World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:09, 2014

The Journey of a Malicious HTTP Request

Authors : M. Mansouri, P. Jaklitsch, E. Teiniker

Abstract : SQL injection on web applications is a very popular kind of attack. There are mechanisms such as intrusion detection systems in order to detect this attack. These strategies often rely on techniques implemented at high layers of the application but do not consider the low level of system calls. The problem of only considering the high level perspective is that an attacker can circumvent the detection tools using certain techniques such as URL encoding. One technique currently used for detecting low-level attacks on privileged processes is the tracing of system calls. System calls act as a single gate to the Operating System (OS) kernel; they allow catching the critical data at an appropriate level of detail. Our basic assumption is that any type of application, be it a system service, utility program or Web application, “speaks” the language of system calls when having a conversation with the OS kernel. At this level we can see the actual attack while it is happening. We conduct an experiment in order to demonstrate the suitability of system call analysis for detecting SQL injection. We are able to detect the attack. Therefore we conclude that system calls are not only powerful in detecting low-level attacks but that they also enable us to detect high-level attacks such as SQL injection.

Keywords : Linux system calls, web attack detection, interception, SQL
Conference Title : ICARS 2014 : International Conference on Availability, Reliability and Security
Conference Location : Paris, France
Conference Dates : September 22-23, 2014