JSON Injection

Thursday, October 19, 2017 10:00 PM

JSON stands for JavaScript Object Notation.

It is a simple and effective lightweight data exchange format.
JSON can be in a lot of forms such as arrays, lists, hashtables and other data structures

JSON is widely used in AJAX and Web2.0 application and is favored by programmers over XML because of its ease of use and speed.

- However, JSON, like XML is prone to Injection attacks
- A malicious attacker can inject the reply from the server and inject some arbitrary values in there

Solution

- Launch WebScarab
- Enter in the form fields for departure and destination
- Intercept the response from the server with the two flight options
- Edit the JSON code to change the price of the more expensive, direct flight
- Accept changes and go back to your web browser
- You are now able to buy the flight for the price you specified in the JSON