PLATINUM
CIBER-SEGURIDAD

www.platinumciber.com | info@platinumciber.com | Tel. +5411 21283279

APPLICATION SECURITY

PENETRATION TEST, VULNERABILITY ASSESSMENT & SOURCE CODE ANALYSIS

Protect your systems and applications by exposing them to the same tests that attackers do. Know your vulnerabilities through the same techniques used by them, and know how to solve them to avoid suffering from those attacks.
Through our services, we simulate real attacks on the systems in order to find their vulnerabilities and even penetrate them, obtaining concrete evidence of how far an attacker could go. We also recommend a possible solution to each finding.

GO TO WEBSITE

VULNERABILITY ANALYSIS

Using this technique, a search is carried out for vulnerabilities present in the systems analysed. It verifies that each vulnerability exists, but it is not exploited. This service has as advantages that in a short time, almost all the possible entry points for an attacker are found. It is carried out with specific automatic tools of the World-Class type and by means of the expertise of our team of consultants.

PENETRATION TESTING

In this case, each vulnerability found is exploited to enter the client's systems and an attempt is made to penetrate as far as technically possible. This technique has the advantage of reliably demonstrating the damage that could be caused by an attacker. Although automatic tools are used for the development of the service, the expertise of our technician is fundamental and determining.

CODE ANALYSIS

To determine the possible vulnerabilities of an application, its source code is analyzed, looking for security flaws that could be access doors for attackers. For this service, automatic tools are used, but since even the best tools only detect a very low percentage of security failures, in this case the knowledge and experience of our specialized technical team is fundamental and determining.

MODALITIES

BLACK BOX

The customer chooses not to give any information about the systems to be verified, so the team must initially explore, find and identify possible targets related to the company or business to be analyzed. Afterwards, the technical team searches for vulnerabilities and/or exploits them, in exactly the same way as an external attacker unknown to the company would. The advantage of this modality is that it is the closest to reality, but its disadvantage is that the duration of the project is necessarily longer.

GREY BOX

It is an intermediate between Black Box and White Box, i.e. the company provides part of the technical information to the team that will carry out the project. This modality is similar to what an attacker would do who knows part of the targeted company, for example, an ex-employee.

WHITE BOX

The technical team has all the information about the environment, interface, connectivity equipment, etc., in order to drastically shorten project times. This modality is the most used for Code Analysis in which the complete source code of the application is delivered for analysis.