Insecure Direct Object References Prevention

CYBER SECURITY &
PRIVACY FOUNDATION

Indirect Object Reference

- Avoid direct object references
- **Indirect Object Reference:** For each objects, create another identifier in the server side script and access those object with this ID.
- For Example:

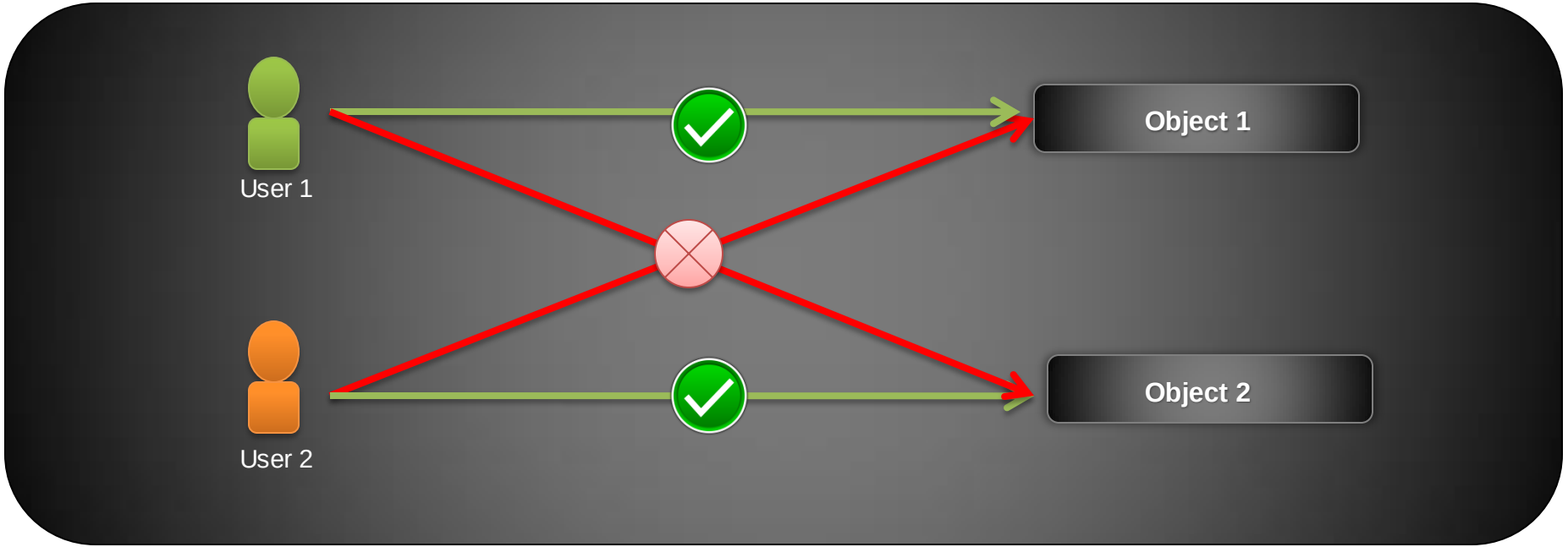
File	Indirect Object Reference
Document.pdf	1d767038b11a85509df00890f855df8a72ac4646
Reader.pdf	2a060be5017071c54ed9674ac87d580556bfd1f1
Subscribe.pdf	b8f64ac1caf839ced46187ab589e640d54b453ec

Example PHP Code

```php
<?php
...
$inref=doFilter($_GET['ref']);
$sql="select * from movies where id=:Indirect";
$stmt=$db->prepare($sql);
$stmt->bindParam(":Indirect",$inref);
$stmt->execute();
$result=$stmt->fetch();
if($stmt->rowcount() >0)
{
    $filename=$row["directobjectreference"];
    Download($filename);
}
else
{
    echo "File not found";
}
...
?>
```

Data Access control

- Make sure the user is authorized to access the requested object before allowing them to access it.



Example PHP Code

```
$num=doFilter($_GET['accountno']);
$userId=$_SESSION['userid']; //Get the User ID from SESSION
$sql="select * from movies where accountno=:num and user=:UserID";
$stmt=$db->prepare($sql);
$stmt->bindParam(":num",$num);
$stmt->bindParam(":UserID",$userId);
$stmt->execute();
..
..
```