Configuring User Defined Patterns

https://campus.barracuda.com/doc/17629561/

The Barracuda Load Balancer ADC allows you to create customized data patterns which can be detected and handled according to the configured security settings.

The Barracuda Load Balancer ADC uses regular expressions (regex) to define data type patterns. Custom data types can be defined using regex patterns to implement advanced data type enforcement on input parameters. For guidelines on how to write regular expressions, see Extended Match Syntax. The pattern-match engine recognizes the lexical patterns in text and compares inputs to defined data type patterns. For example, the following is the default regex pattern for a Visa credit card:

```
4[[:digit:]]{12}|4[[:digit:]]{15}
```

A pattern can also be associated with an algorithm, for example, an algorithm to validate a credit card number can be associated with a credit card pattern. The algorithm runs on all strings matching the regular expression to decide whether they actually conform to this pattern.

Internal Patterns

The **SECURITY > View Internal Patterns** page includes Identity Theft Patterns, Attack Types, Input Types, and Parameter Class. Each data type exhibits a unique pattern. These patterns can be bound to a policy or to profiles of an web application to validate the incoming requests.

The patterns displayed by default under each pattern group cannot be modified. To create a modified pattern, use the **Copy** function to copy a pattern, then modify it as required. The copied pattern group can be found on the **SECURITY > Libraries** page under the corresponding group. You can modify or delete patterns as required, and then apply them to a service security policy. For more information on how to copy a pattern group, refer to Steps to Copy a Pattern Group .

The following provides a brief description about the internal patterns.

Identity Theft Patterns

Identity theft is the loss of personal data resulting in fraud. Disclosure of sensitive information such as credit card numbers, banking information, passwords, or usernames in service communication might enable identity theft. The Barracuda Load Balancer ADC prevents unauthorized exposure of at risk data.

The Identity Theft container includes Credit Cards, Social Security Numbers, and Directory Indexing

data types. In addition, customized identity theft patterns can be created and used. For more information, see How to Configure Data Theft Protection.

Attack Types

An attack is a technique used to exploit vulnerabilities in web applications. Attacks can insert or modify code in requests. If a request contains an attack pattern, it is dropped. The attack data type container includes patterns for identifying Cross-site Scripting, Remote-file Inclusion, SQL Injection, Directory Traversal, and OS Command Injection attacks. In addition customized attack data types can be created and used.

Input Types

Input data types are used to validate the HTTP request parameters. Inputs come from web forms, applications and Services, custom client applications, or file based records. This validation ensures that the data conforms to the correct syntax, is within length boundaries, and contains only permitted characters or numbers. Requests failing validation are assumed intrusions and are blocked. Input types are defined using reg-ex patterns. Default Input Types including credit cards, numeric, hex-number, alpha, alphanumeric, string, name, and date are provided. In addition, customized Input Types can be defined and used.

Parameter Class

Parameter class defines acceptable values for parameters. Parameter classes are bound to Parameter Profiles using **SECURITY > Website Profiles** > **Parameter Profiles** and specify validation criteria for parameters in a request. In addition to the internal parameter classes, customized parameter classes can be created and used.

Steps to Copy a Pattern Group

Do the following to copy a pattern group:

1. From the **SECURITY > View Internal Patterns** page identify the group you want to copy.
2. Click **Copy** next to that group. The **Copy** window appears.
3. In the **New Group** field, specify a new name for the group and click **Paste**.
4. Navigate to the **SECURITY > Libraries** page. The new pattern group appears under the group to which it belongs.
5. Click **Edit Pattern** to edit a particular pattern.
6. Click **Delete** to delete a particular pattern.

Creating and Using Custom Attack Types

The **SECURITY > Libraries > Attack Types** section allows creation of custom attack data types

which, when detected in a request, identify the request as an attack. One or more patterns which define the format of the attack type can be added to each group.

Creating a Custom Attack Type Pattern

1. Go to the **SECURITY > Libraries > Attack Types** section.
2. Enter a name in the **New Group** text box and click **Add**. The new attack type group created appears in the **Attack Types** section.
3. Click **Add Pattern** next to that group. The **Attack Types** window appears. Specify values for the following fields:
    1. **Pattern Name** – Enter a name for the pattern.
    2. **Status** – Set to *On* if you wish to use this pattern for pattern matching in the responses.
    3. **Pattern Regex** – Define the regular expression of the pattern or click the **Edit** icon to select and insert the pattern.
    4. **Pattern Algorithm** – Select the algorithm to be associated with the pattern from the list.
    5. **Case Sensitive** – Select *Yes* if you wish the pattern defined to be treated as case sensitive.
    6. **Pattern Description** – Optional. Enter a description for the defined pattern. Example, Visa credit card pattern would indicate the pattern matches a visa credit card.
4. Click **Add**.

Using a Custom Attack Type

The added attack type pattern becomes available under **Custom Blocked Attack Types** on the following pages and sections:

- **SECURITY > Libraries > Custom Parameter Class**
- **SECURITY > Website Profiles > URL Profiles**
- **SECURITY > Security Policies > URL Protection**
- **SECURITY > Security Policies > Parameter Protection**

The **Custom Blocked Attack Types** are enabled by default under the **SECURITY > Libraries > Custom Parameter Class** section and the **SECURITY > Website Profiles > URL Profiles** section. Whereas in the **SECURITY > Security Policies > URL Protection** and **SECURITY > Security Policies > Parameter Protection** pages you have to manually select the custom attack types.

Creating and Using Custom Input Types

The Barracuda Load Balancer ADC includes a collection of predefined and custom input data types, which can be used to validate HTTP Request parameters. Input data types are used to validate that request parameters conform to expected formats. Most attacks can be prevented by properly validating input parameter values against expected input data types. Input Type validation enforces the expected formats rather than trying to identify malicious values. Requests failing validation are

identified as intrusions and blocked. Default Input Types including alpha-numeric strings, credit card, date and positive-long-integer are provided. Custom Input Data Types can also be added.

The **SECURITY > Libraries > Input Types** section allows you to create customized input data types. One or more patterns which define the format of the input type can be added to each group.

Creating a Custom Input Type Pattern

1. Go to the **SECURITY > Libraries > Input Types** section.
2. Enter a name in the **New Group** text box and click **Add**. The new input type group created appears in the **Input Types** section.
3. Click **Add Pattern** next to that group. The **Input Types** window appears. Specify values for the fields and click **Add** to save the pattern.

Using a Custom Input Type

Perform the following steps to use a custom input data type:

1. Go to the **SECURITY > Libraries > Custom Parameter Class** section.
2. Click **Add Custom Parameter Class**. The **Add Custom Parameter Class** window appears.
3. In the **Name** text box, enter a name for the custom parameter class.
4. Select **CUSTOM** from the **Input Type Validation** drop-down list.
5. Select the custom input type you created from the **Custom Input Type Validation** drop-down list.
6. In the **Denied Metacharacters** text box, enter the metacharacters or click the **Edit** icon to select and apply the metacharacters to be denied in this parameter value.
7. Select the required check box(es) of **Blocked Attack Types** and **Custom Blocked Attack Types** and click **Add**.
8. Bind this custom parameter class to a parameter profile.

Creating and Using Custom Parameter Class

The **SECURITY > Libraries > Custom Parameter Class** section allows creation of custom parameter classes which enforce expected input formats and block attack formats for request parameters. One or more patterns which define the format of the data type can be added to each group. Bind the custom parameter class to a parameter profile by adding a new parameter profile or editing an existing parameter profile using **SECURITY > Website Profiles**.

Creating a Custom Parameter Class

1. Go to the **SECURITY > Libraries > Custom Parameter Class** section.
2. Click **Add Custom Parameter Class**. The **Add Custom Parameter Class** window appears. Specify values for the following fields:

1. **Name** – Enter a name for the custom parameter class.
2. **Input Type Validation** – Select the expected type of value for the configured parameter on the **SECURITY > Website Profiles**. Most of the attacks could be prevented by properly validating input parameter values against the expected input. Input Type validation enforces the expected value type as opposed to looking for malicious values. Values of configured parameters are validated against the specified Input Type and requests with failed validations are detected as intrusions and blocked.
3. **Custom Input Type Validation** – Select the expected custom input data type for the configured parameter.
4. **Denied Metacharacters** – Enter the metacharacters to be denied in the parameter value, or click the **Edit** icon to select and apply the metacharacters.
5. **Blocked Attack Types** – Select the check box(es) to detect malicious patterns in the configured parameter. An intrusion is detected when the value of the configured parameter matches one of the specified Attack Types and the request is blocked.
6. **Custom Blocked Attack Types** – Select the custom attack type check box(es) to be used to detect the intrusions.

3. Click **Add** to add the above configuration.

Using a Custom Parameter Class

Perform the following steps to use a custom parameter class:

1. Go to the **SECURITY > Website Profiles** page
2. In the **Service** section, click the **Website** drop-down list and select the Service for which you wish to add the parameter profile.
3. In the **URL Profiles** section, select the check box next to the URL profile to which you want to add the Parameter profile.
4. In the **Parameter Profiles** section, click **Add Param**. The **Create Parameter Profile** window appears.
5. In the **Parameter Profile Name** text box, specify a name for the parameter profile. Ensure the **Status** is set to *On*.
6. Select **CUSTOM** from the **Parameter Class** drop-down list.
7. Select the custom parameter class you created from the **Custom Parameter Class** drop-down list and click **Add**.
8. Now, the parameter profile is used to validate the requests coming for the Service you selected depending on the Mode you configured in the URL profile. For more information on URL and Parameter Profiles. See Configuring Website Profiles.

Creating and Using Custom Response Page

The **SECURITY > Libraries > Response Pages** section allows creation of customized HTML response pages for HTTP requests that violate security policies on the Barracuda Load Balancer ADC. Either **Edit** an existing default response page or use **Add Response Page** to add customized

response pages that can be shared among multiple Services.

Creating a Custom Response Page

1. Go to the **SECURITY > Libraries > Response Page** section.
2. Click **Add Response Page**. The **Add Response Page** window appears. Specify values for the following fields:
    1. **Response Page Name** – Enter a name for the response page.
    2. **Status Code**- Enter the HTTP status for the response page. Examples:
        1. 403 Forbidden
        2. 405 Method Not Allowed
        3. 406 Not Acceptable
    3. **Headers**- Enter the response headers for the response page. Examples:
        1. **Allow** – What request methods (GET, POST, etc.) does the server support?
        2. **Content-type** – Content type of the resource (such as text/html).
        3. **Connection** – Options that are specified for a particular connection and must not be communicated by proxies over further connections.
        4. **Location** – Where should client go to get document?
        5. **Refresh** – How soon should browser ask for an updated page (in seconds)?
    4. **Body**- Enter the response body for the response page. The following macros are supported:
        1. **%action-id** – This will be replaced by the attack ID of the violation which resulted in the response page to be displayed.
        2. **%host** – This will be replaced by the host header which sent the request.
        3. **%s** – This will be replaced by the URL of the request which caused the violation.
        4. **%client-ip** – This will be replaced by the Client IP of the request which caused the violation.
        5. **%attack-time** – This will be replaced by the time at which the violation occurred.
        6. **%attack-name** – This will be replaced by the attack name of the violation which resulted in the response page to be displayed.
3. Click **Add** to add the new custom page.

Example of a custom response: The request from %client-ip at %attack-time for the URL %s cannot be served due to attack %action-id on the host %host.

An image can also be embedded in the response page. Here are the steps to do so:

1. Convert the image to base64 using openssl or any other utility. Example: openssl base64 -in barracuda.jpg -out barracuda-jpg.b64
2. Embed the base64 encoded image into html with the "img" tag. Example: <html></html>

Using a Custom Response Page

The added response page is listed under the following pages and sections:

- **SECURITY > Security Policies > Global ACLs > Existing Global ACLs**
- **SECURITY > Security Policies > Action Policy > Action Policy**
- **SECURITY > Allow/Deny > URL : Allow/Deny Rules**

Perform the following steps to use a custom response page:

Steps to Use a Custom Response Page in the URL : Allow/Deny Rules

1. Go to the **SECURITY > Allow/Deny > URL : Allow/Deny Rules** section.
2. Click **Add** next to the Service for which you want to configure the response page. The **Create ACL** window appears.
3. In the **URL ACL Name** text box, enter a name for the URL ACL.
4. Select **Response Page** from the **Deny Response** drop-down list.
5. Select the response page you created from the **Response Page** drop-down list.
6. If required change values of other parameter(s) and click **Add**.

Steps to Use a Custom Response Page in the Action Policy

1. Go to the **SECURITY > Security Policies > Action Policy > Action Policy** section.
2. Click **Edit** next to the action policy for which you want to add the response page. The **Edit Attack Action** window appears.
3. Select the response page you created from the **Response Page** drop-down list, and click **Save Changes**.

Steps to Use a Custom Response Page in the Existing Global ACLs

1. Go to the **SECURITY > Security Policies > Global ACLs > Existing Global ACLs** section.
2. Click **Edit** next to the URL ACL for which you want to add the response page. The **Edit Global ACL** window appears.
3. Select the response page you created from the **Response Page** drop-down list, and click **Save Changes**.