

java代码审计 深度解析





第二课 修改密码

PART 01

逻辑漏洞

4



逻辑漏洞

逻辑漏洞是一种业务逻辑上的设计缺陷，业务流存在问题。

这里说一下密码找回漏洞、多线程条件竞争漏洞和支付漏洞。



逻辑漏洞-任意修改密码

```
//判断用户密码和原采的密码是否一样
public String findUserByPwdAndUserName(){
    HttpServletResponse response = ServletActionContext.getResponse();
    //设置字符集
    response.setContentType("text/plain");//设置输出为文字流
    response.setCharacterEncoding("UTF-8");
    user = userService.findUserById(userid);
    String responseText="";
    if(password==null||password.trim().length()<1){
        responseText="2";
    }
    else{
        if(user.getPassword().equals(new MD5().MD5Encode(password))){
            try {
                response.getWriter().println("0");
            } catch (IOException e) {
                // TODO Auto-generated catch block
                e.printStackTrace();
            }
        }
        else{
            try {
                response.getWriter().println("1");
            } catch (IOException e) {
                // TODO Auto-generated catch block
            }
        }
    }
}
```



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. It includes a glowing globe on the right side, overlaid with a network of white and blue lines and dots. Scattered throughout the background are several padlock icons, some of which are open, suggesting themes of security, hacking, or digital access. The overall aesthetic is futuristic and tech-oriented.

谢谢观赏