REST API and JSON Security

https://campus.barracuda.com/doc/45024047/

JavaScript Object Notation (JSON) security performs deep inspection of incoming packets/requests for web applications that use the JSON protocol to exchange data over HTTP. Many applications including mobile applications exchange data with the servers using JSON (RFC 4627), which is a light-weight data-interchange format. JSON-based applications can be attacked in multiple ways, such as sending data in an improper format or embedding attack vectors in the data. It is important for applications using the JSON format to validate the inputs before being processed. The Barracuda Web Application Firewall enforces input validations and other security checks to ensure that attacks are not tunneled inside HTTP requests with JSON content.

Example:

A traditional application sends an “application/x-www-form-urlencoded” post request with the following URL query parameters:

First-name=John&Last-name=Peter&email=john@fastmail.com

The same application in JSON could form the “application/json” post request with JSON objects in the request body as shown below:

{“First-name”:”John”,”Last-name”:”Peter”,”email”:”john@fastmail.com”}

The JSON key value pairs in the request body require the same level of input validation as the URL query parameters.

JSON security is applicable only for HTTP and HTTPS services on the Barracuda Web Application Firewall.

When a service is created, a default JSON profile is automatically created by the system for that service on the **WEBSITES > JSON Security** page. By default, this JSON profile applies to the whole URL space of the service; however, you can create multiple JSON profiles for different URL spaces within the service.

If a request contains content type as “application/json”, the Barracuda Web Application Firewall validates the request against the JSON profile(s) associated with the service and enforces the configured policy. The Barracuda Web Application Firewall enforces a JSON policy based on the following settings:

URL Match

The URL compared to the URL in the request. The URL should start with a "/" and can have at most one " * " anywhere in the URL. For example, /netbanking.html Any request matching this URL is required to authenticate before accessing this page. A value of “/*” means that the access control rule (ACL) applies for all URLs in that domain.

Host Match

The host name compared to host in the request. This can be either a specific host match or a wildcard host match with a single * anywhere in the host name. For example, *.example.com Any request matching this host is required to authenticate before accessing this page.

Mode

The service Mode takes precedence over the JSON profile mode. When Mode is set to Active, any request that violates JSON profile settings is blocked if the Mode of the service on the **BASIC > Services** page is also set to Active. If the Mode of the service is Passive, and the request violates JSON profile settings, the request is allowed to pass through, but logs request errors on the **BASIC > Web Firewall Logs** page.

The service Mode takes precedence over the JSON profile mode, i.e., if the JSON profile mode is Active and the service mode is Passive, all requests are allowed to pass through, but logs request errors on the **BASIC > Web Firewall Logs** page. If the mode is Active in the JSON profile and service, any request that violates JSON profile settings is blocked.

When Mode is set to Active, any request that violates JSON profile settings is blocked if the Mode of the service on the **BASIC > Services** page is also set to Active. If the Mode of the service is Passive and the request violates JSON profile settings, the request is allowed to pass through, but logs request errors on the **BASIC > Web Firewall Logs** page.

Validate Key

Set this to Yes to enforce validation on keys in the JSON request.

JSON Policy

Select the policy to validate the requests matching this JSON profile. You can create a new policy and associate with the JSON profile or fine-tune the default policy by clicking Edit next to it under **JSON Policies** on the **WEBSITES > JSON Security** page. See Configuring a JSON Policy.

Ignore Keys

Add the keys that need to be exempted from JSON security checks. This is an exact match; wildcards

are not supported. In other words, a value with "*" does not work like a wildcard.

Methods

Enter the methods to be matched in the request for JSON data inspection. The methods that are allowed to be configured are: GET,POST,PUT,HEAD,OPTIONS,DELETE,TRACE,ALL. Note: If set to "ALL", JSON data inspection will be done on all requests with "application/json" as content type.

Blocked Attack Types/Custom Blocked Attack Types

Attack types are malicious patterns that can be checked in a JSON request. Select attack types that need to be matched in the JSON request.

Exception Patterns

Specify patterns that need to be exempted from JSON security checks.

Steps to Configure JSON Security

To add a JSON security policy, perform the following steps:

1. Go to the **WEBSITES > JSON Security** page, **JSON Security** section.
2. Identify the service that you want to add a JSON security policy to, and click **Add JSON Profile** next to it.
3. On the **Add JSON Policy** page, enter a name for the JSON profile, set the **Status** to **On**, specify values for other parameters as required, and click **Save**.