# Complex Bypass of Security Questions

Let’s take as an example a possible real-life scenario where you identify that the password reset function might be used for bypassing the authentication method and perform a account takeover of a sensitive administrator.

## Identify

You identified that the reset process is composed of 3 steps to be done in succession and every step holds the information in the session cookie (by removing the session cookie it forces you to the step before).

1. **First phase: Provide the username**
2. **Second phase: Answer the security question**
3. **Third phase: Reset the password**

Now the first step can we do it, the second no as we don’t know the admin secret answers but the third we can as we can choose our password and send the actual reset process!

## Attack

The issue arises when the same session cookie is re-used between 2 dirrerent functions like reset &register. If so then we can do these steps to bypass the auth process:

1. **Do the first phase of the password reset process for the admin account**
2. **Complete phases 1&2 of the registration process, marking phases 1&2 complete in our session**
3. **Access /reset\_3.php to set the password of the admin account**
4. First, we perform the first step 1 of the reset process (choose the victim to reset its password):

A screenshot of a computer

Description automatically generated

1. Next, we perform the step 1 of register a new user (info of new user like username/password etc):

A screenshot of a computer

Description automatically generated

1. Next, we perform step 2 of the registration of a new user (phone & address):´

A screenshot of a computer

Description automatically generated

4)Lastly, use the cookie from step 3 to perform a password reset and actuall bypass the step 2(security question) over password reset process:

A screenshot of a computer

Description automatically generated