

Forum: [Hack Forums](#)

Thread: [Web App Bug Hunting Tips - 2 - JSON Parsing Issues](#)

?Criminal - April 6, 2018, 4:02 pm

JSON Parsing is a very complex concept and it's very hard to get right for many, tens of hundreds of different JSON parsers exist and each treat JSON slightly differently than the other. By using differential fuzzing you can try payloads across various parsers and get different results for each one. So you also must be wondering well from a web app perspective why should I care about JSON parsing? Well you should care because it can cause these major issues in web applications:

- RCE
- DoS(Denial Of Service)
- Privilege Escalation

Here are some videos and different materials on this subject:

<https://www.youtube.com/watch?v=B598kLov7TA&feature=youtu.be>
http://seriot.ch/parsing_json.php
<https://justi.cz/security/2017/11/14/couchdb-rce-npm.html>

As you can see a CouchDB RCE was found simply because there was an issue in how the JSON parser parsed user input.

You also must be wondering, well how can I start finding JSON Parsing related exploits?

Simply code up a JSON fuzzer that attacks different parsers, simply install random ones on localhost and hope one you find one with weird inconsistencies and then attempt to utilize the issues found via localhost JSON fuzzing on the production web app and hopefully you can leverage it into an RCE. Hope you guys enjoyed this tip and happy bug bounting!