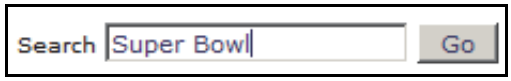
5 Cross-site scripting exercises

You can use cross-site scripting attacks to access sensitive information such as user session cookies. In this exercise, you determine whether the site is susceptible to attack, use a script to get access to cookies, and determine how this type of attack can be used to retrieve another user's cookies.

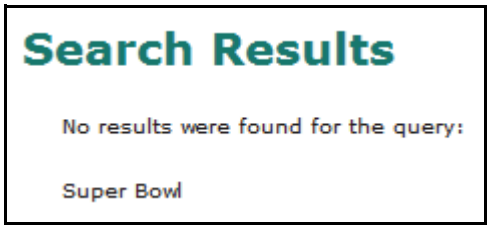
Exercise 1 Steal the user cookie

Determine the best attack method

1. Open the Firefox web browser.
2. Type the URL `demo.testfire.net`.
3. In the **Search** field, type `Super Bowl`.



4. Click **Go** and review the returned results.



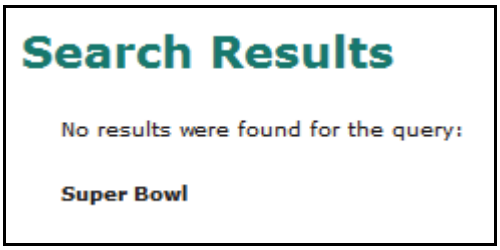
Attackers profile a site to learn how users interact with the application and how the application reacts to user input. In this probe, you learn the search string, *Super Bowl*, is reflected on the page.

Find the application vulnerability

5. In the **Search** field, type `<B>Super Bowl</B>`.

Note: <B></B> are the HTML tags that tell the browser to render the enclosed string in bold.

6. Click **Go** and review the returned results.



Because *Super Bowl* displays in bold, you know that the browser processed the tags instead of displaying them. Now the attacker can try something more complex.

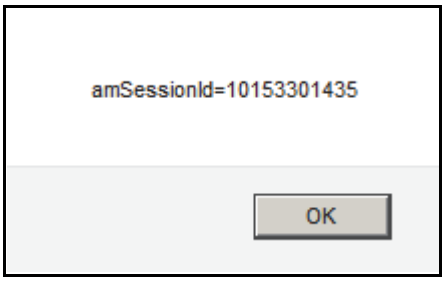
- If you see only *Super Bowl* rendered in bold without the tags, you know that the application is not properly handling the HTML tags entered because the application echoed them back without encoding them.
- If the application renders *<B>Super Bowl</B>* as is, the application is not susceptible to cross-site scripting, because it neutralized the HTML meta characters to properly display them just as the user entered them.

7. To try a more complex search using a test script, perform the following steps:
   a. In the **Search** field, type `<script>alert(1)</script>`.
   b. Click **Go** and review the returned results.

You learn that the output is not encoded and the browser processed the script tag.

   c. To close the alert window, click **OK**.

8. To use the same approach but access the cookie container, perform the following steps:
   a. In the **Search** field, type `<script>alert(document.cookie)</script>`.
   b. Click **Go** and review the returned results.



You learn that the cookie is available to JavaScript.

Note:

- Your cookie data might have a different value than the screen capture.
- JavaScript is a language most browsers can run.

   c. Click **OK** to close the alert window.

9. If time permits, try other scripts to perform the following tasks:
   - Open a window
   - Embed a frame
   - Link to an image from outside the application