VERACODE

Whitepaper

Web Application and API Security Best Practices

Table of Contents

Web App and API Security Overview

In today's interconnected world, the security of web applications and APIs is critical to protect sensitive information and ensure the integrity of online interactions. As organizations increasingly rely on web-based platforms to deliver services and share data, the vulnerabilities associated with these technologies become more complex and pronounced.

In this white paper, we dive into the dynamic landscape of cybersecurity, offering a comprehensive exploration of the latest strategies and methodologies designed to protect web applications and APIs against evolving threats. From best practices to automated security testing, this document discusses practical steps you can take today to build and maintain secure web applications and APIs in the face of an ever-expanding cyber threat landscape.

Making Security a Priority

Every company should consider security as a foundation for the survival of the business[4]. Therefore, it is particularly worrying that this issue is still not prioritized in almost half of organizations. As Amazon's VP & CTO said at the Bits & Pretzels conference. "Without security, you have no business!". This statement from a leading CTO supports the argument that insufficient security can put a company's customers, and therefore its entire business, at risk. Accordingly, security should have the same priority in both development and management as, for example, software functionality or customer service. If the developed functions contain security gaps, the company will lose customers and may even have to file for insolvency.

1.

Create and allocate resources

No company has endless resources available for a particular area. But in any case, the resources should be created to secure the company. Fixing a security vulnerability after it is found is ten times more expensive than securing it in advance. That's why it's crucial to create the budget, personnel, and IT infrastructure to maintain the integrity of your enterprise. However, companies that do not have the financial resources for full-time security experts should make at least one person responsible for IT security (e.g., the CIO or CTO). This way, every decision is double-checked to see how it impacts the security posture.

2.

Security starts from the top

When IT security is on the management's agenda, it ensures that the problem is anchored at the highest level in the company and is a high priority. The current security status should be discussed in weekly meetings and access to all departments at all times. As with any critical issue, proper management is essential to keep security in employees' minds at every decision.

3.

Matching the priorities of the divisions

Security should be a priority, but this does not mean that a you should devote all available resources. Enterprises should find sub-priorities and prioritize securing essential parts of the business. Not every company has the same data structure or the same systems. Therefore, this is not to be understood as a checklist but rather as a possible guideline on how a basic level of security can be created, which you can then build to suite your organization and priorities. A "threat analysis" can be helpful here, revealing which vulnerabilities should be treated with which priority. The main headings of this white paper can be used as starting points.

> "Without security you have no business!
>
> **Werner Vogels**
> VP & CTO Amazon

The Importance of Employee Security Education

According to surveys, negligence is the main cause for security incidents. Although this could be easily prevented, many enterprises still place too little emphasis on raising their employees' awareness of security issues. Especially for companies with valuable information and data, all employees must have sufficient knowledge regarding security[5].

1.0

A part of the corporate culture

Addressing the issue at the highest level in the company is essential but not sufficient if most employees are not aware in their daily work of the consequences that incorrect behavior can have for the company's security.

To ensure security is integrated into the culture, a security plan can outline what actions each employee can take to prevent hacking attacks.

Such an approach is critical if you plan to have your company ISO 27001 certified.

Every employee should know basic measures through the plan and apply them in their daily work.

As part of such a plan, password rules that all system users must follow can be implemented. We will show more examples in the next chapter.

In addition, the company's security status can be shown regularly in meetings using a dashboard to see the impact of their work on the company's security. By increasing awareness, you can ensure that the protection of the company's data is present in the mind of each employee.

1.1

Security coaching for employees

Although all beginnings are challenging, focusing on the little things can be sufficient. For example, requesting that personal computers be locked when not is use is a good place to start. It is easy to obtain internal company data if there is no encryption or protection. Another simple measure is to perform software updates whenever possible. Hackers use known vulnerabilities to get into systems. Updates usually include bug fixes and security enhancements that make life much harder for hackers.

For more specialized topics (e.g., phishing attacks), advanced training workshops are recommended. This allows employees to identify and report attacks early. A reward system for reporting vulnerabilities or attacks can be successful in motivating employees to address these issues. Special training courses on secure programming should be offered for employees who work directly on the IT infrastructure, especially software developers.

Establishing a Strong Password Policy

As mentioned earlier, rules about passwords should be integrated into your security plan. These rules should be applied not only by employees but by all users who have access to the system. There are a few things to keep in mind when passwords are created.

Passwords must be strong enough

Hackers have databases of passwords that are often used, so the security level increases significantly with the strength of a password. Experts recommend passwords that consist of at least 20 characters and contain special symbols so that hackers cannot easily crack them.

Specific passwords for each application

However, if a password is found out, hackers should not have immediate access to every user application. Therefore, to secure the entire IT infrastructure, specific passwords must be used for each application.

Passwords should be changed often

It is recommended that system users change their passwords every 30 to 60 days. A strong password with more than 20 characters will take hackers more than 60 days to decrypt. In addition, by changing passwords regularly, hackers have to start from scratch, and applications become more secure.

Password manager as an auxiliary tool

Strong and specific passwords are difficult to remember, and writing them down is not recommended. Password managers help to keep track of passwords, and users only need to remember one master password. However, this should then be strong enough to protect all others adequately.

Two-factor authentication for additional security

Two-factor authentication is an effective measure to provide an extra layer of security. Even if a hacker solves a user's password, the account must be unlocked, e.g., by an SMS code. However, this then requires a second device to. Add space between these two paragraphs inexpensive measures that every employee can take through password protection alone to secure the company's IT landscape.

Understanding Access Control for Users

The more users a system has, the more potential attack targets and vulnerabilities the system has through these users. Therefore, it is imperative to control which user has access to the system.

Introduction of user verification

The first step in securing data is to control who has access to it. Especially users from outside the company should be verified and monitored. Any input can be bad for security, and sufficient verification should be implemented for each user. The password basics described in Chapter 3 should apply to every user in the system.

Only the most necessary rights for all users

After verifying each user, it is vital to be as restrictive as possible with their rights. Officially, this measure is called the "Principle of Least Privilege." Users should be given as few rights ("Least Privileges") as possible at the beginning. Later, of course, main users and administrators can be given additional privileges. The division of responsibilities is another critical basis. In its report, the SANS Institute suggests that users should be divided into different roles.

Even top managers should only be able to see what they need for their work. This keeps corporate data as secure as possible and allows employees to focus on what they are working on. The number of primary users should be minimized, and even these users must be continuously monitored. They should serve as role models for other users, strictly adhering to IT security rules.

Steps to Integrate Security Testing into Your Development Workflows

All of the above measures can be easily integrated into your organization's systems to minimize the risk of vulnerabilities. However, it is clear that people always make mistakes, and even the developers' code can never guarantee complete security. One way to ensure that your development workflows are secure is with automated application security testing. Manual penetration tests are too expensive and time-consuming in agile software development, which uses continuous integration and deployments (see Fig. 1). In these forms of agile development, applications are developed and released in short cycles. Only automated tests can be used to test each version in this process, as manual tests for each new development stage would represent considerable time and financial effort. Existing vulnerabilities are found before a new software version is released. The latest version is released on time.

With Veracode Dynamic Analysis, you can leverage automated security testing in your development process to secure web applications earlier in the software development lifecycle.

Automated security testing allows developers to fix these problems directly. This gives them more time to develop the features that add real value to customers and create a competitive advantage for your business. In addition, by providing direct feedback on the current security posture of your web application and an integrated knowledge base, developers are helped to integrate secure programming into their daily workflow.

In addition, managers receive direct information about the company's security status through integrated dashboards and email reports after each application scan(s).

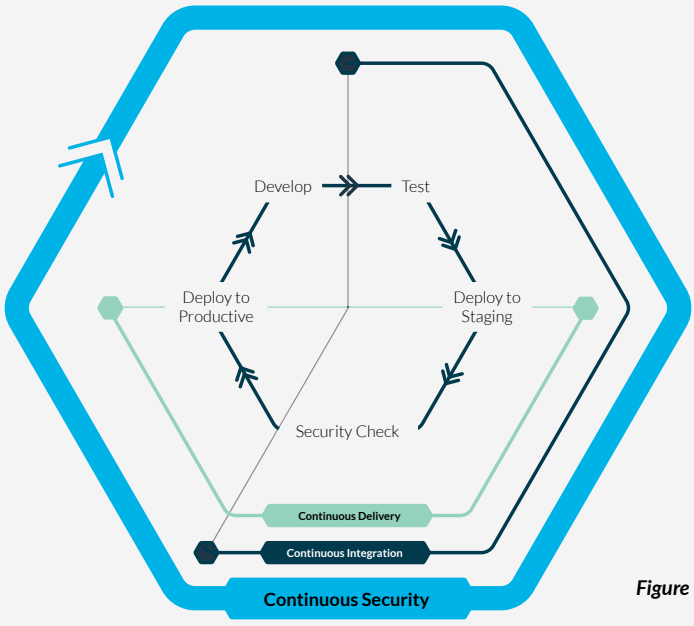

Figure 1: *Security in the Agile Development Environment*

Strengthen Your Web Applications and APIs Against Attack

The landscape of web application and API security is both intricate and dynamic, demanding a proactive and multifaceted approach to mitigate evolving threats. Below, we have summarized the key critical points.

- Web applications are always vulnerable to hacker attacks and always will be. How these vulnerabilities are addressed and avoided depends on management, developers, and each employee.
- Supporting and continuously training employees is crucial as they form the foundation of any company's security.
- The presence of a security culture within your company increases the likelihood of quickly identifying and addressing vulnerabilities.
- Automated security tests enable you to maintain a continuous overview of your security and take immediate action when necessary

Veracode can help you integrate automated security testing into your modern development workflows to proatively secure your web applications and APIs while promoting a secure coding culture. Sign up for a free trial to start scanning today.

Start Free Today

VERACODE

Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at **www.veracode.com**,
on the **Veracode blog** and on **Twitter.**