Enabling API Discovery for JSON Profiles

https://campus.barracuda.com/doc/19645/

Modern APIs are designed using an Interface Description Language such as JSON using software tools like Swagger. These schema files written in JSON or YAML language can then be used to generate API documentation and stub code.

The schema files can be imported to create JSON security profiles on the Barracuda WAF. However, in many cases, administrators may not have access to the schema files and are therefore required to create the profiles manually, which can be a complex if the API server has a lot of API objects. These problems can be mitigated using the API Discovery feature.

> The API Discovery feature requires an active subscription for the Advanced Bot Protection (ABP) license. If you have purchased the ABP license, API Discovery is enabled by default for all service(s) configured on the **BASIC > Services** page. To disable the discovery, click **Disable Discovery** under **Actions**.

The Barracuda WAF API Discovery contains two parts:

- Endpoint Discovery
- Structure/Key Discovery

Endpoint Discovery

When API Discovery is enabled, the endpoints of a service that receives REST API traffic are discovered and corresponding recommendations are provided to create JSON profile(s) next to the service. Click **Endpoints** under **Discovery** to review and apply the configuration.

API Discovery Wizard for Endpoints

Use this section to review the discovered endpoints, modify brute force values, and apply the configuration.

1. Navigate to the **WEBSITES > JSON Security** page, **JSON SECURITY** section.
2. Click **Endpoints** under **Discovery** next to the service. The **API Discovery Wizard** opens.
3. On the **API Discovery Wizard** page:
    1. **Service** - Displays the name of the service for which the endpoints are discovered.

2. **API Endpoints to Configure** - Displays the endpoint paths, REST method, and Rate Limit that are appended to the base URL. By default, all endpoint paths are selected and **Structure Discovery** is enabled. You can clear the check box(es) next to the endpoint path if required. Use the down arrow button to modify the brute force values for endpoints.
3. Click **Preview Configuration** to view the configuration.
4. Click **Apply** to apply the schema through RESTful API.

Structure/Key Discovery

The JSON security can be further fine-tuned by enabling **Structure Discovery** for JSON payloads. When **Structure Discovery** is enabled for a JSON profile, the payload-related metadata is sent to Barracuda Advanced Threat Intelligence (ATI) for further analysis. Based on the analysis, the JSON key/value structure is identified, and key profile recommendations are generated and displayed for review. Click **Keys** under **Discovery** to review the discovered key profiles and apply the configuration.

API Discovery Wizard for Keys

Use this section to review the discovered keys and apply the configuration.

1. Go to the **WEBSITES > JSON Security** page, **JSON SECURITY** section.
2. Click **Keys** under **Discovery** next to the JSON profile. The **API Discovery Wizard** opens.
3. On the **API Discovery Wizard** page:
    1. **JSON Profile** - Displays the name of the JSON profile for which the keys are discovered.
    2. **JSON Keys to Configure** - Displays the following details for the discovered keys:
        1. Key Name
        2. Type of Value (string, object, array, or number) associated with the key.
        3. Minimum/Maximum value of the string, object, array, or number. The minimum value can be configured in a key profile if the value type is **Number**.
        4. Class of the key value discovered in the requests and responses.
        5. By default, all keys are selected. You can clear the check box(es) for the key profiles you do not want to create.
    3. Click **Preview Configuration** to view the configuration.
    4. Click **Apply** to apply the schema through RESTful API.