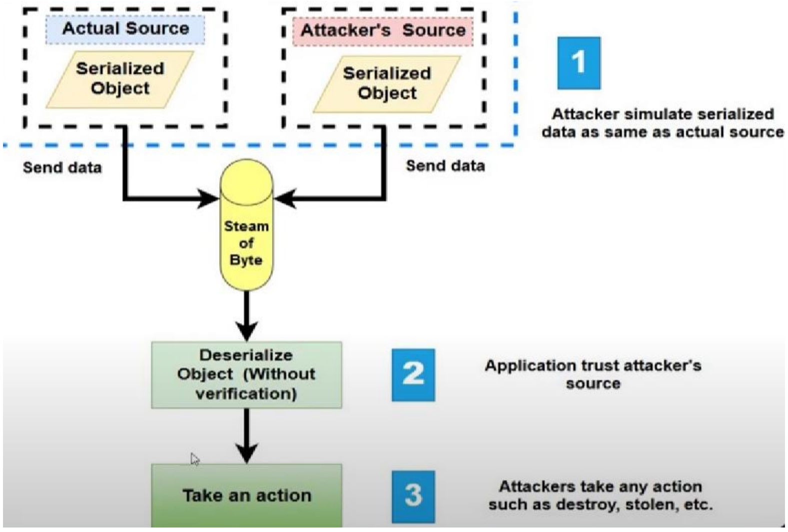
As we know that all the functions and variables must be travelled from one device to another to communicate or send get respective responses and requests they will be converted to JSON,XML or any other this concept is called serialization.
After receiving at another device the serialized data must be converted in to same functions or variables this process is called de-serialisation.
In this deserialization process attackers use advantage of it like if ay developer blindly trust the data user input’s data, there’s a high chance that attacker could win by executing malicious things which results in privilege escalation or command execution.

Exactly how does it works


Actual Source
Serialized Object
Attacker's Source
Serialized Object
1
Attacker simulate serialized data as same as actual source
Send data
Send data
Steam of Byte
Deserialize Object (Without verification)
2
Application trust attacker's source
Take an action
3
Attackers take any action such as destroy, stolen, etc.

for example we have data like this

```
$Site->Name =”cybersecurity”;
$Site->ISPOPULAR=TRUE;
```

Then it’ll be converted/serialized to like this

```
->O:4:”Site”:2:{s:4:”NAME”:S:15:”CYBERSECURITY;s:9:”ISPOPULAR”:B:1}
```

Magic Methods(PHP):
They override PHP’s default’s action when certain actions are performed on an object.

__CONSTURCT

__SLEEP

__WAKEUP

__TOSTRING

Dangerous if methods contain attacker-controlled Data.
Look for word unserialize

PHPGCC -> ./PHPGGC MONOLOG?RCE1 PASSTHRU ‘PHPINFO()’

```
Function SGIMPORTANTPOPUPS()
{
GLOBAL $WPDB;

$URL = $_POST[‘ATTACHMENTURL’];
$CONTENTS = UNSERIALIZE(BASE64_DECODE(FILE_GET_CONTENTS($URL)));
}
```

PHPGGC is tool. Useful tool

For python pickle is used for serialixation and deserialization.
pickletools. Object._reduce_()