# Bypass Security Questions

This attack happens when you can bypass security questions that involves several steps and if the information is stored into SESSID then you can use that to bypass authentication processes

# Attack Scenario

Take as an example a register page form where on the first part you can add infos like username, password, desc, security questions etc:

A screenshot of a computer

Description automatically generated

This redirects to the second page as “approval”:

A screenshot of a computer

Description automatically generated

And if we proceed to register, we will get an error message telling us that the user exists already, but if we remove the cookie, we get the message to pass by step 1:

A screenshot of a computer

Description automatically generated

This means that the information of the user to be registered are temporally stored into session cookie.

The idea then is to use that cookie to login and grab the flag as admin user:

A screenshot of a computer

Description automatically generated

**OBS: This happens when the same cookie is used for login/register function!**

<SNIP>

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

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

header("Location: reset\_2.php");

exit;

}

<SNIP>

**And same for login:**

<SNIP>

if(!isset($\_SESSION['Username'])){

header("Location: login.php");

exit;

}

<SNIP>