# Understanding Libraries

https://campus.barracuda.com/doc/86543122/

The Barracuda Web Application Firewall has developed a solution for bot protection that ensures accurate classification of traffic such as genuine users, good bots, search engine crawlers, and bad bots. The solution filters block bad bots before they infiltrate your web applications. It also allows you to allow-list trusted sources based on IP, URL, and subnet mask.

Some of the features included:

### Allowed Bots

Barracuda WAF enables you to create an allow list of bots as part of a web scraping policy. You can add a bot either by selecting a bot definition from the Barracuda Advanced Threat Intelligence (ATI) service or by adding a custom bot definition. The bot definitions can be created on the **BOT MITIGATION > Libraries** page.

After a bot definition is added to the **Allowed Bots** list, it gets displayed under **Allowed Bots** in the Web Scraping policy on the **BOT MITIGATION > Bot Mitigation > Web Scraping** section. You can select the bot under **Allowed Bots** to ensure that the bot-related checks happen when the matching request is received. See How to Add a Bot to the Allow List.

### Bot Lookup

Displays the top ten bot entries that is ordered by the "Last Seen" column. Specify the name of the bot to be displayed and then click **Lookup**.

### Spam URL List

Click the **View Spam URL List** button to view the list of all the referer entries against which the WAF provides protection.

### Comment Spam Parameter Class

This section allows you to edit the attack types in the Comment Spam Parameter class. By default, the attack types are specified to detect malicious patterns in the custom parameter.

### Custom Referer Bots

Specifies the custom referer spam types to be used to detect the spam. To create a new spam data type, enter a name in the New Group field and then click **Add**. To each group, one or more "patterns" that define the format of the data type can be added. To add a pattern to a particular group, click the **Add Pattern** link in that group.

### Session Identifiers

The Session Identifiers allow the Barracuda Web Application Firewall to recognize the session information from the requests and responses. For configuring Session Identifiers, see How to Configure Session Tracking.