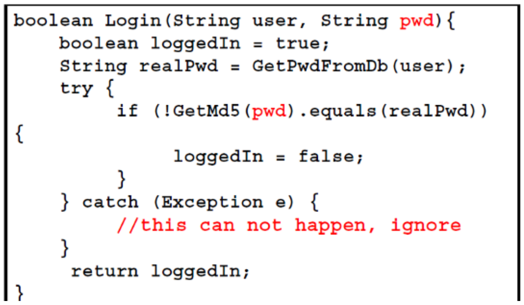
Active Learning Activity: Secure Coding Practices

ECE 60872/CS 59000 – Fault Tolerant Computer System Design
School of Electrical and Computer Engineering
Purdue University
Fall 2018

What are possible vulnerabilities in this code fragment that is supposed to check for correct login?



```
boolean Login(String user, String pwd){
    boolean loggedIn = true;
    String realPwd = GetPwdFromDb(user);
    try {
         if (!GetMd5(pwd).equals(realPwd))
{
              loggedIn = false;
         }
    } catch (Exception e) {
         //this can not happen, ignore
    }
     return loggedIn;
}
```

10/15/18

Secure Coding ALA

1. Set logged In = false at init.
Make changes in rest of code accordingly.
2. Input validation.

3. GetPwd fromDb within ~~Get~~ equals.
Reduces window of vulnerability.
within try, catch block.

4. Set realPwd to null quickly after use to reduce chance of information leakage.