

Code Quality

Chủ ý của bài tập lần này nói về việc phát hiện các manh mối, thông tin ẩn mà những nhà phát triển website đôi khi để lại trong lúc xây dựng web. Các nhà phát triển nổi tiếng với việc để lại các câu như FIXME's, TODO's, Code Broken, Hack, v.v... bên trong mã nguồn nhằm cho những người phát triển sau này, hoặc cho những người khác biết được thứ cần lưu ý.

Developers are notorious for leaving statements like FIXME's, TODO's, Code Broken, Hack, etc... inside the source code. Review the source code for any comments denoting passwords, backdoors, or something doesn't work right. Below is an example of a forms based authentication form. Look for clues to help you log in.

Sign In
Please sign in to your account. See the OWASP admin if you do not have an account.

*Required Fields

*User Name :

*Password :

Bài tập yêu cầu ta tìm ra một tài khoản bị nhà phát triển bỏ lỡ đâu đó trong tài nguyên website, và dùng nó để đăng nhập.

Thường thì các tài nguyên như này người phát triển sẽ nhúng chúng bằng việc comment, vì vậy nội dung bị ẩn đi. View source code và tìm các comment của website đôi khi sẽ thấy một số thứ thú vị.

```
source code for <!-- 3/4 ^ v X backdoors, or some  
  
ndow</a>  
  
&nbsp;Review the source code for any comments denoting&nbsp; passwords, ba  
  
'><!-- FIXME admin:adminpw --><!-- Use Admin to regenerate database -->
```

Nó đây, dùng nó để submit bài tập thôi.

*** Congratulations. You have successfully completed this lesson.**
*** BINGO -- admin authenticated**

Welcome, admin

You have been authenticated with CREDENTIALS