Committing blunders is a part of human nature, but it is essential to highlight and omit those mistakes. While running a web vulnerability assessment, you may commit some common mistakes.

## 1.Fail to take everyone on board

It is vital to have every team member on board while performing the vulnerability assessment. A prevalent mistake is when you assume that everyone complies with what you are doing. The first step to a perfect start is by having the right people.

## 2. Unjust resource allocation

Understandably, you want to allocate the highest amount of resources to the most critical web application. However, it is a big mistake to skip minor applications. A web vulnerability assessment is for detecting errors in every application that can be a problem source.

## 3. Injection flaws

If you are unable to filter untrusted inputs, then you are facing injection flaws. It is a very classical failure in which you pass the unfiltered data to SQL servers.

## 4. Cross-site scripting (XSS)

It is an input sanitization failure. The intruder or hacker gives your web application JavaScript tags on the input. Therefore, when this un-sanitized input reaches the user browser, it will execute it.

## 5. Unaware of tools

Web vulnerability assessment is made easy with the help of automated tools. However, it requires the right technician to operate them. A person who is unaware of these tools will further complicate the whole process of testing.

## 6. Relying on third party application

Another common web vulnerability assessment mistake is when you rely on a third-party application to secure your web. These threats can increase if you are dealing with a cloud servicing and hosting provider.

## 7. Insecure direct object reference

Direct object references are internal objects such as a file or database key. If you expose this direct object reference, then the attacker can misuse it for authorization. In short, it is a common mistake to trust user input in web vulnerability assessment.

## 8. Compliant web

Another common assumption and mistake are that organizations believe that a secure web is a compliant web. The problem exists vice versa as well. You need to properly ensure the security of your web by protecting your web assets.

## 9. Unable to understand it's the importance

It is a blunder on the management part when they assume that the company will realize the importance of web vulnerability assessment tests. It is not only essential to identify vulnerabilities; you also need to put stress on their impact.

## 10. No follow-up

Lastly, the most common mistake is that companies do not keep a follow-up of their web security after web vulnerability assessment. It is prudent that you regularly monitor your web application to avoid any severe problems.

## Conclusion

When everything is moving on the internet, you must make your web security. To ensure your web application assessment's best results, you should try to avoid the mistakes mentioned above.