ENPM 809W – Introduction to Secure Software Engineering

Homework 2

Date Due: September 21, 2021, by 11:59 PM EST.

Please read the article attached in this week's (Week 2) module on 'Web Application Firewalls - How they work' and 'OWASP-CRS-Request-Body-Bypass-Vulnerability' and answer the following questions.

1. Input validation in Web Application Firewalls is not an intensive process. True or False. Please explain why.
2. With a signature-based approach to detection of malicious input in Web Application Firewalls, when an attack is detected, a new signature based on the attack is sent to all Web Application Firewalls that are subscribed to service. Please explain the pros and cons of this approach.
3. Hackers can easily find bypasses for rules specified in web application firewalls. True or False. Please explain why.
4. In the 'Web Application Firewalls – How they work' paper, the author explains one of the ModSecurity rules to prevent a user from surfing to /phpmyadmin URL path. The author mentions the keywords in the rule "…phase:1,deny,log…". What does the keyword 'log' here do? Please give specifics on what exactly happens.
5. The author of the 'OWASP-CRS-Request-Body-Bypass-Vulnerability' paper is talking about which web application firewall and ruleset?
6. The author of the 'OWASP-CRS-Request-Body-Bypass-Vulnerability' paper highlights that one of the issues in the vulnerability is related to which rule exclusion (RE) package?
7. The author of the 'OWASP-CRS-Request-Body-Bypass-Vulnerability' paper highlights that the other issue in the vulnerability is related to what exactly within that RE package?
8. Based on the 'OWASP-CRS-Request-Body-Bypass-Vulnerability', what is one way the author specifies you can check to see if you have been attacked?
9. Who reported the vulnerability described in the 'OWASP-CRS-Request-Body-Bypass-Vulnerability' paper?
10. It is a good idea to do responsible disclosure (Responsible disclosure - Wikipedia) instead of a full disclosure when you find a vulnerability. True or False.