Securing JSON and AJAX Messages with F5 BIG-IP ASM

JSON is a common AJAX-based application language used to deliver highly dynamic content. JSON is quickly becoming a popular technology for websites that need to replace only personalized sections of an HTML page. Unfortunately, the dynamic and rich nature of JSON messages also brings new security threats that can be targeted at very specific parts of a web page or at individual users. F5® BIG-IP® Application Security Manager™ (ASM) secures JSON and AJAX message payloads to protect against XSS and JSON hijacking.

Protecting AJAX and JSON Applications

Asynchronous JavaScript and XML (AJAX) is a method for exchanging dynamic message-based data between applications, users, and systems. Often referred to as a singular technology, AJAX is a parent term for a group of web-based messaging technologies, standards, and formats for messages, such as HTML, CSS, XML, and JavaScript. A specific AJAX implementation is the JavaScript Object Notation (JSON)—a human-readable collection of name-value pairs similar to XML.

Unlike a traditional synchronous web POST event, where data is pushed to a web server in URI in a linear name-value pair format (such as param1=name&param2=location& …), JSON data is exchanged asynchronously between web applications in a longer message format with structured tiers of name-value pairs called objects.

Much more detailed information (both structurally in the message with objects and with the object data) can be embedded in a JSON message exchange than in a typical web application exchange through a traditional name-value POST event. In addition, JSON messages can also contain binary payloads, such as pictures, data, and executable files, allowing asynchronous and personalized exchange of files outside of a standard HTML page. Many web page widgets, for example, rely on JSON to display personalized information for users, such as a picture stream or weather information.

The data flexibility provided by JSON and AJAX also creates a rich environment for web application attacks that are based on name-value pairs. Poorly written JSON code can allow an attacker to modify the application by manipulating the name-value object data or by inserting or altering the binary payloads, preventing a user from seeing customized content. Sophisticated AJAX attacks can also be used to initiate XSS and JSON hijacking attacks, allowing the attacker to compromise very personalized information for targeted users.

F5 BIG-IP Application Security Manager provides sophisticated application-level protection of JSON messages and applications exchanging AJAX data. BIG-IP ASM is designed to block all known web application vulnerabilities, including the OWASP Top 10 and attacks that can be nested in AJAX message exchanges such as XSS, SQL injection, and cross-site request forgery (CSRF).

Key features

- **AJAX Policies**—Supports security policy for dynamic AJAX and JSON content
- **JSON Parser**—Provides a dedicated AJAX and JSON message parser for object-level inspection
- **Response Injection**—Offers embedded alert responses in affected AJAX components only
- **Any-App Support**—Provides object-level tenability to support custom applications

Key benefits

- **Secures AJAX and JSON Messages**—Secures dynamic AJAX and JSON content by screening messages, objects, and payloads in real time as part of the overall application security policy
- **Custom-Built JSON Protection**—Implements a specialized and dedicated JSON message parser to provide the highest level of protection for AJAX-enabled applications without affecting performance
- **Real-Time Alerts**—Generates reports, alerts, and user responses specific to the AJAX element within an HTML page
- **Flexible Security Policy Configuration**—Provides existing JSON security policies for AJAX-enabled applications that can be fine-tuned by the administrator for specific application and security needs

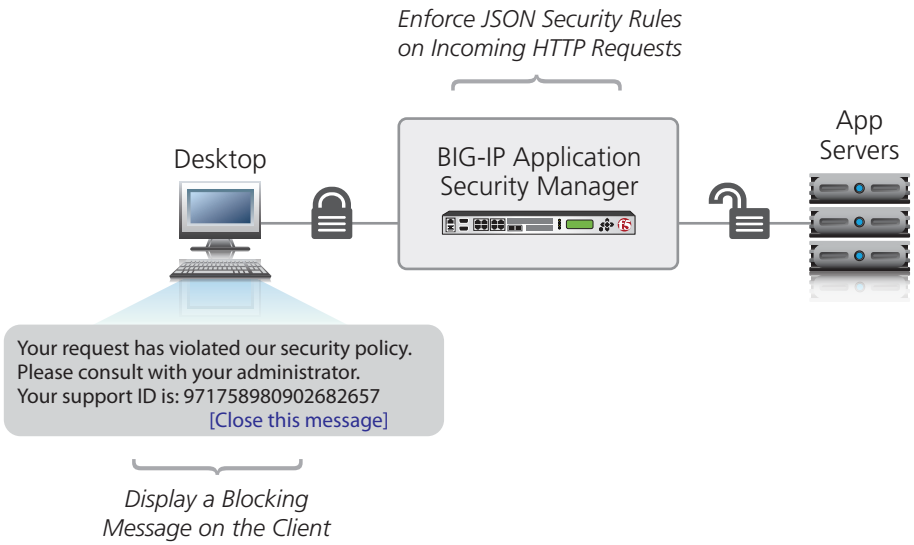
Solution

As an in-line application proxy, BIG-IP ASM parses JSON messages and protects AJAX applications that transfer data between applications, clients, and servers. BIG-IP ASM can apply and enforce a security policy on JSON messages, providing real-time protection, alerting, and reporting.

BIG-IP ASM offers the following features:

- **JSON payload protection**—BIG-IP ASM uses a dedicated JSON parser to inspect all JSON messages and apply security policies to embedded object pairs and binary payloads. BIG-IP ASM enforces many JSON security policy parameters, such as restricting URL wildcards and parameters, malformed data, and JSON payloads, methods, and objects.
- **Real-time embedded blocking alerts**—AJAX controls the exchange of information between applications, clients, and servers without altering the entire contents of an HTML web page. If a JSON violation is detected, BIG-IP ASM is able to return an embedded alert or a URL redirection notifying the user about a security issue related to that singular AJAX control instance.
- **Application signatures**—BIG-IP ASM includes a wealth of application signatures that are updated on a regular basis. These application signatures include many applications that use AJAX and JSON messages. In addition, new application signatures for applications running on platforms such as ASP.NET, JQuery, and MooTools are added daily.

F5 BIG-IP ASM provides total application-level protection for all web-based applications, including those which use AJAX asynchronous communications and JSON messages.



Protect AJAX applications and secure JSON payloads.

Learn more

For more information about BIG-IP ASM solutions, please see the following resources or use the search function on f5.com.

Product overview

BIG-IP Application Security Manager

White papers

Application and Data Security with F5 BIG-IP ASM and Oracle Database Firewall

Application Security in Dynamic Environments with BIG-IP ASM

BIG-IP Virtual Editions—The Virtual ADCs Your Application Delivery Network Has Been Missing

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

CS23-00007 0611