Web Application Testing

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Don't Be A Target

According to the 2017 Contrast Security Research Project, 69% of web applications are plagued by vulnerabilities that could lead to sensitive data exposure. Applications are your most public exposure points and are at high risk of exposing sensitive information or allowing unauthorized access. These types of vulnerabilities may not be detected by standard vulnerability scanners, which is why our Web Application Testing involves scanning as well as manual exploitation to truly understand what a real-world attacker could access.

At a minimum, our testing is based on the Open Web Application Security Project (OWASP) Top 10 Web Application Risks. This helps you determine if your app is a target due to application-layer vulnerabilities such as cross-site scripting or injection attacks. The most common vulnerabilities that we find are cross-site scripting, SQL injection, and web server security misconfigurations, which are all included in the OWASP Top 10.

Stay On Deadline

If you have a new app you are planning to launch, it's imperative that you perform security testing before you set it live. We have the ability to work with your development team to ensure testing does not interfere with the application functionality or the work your team is doing. It is also considered best practice to perform a Web Application Test when changes are made to your application to ensure no new vulnerabilities are introduced.

Since you want your users to have extensive functionality and keep tight development deadlines, security of these applications is often overlooked. However, these applications typically have access to the most sensitive and important information in your organization - things like usernames, passwords, bank account information, protected patient information, and other sensitive data. Our Web Application Testing will find these security gaps and allow your team to continue developing features.

A Web Application Test Gives You:

- **Vulnerability scanning of application(s)**
- **Manual exploitation of vulnerabilities**
- **A comprehensive report including actionable recommendations**

Frequently Asked Questions

What are the key things you're looking for?
At a minimum, we are looking for the OWASP Top 10 web application risks, which includes things like injection attacks, broken authentication, sensitive data exposure, and more.

Should we be concerned about performance and degradation during testing?
No, we have never brought down an application and are very careful about not causing denial of service issues.

Will this test impact development timelines?
No, we can work with your development team to ensure testing does not interfere with the functionality of the application or the work they are doing on it.

How often should we perform this type of testing?
It is best practice to perform a test against the security of your application at least once per year, or any time there is a significant change to the application to ensure no new vulnerabilities are introduced after an update.