ENPM809W – Introduction to Secure Coding

Homework – 2

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

Email: iamibi@umd.edu

1. Input validation in Web Application Firewalls is not an intensive process. True or False. Please explain why.

A. False. Input validation is an intensive process as it requires the WAF handler(s) to have knowledge about their access paths and come up with specific/generic input validation rules that can protect the organization from an input-based attacks. These rules take time to come up with and are expected to work on a wider type of inputs. The rules can at times be simpler, but they might not be very effective on a broader scale.

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.

A. The pros of the signature-based update are that if the organization has subscribed to the WAF service, the signatures will automatically be updated in their organization based WAF even if the attack was carried out in some other organization or discovered by some outside researcher. However, the downside is risky as well since the organization is exposed to all the inputs-based attacks that don't yet have a signature in the WAF service which in turn can expose critical vulnerabilities.

3. Hackers can easily find bypasses for rules specified in web application firewalls. True or False. Please explain why.

A. False. If the rules specified cover a broad range of inputs, then it is quite difficult for a hacker to bypass the WAF. However, if the rules are explicit to certain types of inputs then the hacker can craft an input which can bypass the WAF quite easily and sometimes as fast as any new rule is introduced in the WAF.

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.

A. The log keyword will trigger the logging system to write a log about the denied/blocked request and there will be a message that will be appended (using the msg: flag) giving more details on what type of request was denied. As per the example, the log flag is only trigged for the denied/blocked requests.

5. The author of the ‘OWASP-CRS-Request-Body-Bypass-Vulnerability’ paper is talking about which web application firewall and ruleset?

A. The author is talking about the CRS Web Application Firewall which was unable to prevent the trailing pathname backend vulnerability.

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?

A. The Drupal RE package in REQUEST-903.9001-DRUPAL-EXCLUSION-RULES.conf.

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?

A. There are three other rules that are in effect on top of the existing Drupal RE, which in turn disable request body scanning for a handful of specific requests (which are 9001180, 9001182 and 9001184).

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?

A. The author suggests that if the following paths are accessible with a success HTTP code while the Drupal is not running then it is possible that the system has been exploited:

- /admin/content/assets/add/

- /admin/content/assets/manage/

- /file/ajax/field_asset_

9. Who reported the vulnerability described in the ‘OWASP-CRS-Request-Body-Bypass-Vulnerability’ paper?

A. Andrew Howe

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.

A. True. Reason being that the vulnerable systems or software can be patched so that an attacker cannot leverage it.