Cross-Site Request Forgery (CSRF) and Server-side Request Forgery (SSRF) are two types of malicious attacks on web applications. Both these vulnerabilities take advantage of how a web server handles the URLs. However, both vary in their purposes and the target of the attack.

CSRF attack forces users to carry out unwanted actions in a web application they are currently using. On the other hand, SSRF is a web security vulnerability where an attacker induces server-side application and makes HTTP requests to an arbitrary domain of their choice.

Let’s look at the basic differences between the two.

## Target of Attack

Both CSRF and SSRF exploit the web server. However, SSRF is designed for attacking the target, which is primarily the server. It may affect the users of a service in the long run, but its primary purpose is to steal sensitive information lying on the server or to exploit other vulnerabilities by bypassing countermeasures of input validation.

Conversely, CSRF targets the users. It does that by exploiting flaws in the design of a web application. The purpose of CSRF attack is to carry out legitimate but unauthorised action on a user account with the web service.

## Purpose of Attack

Both attacks also differ in their purposes. For SSRF, the main purpose of attack is gaining access to critical information. A cybercriminal does this either directly (by making the user write the data on a malicious URL), or indirectly, such as by exploiting a vulnerability that can assist in stealing the data.

On the other hand, CSRF vulnerability does not allow the attacker to access sensitive data. The attacker makes the browser of the user visit a targeted site. However, the actual request to do so and the response are carried out separately. If in case the sensitive data is sent as a result of a malicious request, it goes to the user’s computer, and not the attacker’s. The main purpose of the CSRF vulnerability is forcing a user to take action according to how the attacker wants, such as changing the password to one that is known to the hacker.

## How to Detect CSRF and SSRF Vulnerabilities?

While both CSRF and SSRF are different vulnerabilities, they are exploited by same problem i.e. the server’s failure to use URLs properly. Both vulnerabilities can be identified in a web application by examining how it uses URLs along with the format, destinations, and types of requests made.

For detailed penetration testing services of your web application, get in touch with Aardwolf Security today and get a free quote.