Exploit

Return to Glossary

An **Exploit** is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in an application or a system to cause unintended or unanticipated behavior to occur. The name comes from the English verb to exploit, meaning “to use something to one’s own advantage”. Basically, this means that the target of an attack suffers from a design flaw that allows people to create the means to access it and use it in his interest.

Among the most well-known web-based security vulnerabilities are: SQL injection attacks, cross-site scripting, cross-site request forgery and broken authentication code or security misconfigurations. In general, exploits can be classified in two main categories: known and unknown (or Zero-Day vulnerabilities).

The zero-day vulnerabilities are by far the most dangerous, as they occur when a software contains a critical security vulnerability of which the vendor is unaware. The vulnerability only becomes known when a hacker is detected exploiting the vulnerability, hence the term zero-day exploit. Once such an exploit occurs, systems running the software are left vulnerable to an attack until the vendor releases a patch to correct the vulnerability and the patch is applied to the software.

Source: https://www.bitdefender.com/consumer/support/answer/10556/