Insecure Deserialization

> Serialization is the process of turning some object into a data format that can be restored later. People often serialize objects in order to save them to storage, or to send as part of communications. Deserialization is the reverse of that process -- taking data structured from some format, and rebuilding it into an object - OWASP

Check the following sub-sections, located in other files :

- Java deserialization : ysoserial, ...
- PHP (Object injection) : phpggc, ...
- Ruby : universal rce gadget, ...
- Python : pickle, ...

References

- Github - ysoserial
- Github - ysoserial.net
- Java-Deserialization-Cheat-Sheet - GrrrDog
- Understanding & practicing java deserialization exploits
- How i found a 1500$ worth Deserialization vulnerability - @D0rkerDevil
- Misconfigured JSF ViewStates can lead to severe RCE vulnerabilities - 14 Aug 2017, Peter Stöckli
- PHP Object Injection - OWASP
- PHP Object Injection - Thin Ba Shane
- PHP unserialize
- PHP Generic Gadget - ambionics security
- RUBY 2.X UNIVERSAL RCE DESERIALIZATION GADGET CHAIN - elttam, Luke Jahnke
- Java Deserialization in manager.paypal.com by Michael Stepankin
- Instagram's Million Dollar Bug by Wesley Wineberg
- Ruby Cookie Deserialization RCE on facebooksearch.algolia.com by Michiel Prins (michiel)
- Java deserialization by meals
- Diving into unserialize() - Sep 19- Vickie Li
- .NET Gadgets by Alvaro Muñoz (@pwntester) & OleksandrMirosh
- ExploitDB Introduction