XSS Vulnerabilities

Cross-site scripting vulnerability abbreviated as XSS is a kind of common injection web vulnerability. The exploitation of XSS vulnerabilities can hijack users sessions, modify, read and delete business data of web applications, place malicious codes in web applications, and control victims to attack other targeted servers.

XSS detection is divided into three categories according to different mechanisms they are:

1. static analysis methods
   The method is implemented as a tool called deDacota that can be applied to ASP.NET web applications.

2. dynamic analysis methods
   Lekies et al. (2013) presented a fully automated system to detect and validate DOM-based XSS vulnerabilities. The system consists of two main components: a modified browsing engine and a fully automated vulnerability validation mechanism

3. hybrid analysis methods
   Patil and Patil (2015) proposed a sanitizer with detecting XSS vulnerabilities. There are plenty of modules in the system architecture.

Although there are many methods to detect XSS vulnerabilities, it is still a very difficult task to detect all XSS vulnerabilities in one web application. This is mainly because the size of web applications is becoming larger, and the calling logic among modules is also becoming more complicated. In addition, various technologies such as code confusion and dynamic code generation further hinder the detection of XSS vulnerabilities.

Source:
https://ieeexplore.ieee.org/Xplore/home.jsp
https://ieeexplore.ieee.org/document/8935148