LOGIC FLAWS

Thursday, February 6, 2020 11:58 PM

REMEMBER ME

1.In this the application pass a cookie that contain info so that next time it does not need password but it is highly encripted.

EXPLOITATION

2.Find the function in application which pass the data which is encriptaed or nonreadable and displaying input.try to manupulate that to decrypt that cookie.

RESET PASSWORD FUNCTIONALITY

1.Try to remove every parameter included cookie,post data ,variables. One at a time and check the respond
2.don't give existing password in change password functionality and try to execute it.

MULTISTAGE FUNCTION

1.In multistage functions try to skip stages and manupulate applications business logic.use forced browsing to do so.

PARAMETER EXPLOITAION

1.Try to manupulate input like xss etc.
2.then try parameter pollution
3.in multistage function give a additional parameter that was previously used to changed its value.

ALTERING THE LIMITS

1.Try to give negative digits and analise the response.
2.Move furture and check to enumerate and exploit it so make a use out of it.