sent to another deserializing endpoint.
-> PHP uses the **serialize()** and functions to perform serialization.
-> Unlike Java, PHP Serialization is in non-binary format, looks similar to a JSON array and it is human-readable.
`O:6:„Abcdef":1:{s:9:„Something";s:6:"Active";}`

https://www.phpinternalsbook.com/php5/classes_objects/serialization.html

https://www.geeksforgeeks.org/php-serializing-data/

How to exploit

It is not easy, because there is no ysoserial for php.

Exploitation of such a vulnerability was possible because:

.NET Serialization

108-146

https://github.com/nccgroup/VulnerableDotNetHTTPRemoting/

find an exploit .net remoting over http using deserialization

117 continue