# XSS Bug

Reported from the Cyber Engineer

Thanks for submitting a report!

Summary: [Reflected cross-site scripting (or XSS) arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way.

Suppose a website has a search function which receives the user-supplied search term in a URL parameter:

https://insecure-website.com/search?term=gift

The application echoes the supplied search term in the response to this URL:

<p>You searched for: gift</p>

Assuming the application doesn't perform any other processing of the data, an attacker can construct an attack like this:

https://insecure-website.com/status?message=<script>/\*+Bad+stuff+here...+\*/</script>

This URL results in the following response:

<p>You searched for: <script>/\* Bad stuff here... \*/</script></p>

If another user of the application requests the attacker's URL, then the script supplied by the attacker will execute in the victim user's browser, in the context of their session with the application.].

App Version: [ version 1.1.1]

App OS: [Windose,Unixs,Linux]

Steps to reproduce:

1. open github
2. run code in the compiler
3. check if all scripting and value and the return value is true
4. check all of the Url , and then return value of them
5. try injecting script in the all text box
6. and then can make a decision in Shaw close vulnerabilities if there are

As you can see, this template makes it clear what information the hacker is expected to submit.

Solution:   
can solve the problem two ways:

1. User Validation (filtering) for any input and request coming of the user

* Pros (Validation)   
  don't need to change constantly
* Cons(Validation)  
    
  The more it gets of function for Validation, reducing performance.

1. using AntiXss library in Java

* Pros (AntiXss library)   
  easy to use easy, Deal with it.
* Cons((AntiXss library)  
   when Appearance of a new type of XSS bugs It may take a long time to update the library

we prefer 1 over 2 ....  
  
  
  
  
Best,