WHAT IS FALSE POSITIVE?

False positives occur when a scanning tool, web application firewall (WAF), or intrusion prevention system (IPS) incorrectly flag a security vulnerability during software testing. False positives describe the situation where a test case fails, but in actuality there is no bug and functionality is working correctly. Because false positives need to be checked out and this can be a time-consuming process, they typically eat up valuable IT bandwidth that should be applied to more important tasks.

High rates of false positives are efficiency disrupters, having a drag effect on IT software development and testing teams. While a false positive is improperly indicating the presence of a problem when in reality one does not exist (the software is functioning as intended), the false negative is the opposite, giving you a false senses of security by indicating you don’t have a vulnerability when in fact you do.

A False Positive is when you think you have a specific vulnerability in your program but in fact you don't. Many security scanners such as Nessus scan an application (or service/daemon) and attempt to find a vulnerability in it. Sometimes the signatures (the 'check logic') make mistakes and report a vulnerability that may not exist. False positive are not limited to scanners they also affect 'Web Application Firewalls' and 'NIDS's/IDS's/IPS's'. These monitoring products may report an attack attempt but sometimes confuse the data it received with valid information. Every once in awhile you may run a scanner that reports you as being vulnerable to a specific product (Like websphere) that you don't actually run. Sometimes the same vulnerability exists in multiple products but when the 'check' was written it was written with a specific application in mind and therefore the product and/or description for the vulnerability may not be 100% accurate.

Unfortunately false positives will continute to exist but they can be limited by the skill of the person writing the signatures or check logic. Before you go complaining to the vendor/author of the product you're using saying 'you need to learn how to write checks better' remember that these checks are carefully written and tested and you cannot always predict what everyone's custom environment will look like. If you think you have a false positive carefully work with the author/vendor to try and address the solution. Who knows maybe you \*are in fact vulnerable\*, or something else is vulnerable to that particular 'security check' as outlined above.