# **Lesson 6:** **Various vulnerabilities and Precautions**

One of the biggest fears for development managers is not identifying a vulnerability in their web application before an attacker finds it. Web application vulnerabilities leave you susceptible to security attacks during which valuable customer and company data could be at risk. As a result, you will incur huge financial losses while your reputation suffers serious damage.

The good news is that these web application security threats are preventable. roper knowledge of the most common web application vulnerabilities is the key to prevention. While you may conduct [automated scans](https://www.cypressdatadefense.com/blog/2018-3-28-are-automated-scans-enough/) and regularly test for any web application vulnerabilities, those efforts will be in vain unless you know what to look for.

This makes it crucial to understand web security vulnerabilities inside out – right from how a web application gets targeted to what kind of vulnerabilities to look for and how to prevent them. This post is going to help you do exactly that.

## **How Web Application Vulnerabilities Affect Companies**

First, let’s try to gain a better understanding of how exactly these website application vulnerabilities can affect a company. This will help you understand just how harmful these security attacks can be and why you should prioritize preventing them.

One of the biggest, most harmful web application security threats is sensitive data exposure. It even ranks among the [OWASP top 10 vulnerabilities](https://www.cypressdatadefense.com/resources/open-web-application-security-project-owasp-top-10-vulnerabilities/). It involves compromising important data that should have been protected. This includes data like passwords, credentials, personally identifiable information, social security numbers, credit card numbers, health information, etc.

This is one of the most targeted web application vulnerabilities by hackers since there’s a prospect for financial gain for them. They could sell this data or use it themselves to conduct fraud, identity theft, etc.

There are tons of ways for hackers to steal sensitive data through web security vulnerabilities:

* They may look for  SQL injection flaws to retrieve decrypted credit card numbers.
* They could exploit insecure wireless networks to seal a user’s session cookie.
* Attackers could even retrieve sensitive files from the server using a file download vulnerability, or upload malicious files to target your users!

In some cases, you may even encounter Cross-Site Scripting (XSS). This is one of the most widespread website application vulnerabilities and involves utilizing the website as a propagation method. Hackers would inject malicious client-side scripts and modify how the website functions or how it is displayed.

An XSS attack could infect your visitors’ devices with malware or have them recruited into large botnets. It could mislead your visitors and damage your credibility and reputation, which can be extremely difficult to rebuild.

These are just a few ways in which hackers can exploit web application vulnerabilities and cause serious harm to your company and its customers. But even from this, you can clearly see just how damaging these attacks can be and how crucial it is to prevent them. We need to take web application security threats seriously and turn our development teams into security champions.