Web Application

Find and Address Application Security Flaws

SentryArk

Millions of people around the world depend on web apps to handle their most sensitive information, whether it be for financial planning or medical care. The rise of microservices and APIs while bringing immense benefits, have also made Web Applications much complex. With this complexity comes unforeseen Security risks and hackers are exploiting new methods every day to bend and break to make these applications.

As recent trends have revealed, a small fault in the application is enough for a breach and a single breach is enough for serious financial, reputational and/or operational losses to an organisation. A good way to prevent this is to assess the Application from the eyes of an attacker to uncover the flaws.

Application penetration testing does this exactly. By using the same techniques as sophisticated hackers, SentryArk's penetration tests target the entire range of vulnerabilities and provides visibility into the security risks of web apps and/or APIs.

APPLICATION TESTING BEYOND THE OWASP TOP 10

The OWASP Top 10 and it's testing methodology is generally accepted as the standard for identifying application's security flaws. It provides a great starting point for anyone looking to pen test and protect their application.

However, OWASP Top 10 isn't the exhaustive holy grail and not all vulnerabilities are included in the list. Automated vulnerability scanning, or penetration tests focused only on OWASP Top 10 will not provide the complete picture, leaving the application exposed to unknown risks. Instead Organisations should look beyond OWASP top 10 and prepare for a pent test program that is tailored for their application and not just standard procedures.

BUSINESS LOGIC TESTING

As the number of common vulnerabilities such as SQL Injection and Cross-Site Scripting are reduced, the bad guys are increasing their attacks on business logic flaws. Attackers don't need an exploit to abuse your Web application here, all they need is to identify a design weakness and take advantage of a business logic flaw and wreak havoc.

Abuse and exploitation of the business logic in an application is very common. However, they are the hardest to identify because they require both an understanding of the application and of security risks associated with it. Often, teams understand the business logic, but they aren't security experts and lack the expertise on clever attack techniques based on the business logic.

A good Pen Test program should include every business scenario to cover all possible abuses. This is unique for every application and teams should work closely in achieving complete coverage.

ASSESSMENT DETAILS AND METHODOLOGY

To ensure high quality and repeatable engagements, SentryArk's assessment methodology for applications is a combination of automated and manual processes that go beyond OWASP Top 10 and other standards. With greater emphasis on the context and business logic of the application, in addition to identifying technical flaws, The SentryArk methodology ensures application vulnerabilities are identified with the highest precision.

Planning and Information gathering

Penetration test begins with information gathering. Collecting, parsing, and correlation information on the target is key to identifying vulnerabilities.

Vulnerabillty Analysis

Once the target has been fully enumerated, SentryArk uses both vulnerability scanning tools and manual analysis to identify security flaws. With decades of experience and custom-built tools, our security engineers find weaknesses most automated scanners miss.

Exploitation

At this stage of the assessment, our consultants review all previous data to safely exploit identified vulnerabilities. Once sensitive access has been obtained, focus turns to escalation to identify total business impact

Risk Determination

In this phase Our consultants set an industry standard for clear and concise reports, prioritizing the high, medium and low risk vulnerabilities.

Reporting

Once the engagement is complete, SentryArk delivers a detailed analysis and threat report, including remediation steps.

The assessment includes the following:

- Executive Summary
- Strategic Strengths and Weaknesses
- Identified Vulnerabilities and Risk Ratings
- Detailed Risk Remediation Steps
- Assets and Data Compromised During Assessment

ABOUT SENTRYARK

SentryArk is a team of Security professionals, white-hat hackers and security enthusiasts seeking innovation in the Information security industry. We expertise and focus on providing offensive security solutions that help understand the real-world risks impacting your business. Our goal is to deliver top tier professional and innovative services and help organisations champion their cyber security initiatives.