GoDaddy Web Application Firewall (WAF)

Module 6 Assignment Submission

Functional and Non-functional Requirements

by

Neel Prajapati

CS6525 – Software Requirements Analysis

University of New Brunswick

DISCLAIMER: This report is not affiliated in any way with GoDaddy, nor does it intend to provide an accurate view of how GoDaddy conducts their business activities. This is a learning exercise at the University of New Brunswick based on unfounded assumptions and “best guesses” made by the author. The author has no inside knowledge of how GoDaddy’s software or business practices work. The objective is to simulate how requirements analysis might have been documented during the development of WAF for GoDaddy’s.

Table of Contents

1. Use Case Scenarios

EVENT-012 Customer request details of bots/threats/security attacks based on URLs attacked. Filtered based on criteria such as time, date, region, network provider, IP. ○ OBJECTIVE-001	Request for details of bot/threat/security for selected criteria (in) Display page with list of affected URLs along with attack/bot/threat score(Out)	Attack Information can include frequency of attacks, types of attacks (SQL injection, cross site scripting), etc. For Bot management, information will be stats of requests categorized into likely humans and likely bots along with histograms of scores.

The business event "EVENT-012" is related to the presentation of analytics results of bots/threats/security attacks. For simplicity the scenarios only mention security attacks, similar scenarios for bot analytics and threat analytics can be arranged along the same lines.

GoDaddy performs analytics on all the requests that it receives, however only WAF customers have access to the analytics data on the traffic they received. These results can be accessed by using tabs on the left hand toolbar. This use case is initiated by the customers and Godaddy WAF receives and serves the requests.

Scenario 1: Security Attacks meeting the selected criteria were logged and are available for display.

Steps in the **Scenario 1**:

1. User opens the WAF page in their account.
2. User clicks on the Attack analytics tab.
3. Present the user with the page with last 24 hours of details on Security Attacks. The information displayed includes:
   - Number of Total requests
   - Number of requests classified as Attacks
   - Number of requests classified as Clean
   - Number of requests classified as Likely Attack
   - Number of requests classified as Likely Clean
   - Graphs showcasing the spread of requests over time
   - List of requests with logged details
4. User selects the criteria (Excludes/Includes items from the filter criteria) and clicks filter. The following list shows the items that can be part of the filter criteria:
   1. Source IP

2. Time
3. Dates
4. Region
5. Country
6. Autonomous System Number (ASN)
7. JA3 Fingerprint
8. Method (POST/GET)
9. User Agent
10. Attack Score
11. Cross-site scripting (XSS) Score
12. SQL injection (SQLi) Score
13. Remote code execution (RCE) score

5. Update the page with the details as per filter criteria.
   The information displayed for the selected criteria includes:
   - Number of Total requests
   - Number of requests classified as Attacks
   - Number of requests classified as Clean
   - Number of requests classified as Likely Clean
   - Number of requests classified as Likely Attack
   - Graphs showcasing the spread of requests over time
   - List of requests with logged details

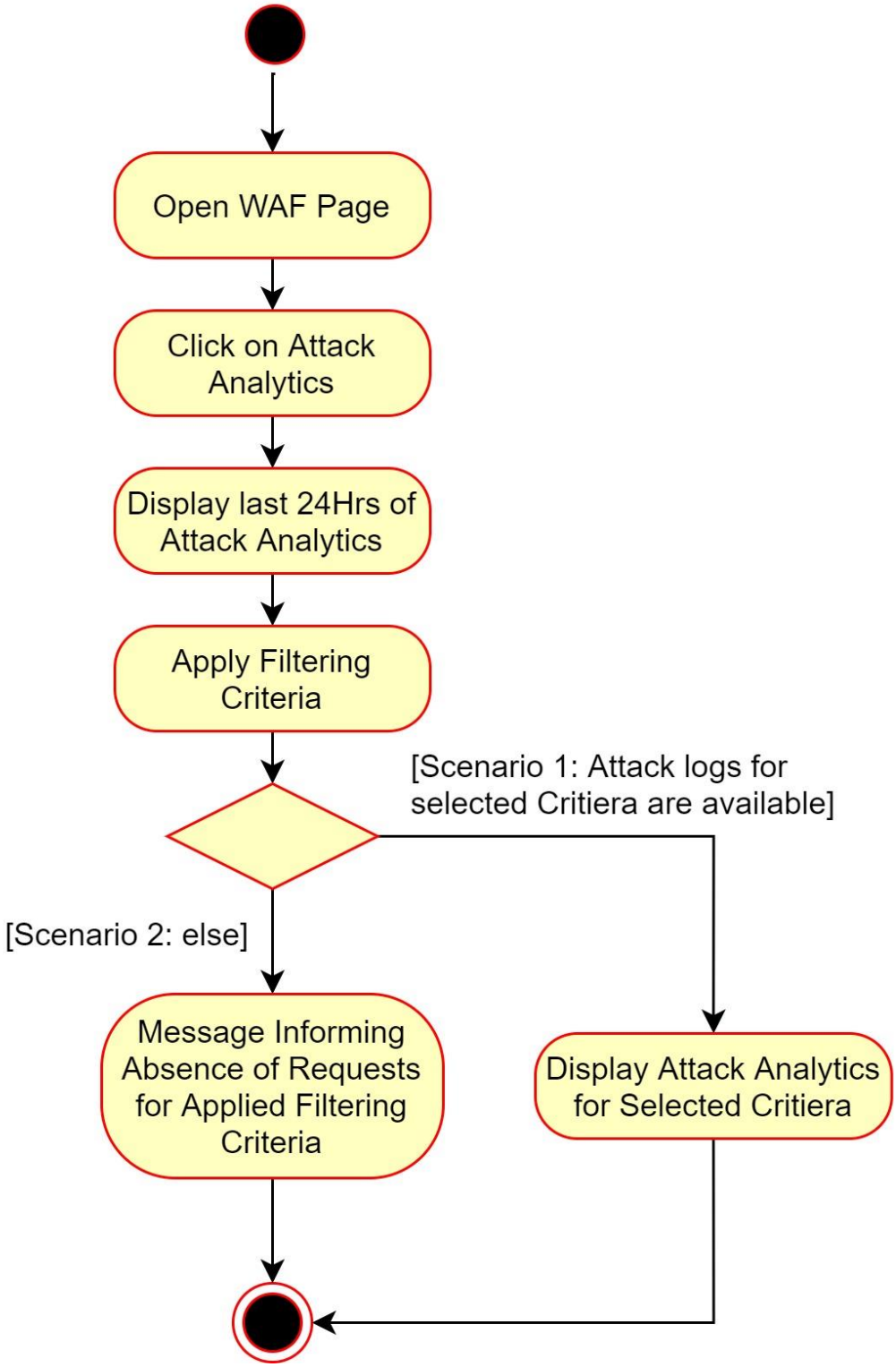
Scenario 2: Attack logs for the selected criteria do not exist, i.e., as per the system no attacks took place that meet the criteria and therefore the system has nothing to display.
Steps in the **Scenario 2**:

1. User opens the WAF page in their account.
2. User clicks on the Attack analytics tab.
3. Present the user with the page with the last 24 hours of details on Security Attacks. The information displayed includes:
   - Number of Total requests
   - Number of requests classified as Attacks
   - Number of requests classified as Clean
   - Number of requests classified as Likely Attack
   - Number of requests classified as Likely Clean
   - Graphs showcasing the spread of requests over time
   - List of requests with logged details
4. User selects the criteria (Excludes/Includes items from the filter criteria) and clicks filter.
   The following list shows the the items that can be part of the filter criteria:
   1. Source IP
   2. Time
   3. Dates
   4. Region

5. Country
6. Autonomous System Number (ASN)
7. JA3 Fingerprint
8. Method (POST/GET)
9. User Agent
10. Attack Score
11. Cross-site scripting (XSS) Score
12. SQL injection (SQLi) Score
13. Remote code execution (RCE) score

5. Display message to inform user of absence of requests for selected chosen criteria.

2. Acitivity Diagram for Use Case



3. Non-functional Requirements

NFR-001

Requirement: The WAF user interface will seamlessly integrate with the existing user interface and will follow the same design language as the rest of the user interface.

Rationale: The user interface is the only part of the system that the customer interacts with and as a result customers develop procedural memory with the design language and layout. To ensure continuity of this familiar experience, uniformity in the user interface is important.

How / when to measure: Once WAF user interface design is complete, ask the end-user representatives to compare the WAF user interface with the existing GoDaddy user interface and provide feedback for improvement.

Originates from business event(s): All except EVENT-001.

NFR-002

Requirement: The WAF user interface will be accessible to people with disabilities.

Rationale: Giving due consideration to the accessibility needs of users with disabilities in UI essential to ensure that such users are not restricted from using WAF.

How / when to measure: Once WAF UI development is complete check if it meets the latest W3C Web Content Accessibility Guidelines.

Originates from business event(s): All.

NFR-003

Requirement: WAF rule set execution on any request will not add more than 1ms of delay 99.99% of the time.

Rationale: Excessive delay introduced by WAF will reflect as slow response time of the website and will be perceived as sluggish interactability of the system, negatively impacting the user experience.

How / when to measure: Once WAF development is complete, run industry standard latency test suites targeting all host nodes to ensure the added delay is within limits across all servers.

Originates from business event(s): All.

NFR-004

Requirement: WAF will be compatible with Intel x86 and Arm ISA based servers.

Rationale: x86 and Arm are the most widely used instruction sets and only CPUs based on these architectures are used by GoDaddy. To ensure that the WAF can be deployed on any GoDaddy server hardware, compatibility with their CPU architectures is essential.

How / when to measure: Once WAF development is complete, is the system compatible with Intel x86 and Arm ISA?

Originates from business event(s): All.

NFR-005

Requirement: WAF's web front-end will support all the browsers that GoDaddy claims to be compatible with.

Rationale: All widely used web browsers render the content differently. This requires frontend development that targets different types of browsers individually to ensure proper rendering of content.

How / when to measure: Once WAF development is complete, is the system successful in the browser compatibility testing?

Originates from business event(s): All.

NFR-006

Requirement: WAF will be deploying GoDaddy's standard cipher suite.

Rationale: Confidentiality, Integrity, and Availability of the system and the information while it is being stored, processed and transmitted is imperative to ensure malicious actors are not able to harm the system which can result in legal liability and/or reputational damage to GoDaddy.

How / when to measure: Once WAF development is complete, is the system using the organisation standard cipher suite?

Originates from business event(s): All.

NFR-007

Requirement: WAF user interface will be able to switch to any of the list of languages supported by GoDaddy.

Rationale: GoDaddy has a global client base all of which use different languages even in professional settings. For this reason, GoDaddy provides the users the option of choosing a language from a list of languages for interacting with the UI.

How / when to measure: Once WAF development is complete, is the system able to switch between GoDaddy's list of supported languages?

Originates from business event(s): All.

NFR-008

Requirement: WAF will comply with all the laws and regulations based on the jurisdiction that applies to clients and their customers.

Rationale: GoDaddy has clients that have global presence, and their customers are expected to interact with WAF across the borders. This will make them and GoDaddy fall under varying combinations of scopes of authority. For this reason, it is essential that the WAF is able to dynamically adjust its services based on the applicable jurisdictions to each client and their individual customers.

How / when to measure: Once WAF development is complete, is the system able to dynamically vary its operations to meet the needs of applicable laws and regulations?

Originates from business event(s): All.