GraphQL Security

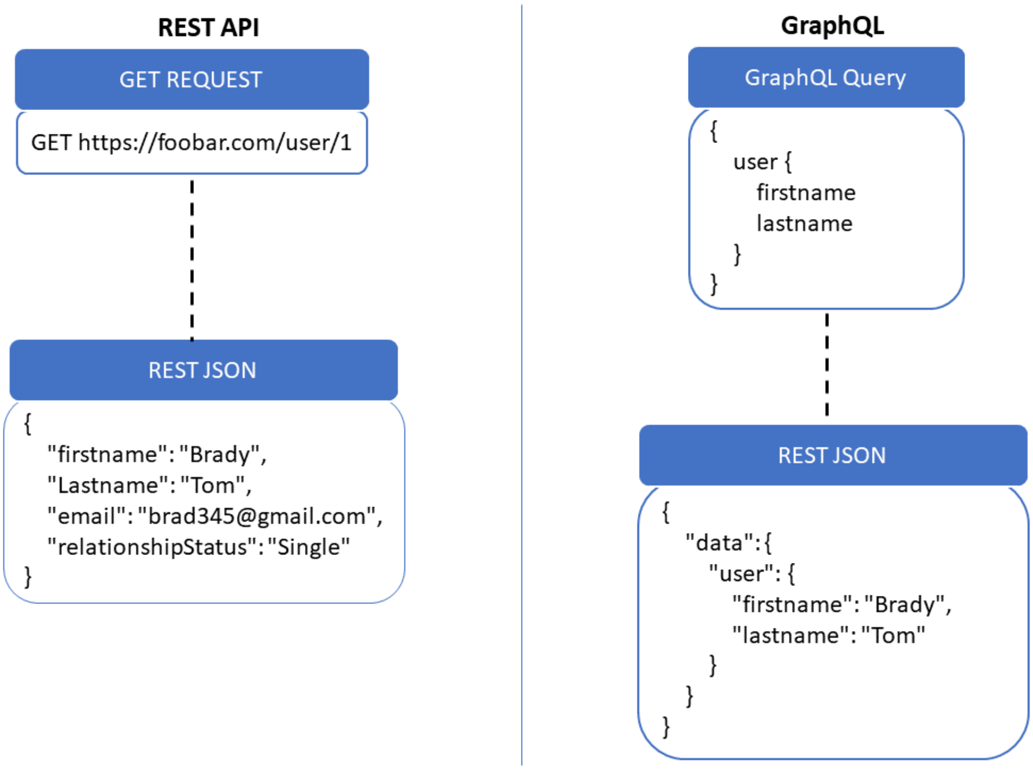
https://campus.barracuda.com/doc/96770854/

The Barracuda Web Application Firewall provides security for GraphQL APIs. GraphQL is an open-source data query and manipulation language for APIs and is served over HTTP. It is an alternative to REST and SOAP and overcomes issues like over-fetching and under-fetching. With GraphQL, a single endpoint can be used to query multiple resources and obtain only the data that clients request. While GraphQL enables the creation of flexible APIs, it involves complex configurations that may expose the applications to various security vulnerabilities, such as DoS attacks, injection attacks, introspection queries (which can expose sensitive data), or other malicious queries. The Barracuda WAF GraphQL Security provides native parsing of GraphQL requests and enforces security checks to protect against these attacks. For more information, see GraphQL.

GraphQL Security is not supported on Platform 2 units.

To determine the platform version of your appliance/virtual machine, contact Barracuda Networks Technical Support.

REST vs GraphQL:



```
GET https://foobar.com/user/1
```

```
{
  "firstname":"Brady",
  "Lastname":"Tom",
  "email":"brad345@gmail.com",
  "relationshipStatus":"Single"
}
```

```
{
  user {
    firstname
    lastname
  }
}
```

```
{
  "data":{
    "user":{
      "firstname":"Brady",
      "lastname":"Tom"
    }
  }
}
```

The Barracuda WAF GraphQL security:

- Provides native parsing of GraphQL requests.
- Supports GraphQL use cases, where JSON payload is sent over POST (body) or GET (URL parameter) requests or any other content type with JSON body document (for e.g., application/graphql+json).
- Checks attack signature against each field in JSON or GraphQL payload.
- Supports best practices of GraphQL APIs deployment with configurable allow or deny introspection query.
- Protects against denial-of-service (DoS) attacks by enforcing:
    - Maximum query depth.
    - Batch query configuration (Allow or Deny). If allowed, configurable maximum batch size.
- Provides configurable size limits for:
    - Complete request payload
    - GraphQL “query” in JSON payload

A GraphQL profile can be configured for a URL match, a host header match, a set of optional extended match criteria, or HTTP methods and content types. If a match is found, the request is validated against the configured profile settings. The Barracuda Web Application Firewall enforces a GraphQL policy based on the following settings:

GraphQL Profile

Mode

The service Mode takes precedence over the GraphQL profile mode. When **Mode** is set to **Active**, any request that violates GraphQL 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 GraphQL 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 GraphQL profile mode. In other words, if the GraphQL 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 GraphQL profile and service, any request that violates GraphQL profile settings is blocked.

When **Mode** is set to **Active**, any request that violates GraphQL 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 GraphQL profile settings, the request is allowed to pass through, but logs request errors on the **BASIC > Web Firewall Logs** page.

Match Criteria

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 the 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, in *.example.com, any request matching this host is required to authenticate before accessing this page.

Extended Match

An expression that consists of a combination of HTTP headers and/or query string parameters. This expression is used to match against special attributes in the HTTP headers or query string parameters in the requests. Use '*' to denote "any request"; that is, do not apply the Extended Match condition. For more information on how to write an extended match expression, see Extended Match Syntax Help.

Extended Match Sequence

This is used to specify an order for matching the extended match rule when a request matches multiple rules with the same host match and URL match.

Inspect Content Types

The content type(s) that needs to be inspected in the POST body for a URL. By default, "application/json" is added to the GraphQL profile.

Allowed Methods

Methods that you want to allow in the request. This will help the Barracuda Web Application Firewall to allow or disallow certain methods. For example, you can configure to disallow the PUT method. This blocks any attempt to upload files. Similarly, disallowing the CONNECT method thwarts any attempt to set up tunnels through servers. By default, the POST method is added to the GraphQL profile.

Attack Protection

Blocked Attack Types

Attack types are malicious patterns that can be checked for in the GraphQL request payload or JSON payload containing a GraphQL query. Select the attack type(s) that needs to be checked in GraphQL requests. An intrusion is detected when any pattern in the request matches one of the specified attack types.

Custom Blocked Attack Types

Apart from the default set of attack types provided, you can create your own attack patterns on the **ADVANCED > Libraries** page. Every such custom-defined pattern appears here as a possible choice for you to enable as a Blocked attack type.

Exception Patterns

Displays the list of patterns that are allowed as exceptions even though they are part of a malicious pattern group. The configuration should be the exact Pattern Name as found on the **ADVANCED > View Internal Patterns** page, or as defined during the creation of a New Group through the **ADVANCED > Libraries** page. The pattern name can also be found in the web firewall log when a false positive occurs due to such a potentially "exception" pattern. For example, if the parameter value matches the "sql-comments" regex pattern under "sql-injection medium" attacks on the **ADVANCED > View Internal Patterns** page, then adding "sql-comments" to this list will allow "sql-comments" in the future.

Introspection

Introspection enables the client to query the GraphQL server for the resources that are available in the API schema. The information includes data like types, fields, queries, mutations, and also the field-level descriptions. Set **Allow Introspection Queries** to **Yes** to enable introspection queries. When set to **No**, the Barracuda WAF does not allow introspection queries.

It is recommended to set **Allow Introspection Queries** to **No** in production.

Batching

Batching enables you to send multiple queries to the server in one request. When **Allow Batch Queries** is set to **Yes**, clients are allowed to make batch queries. If set to **No**, batch requests are denied when the service and this profile are in the **Active** mode.

Also, specify the maximum number of GraphQL queries to be allowed in a batched request.

Limits

Configure the threshold for request and response payloads.

Maximum Request Payload Length

The maximum length to be allowed in the GraphQL request payload.

Maximum Response Length

The maximum length of the GraphQL response that can be sent back to the client.

Maximum Query Depth

The maximum query depth to be allowed in the GraphQL request payload. The query depth is the number of nesting levels of the field that needs to be allowed in the request.

Max Query Value Length

The maximum query value length to be allowed in the request.

Exemptions

Attributes (GraphQL field names, argument names, variable names, and JSON key names) that you want to be exempted from Attack Protection checks configured in the GraphQL profile.

Configure GraphQL Security

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

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

Figures

1. RESTvsGraphQL.png