

## Configuring User-Defined Patterns

<https://campus.barracuda.com/doc/4259978/>

The Barracuda Web Application Firewall allows you to create customized data patterns that can be detected and handled according to configured security settings.

The Barracuda Web Application Firewall 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 Help](#). 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 **ADVANCED > 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 a 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 **ADVANCED > 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, see [Steps to Copy a Pattern Group](#).

The following provides a brief description of 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 Web Application Firewall 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 [Enabling 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 to be 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 **WEBSITES > Web Site 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.

## Copy a Pattern Group

1. From the **ADVANCED > View Internal Patterns** page, identify the group you want to copy.
2. Click **Copy** next to that group. The **Copy** window opens.
3. In the **New Group** field, specify a new name for the group and click **Paste**.
4. Go to the **ADVANCED > 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 **ADVANCED > Libraries > Attack Types** section allows the creation of custom attack data types, which, when detected in a request, identify the request as an attack. One or more patterns that define the format of the attack type can be added to each group.

### Create a Custom Attack Type Pattern

1. Go to the **ADVANCED > 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:
  - **Pattern Name** – Enter a name for the pattern.
  - **Status** – Set to *On* if you wish to use this pattern for pattern matching in the responses.
  - **Pattern Regex** – Define the regular expression of the pattern or click the **Edit** icon to select and insert the pattern.
  - **Pattern Algorithm** – Select the algorithm to be associated with the pattern from the list.
  - **Case Sensitive** – Select Yes if you wish the pattern defined to be treated as case sensitive.
  - **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:

- **ADVANCED > Libraries > Custom Parameter Class**
- **WEBSITES > Web Site Profiles > URL Profiles**
- **SECURITY POLICIES > URL Protection**
- **SECURITY POLICIES > Parameter Protection**

The **Custom Blocked Attack Types** are enabled by default under the **ADVANCED > Libraries > Custom Parameter Class** section and the **WEBSITES > Web Site Profiles > URL Profiles** section. However, you must manually select the custom attack types in the **SECURITY POLICIES > URL Protection** and **SECURITY POLICIES > Parameter Protection** pages.

### Creating and Using Custom Input Types

The Barracuda Web Application Firewall includes a collection of predefined and custom input data types that 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 **ADVANCED > Libraries > Input Types** section allows you to create customized input data types. One or more patterns that define the format of the input type can be added to each group.

#### Create a Custom Input Type Pattern

1. Go to the **ADVANCED > 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 opens. Specify values for the fields and click **Add** to save the pattern.

#### Use a Custom Input Type

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

1. Go to the **ADVANCED > 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 **ADVANCED > Libraries > Custom Parameter Class** section allows the creation of custom parameter classes that enforce expected input formats and block attack formats for request parameters. One or more patterns that 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 **WEBSITES > Web Site Profiles**.

#### Create a Custom Parameter Class

1. Go to the **ADVANCED > Libraries > Custom Parameter Class** section.
2. Click **Add Custom Parameter Class**. The **Add Custom Parameter Class** window appears. Specify values for the following fields:
  - **Name** – Enter a name for the custom parameter class.
  - **Input Type Validation** – Select the expected type of value for the configured parameter on the **WEBSITES > Web Site Profiles** page. Most of the attacks can 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.

- **Custom Input Type Validation** – Select the expected custom input data type for the configured parameter.
- **Denied Metacharacters** – Enter the metacharacters to be denied in the parameter value, or click the **Edit** icon to select and apply the metacharacters.
- **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.
- **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.

### Use a Custom Parameter Class

Perform the following steps to use a custom parameter class:

1. Go to the **WEBSITES > Web Site Profiles** page
2. In the **Service** section, click the **Web Site** 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 opens.
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. The parameter profile is now 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 **ADVANCED > Libraries > Response Pages** section allows the creation of customized HTML response pages for HTTP requests that violate security policies on the Barracuda Web Application Firewall. Either **Edit** an existing default response page, or use **Add Response Page** to add customized response pages that can be shared among multiple services.

### Create a Custom Response Page

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

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 POLICIES > Global ACLs > Existing Global ACLs**
- **SECURITY POLICIES > Action Policy > Action Policy**
- **WEBSITES > Allow/Deny > URL : Allow/Deny Rules**

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

1. Go to the **WEBSITES > Allow/Deny > URL : Allow/Deny Rules** section.
2. Click **Add** next to the service you want to configure the response page for. The **Create ACL** window opens.
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 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**.

### Use a Custom Response Page in the Existing Global ACLs

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

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.