# Premature population Bypass

As the title advises, this bypass can happen when the backend pre-populate the session id before an actual login where instead the session id should be populated after a successful login!

## Identification

We can use as an example a login page that redirects you to **/profile.php** upon successful authentication. But if we fail the authentication we are redirected towards **/login.php?failed=1**

And it shows the username failed:

A login screen with a blue and pink box

Description automatically generated

This means that most likely the cookie assigned during the login process is prematurely populated:

A screenshot of a computer

Description automatically generated

We can double check that by removing the cookie from the request and see that now the name is no more parsed which denotes the information is saved into SESSID cookie:

A screenshot of a computer

Description automatically generated

1. Now the solution here is to get the cookie we get from the first login attempt with non-valid credentials:

A screenshot of a computer

Description automatically generated

1. Next we use the cookie from first step in the following successful request **/login.php?success=1** to tell the backend to allow the redirect and this is a “successful login” (OBS: this is taken from a successful login process with a legit user)

A screenshot of a computer

Description automatically generated

1. Lasty by using same cookie again from step 1 we should be able to unveil the flag and login as ADMIN where we successfully bypassed the AUTH process.

A screenshot of a computer

Description automatically generated

OBS: This attack can be used only when the backend pre-populates the cookie to show the username warning, but it only gets cleaned up after successful redirect.

This can be caught as we showed via Burp and used to perform a login bypass!

This is the wrong code used:

<SNIP>

if(isset($\_POST['Submit'])){

$\_SESSION['Username'] = $\_POST['Username'];

$\_SESSION['Active'] = true;

// check user credentials

if(login($Username, $\_POST['Password'])) {

header("Location: profile.php");

exit;

} else {

header("Location: login.php?failed=1");

exit;

}

}

if (isset($\_GET['failed'])) {

session\_destroy();

session\_start();

}

<SNIP>