How to Mitigate Your Security Vulnerabilities in 2 Minutes

Or Katz, 2011-08-11

One of the first things that come to mind when talking about a Web Application Firewall is its ability to mitigate web application vulnerabilities. For this reason, it is natural to think about both Application Security Scanners and Web Application Firewalls as complementary products that need to talk to each other in order to solve security hazards waiting to be exploited.

For the reasons mentioned above, BIG-IP ASM and Whitehat sentinel offers a unique integration between a Web Application Firewall and an application security scanner that allows the application administrator to patch web application vulnerabilities in a simple and intuitive way.

Integration between ASM and Whitehat allows ASM administrator full control over the vulnerability mitigation life cycle by the following 3 steps:

1. Direct and in-direct import of application vulnerabilities from Whitehat service:
    1. In-direct approach allows the application administrator to import an offline XML file that includes web application vulnerabilities.
    2. Direct approach allows the application administrator to import a vulnerabilities list with a direct connection to the Whitehat server.
2. Mitigate the vulnerable object by adding it to the security policy and applying targeted protection.
3. Retest the vulnerability – inform Whitehat that retesting of the vulnerability is required and as a result sets the vulnerability status to "closed".

In the attached video you can see how in less than 2 minutes your vulnerabilities can be virtually patched by BIG-IP ASM's award winning Web Application Firewall mitigating risks until application software code is fixed and tested.