INITIAL POST

One of the top 10 weaknesses identified by OWASP is Cross Site Scripting – XSS (A7), described below-

As an example of an injection attack, cross-site scripting (XSS) attacks include the introduction of malicious scripts into otherwise safe and trustworthy websites. When an attacker exploits a vulnerability in an online application, they can launch a cross-site scripting (XSS) attack on another user.

If a Cross-Site Scripting exploit is successful, it can be used to steal cookies, impersonate a legitimate user, access private data, or even run malicious malware on the victim's computer.

There are multiple types of XSS – Reflected, DOM & Stored XSS

(A7-XSS, 2017)

It can be prevented by sanitizing and validating user input. (Ben Lutkevich, N.D)

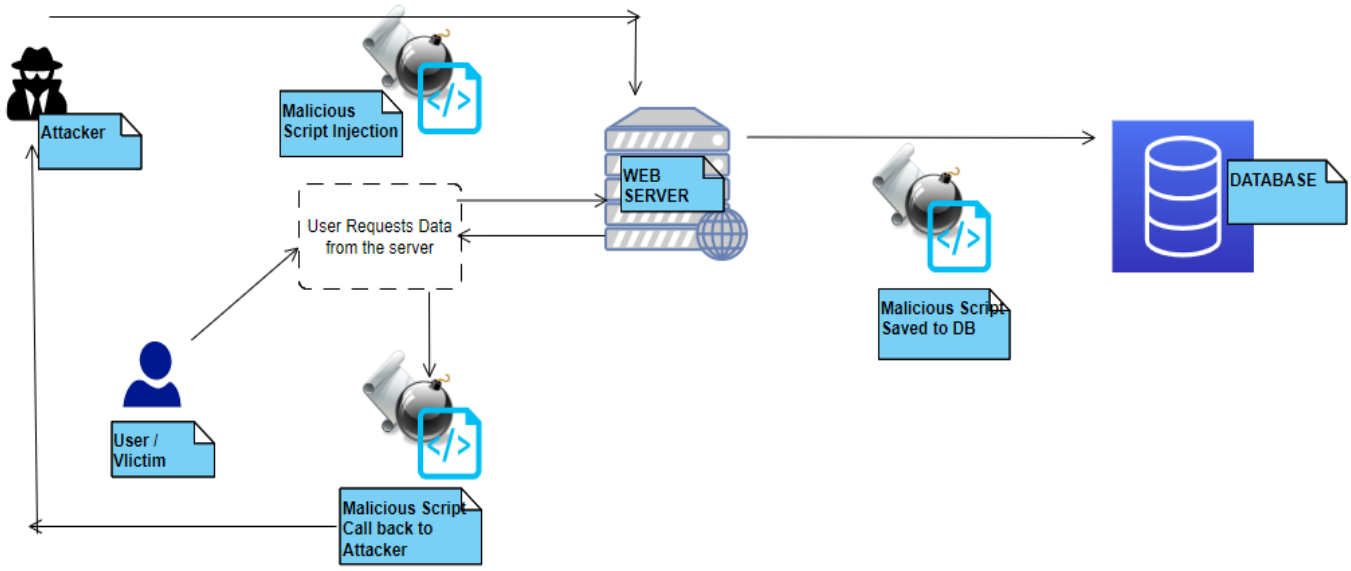
The following UML types, among others, might be used to describe this OWASP vulnerability:

Activity: The activity diagram is a visual representation of the process flow within a system. These diagrams, which resemble flowcharts, display the results of each action and the consequences of various replies.

Sequence:

When it comes to visualizing the interplay between objects, sequence diagrams fall under the category of "interaction diagrams," and their primary focus is on the periodic or chronological aspects of that interplay.

UML diagram representation for XSS:



References:

1. A7: Cross-Site Scripting (XSS) [2017]

   https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

2. Ben Lutkevich [N.D.]
   https://www.techtarget.com/searchsecurity/definition/cross-site-scripting