Client-side penetration testing, also known as internal testing, is the act of exploiting vulnerabilities in client-side application programs such as an email clients, web browsers, Macromedia Flash, Adobe Acrobat and others. According to the Symantec Internet Security Threat Report, threat actors are moving away from large and multipurpose cyberattacks on the network perimeter and are more focused on smaller and more targeted attacks directed at web and client-side applications.

Client-side penetration tests are performed to answer the following questions:

- How reliable is the security posture of an organization?
- Are there any vulnerabilities?
- What harm can an attacker do

posture of an organization?

- Are there any vulnerabilities?
- What harm can an attacker do by exploiting these vulnerabilities?
- How can a malicious actor exploit a vulnerability?
- Are the access rights and privileges for employees set correctly?
- How can the detected weak points be closed in an economical and sensible way?

Answering all these questions can provide a realistic picture of the current security posture of any organization. Based on the results of pentesting, additional steps can be taken to enhance the security of an organization if it's required.

In this article, you will learn how often pentests should be performed, how important pentesting and vulnerability assessments are for client-side security, organization if it’s required.

In this article, you will learn how often pentests should be performed, how important pentesting and vulnerability assessments are for client-side security, what information is required for pentesting, and the names of the biggest client-side security vulnerabilities and threats, as well as the damage they caused in 2017. By the end, you will be mindful of some best practices that companies should use to educate their employees.