

Forum:[Hack Forums](#)

Thread: [Array Injection: Bypass JSON XSS Filter \[Learn How\]](#)

Replace - November 14, 2025, 9:41 am

Hey HF members, I am back with another short tutorial for you guys, an offensive hat subject, Bypass Json XSS Filter using Array Injection. ?

Edit: Unable to post any of the codes in the forum thread, which really sucks, the new firewall rule is making things real complicated, doesn't even allow to post normal codes like bash (saw on my other thread when a user posted a bash script), I really wish any of the forum devs would fix this issue. It's over protective! ?? I have written the examples (codes) over pastebin and added in the pictures of them, hope it doesn't annoys you to understand the 'how to' and helps you to learn, so, let us start.

Bypass JSON XSS Filter with Array Injection ?

First let us take a Target Scenario : A web-service receives JSON input from the user:

Code HF doesn't allow me to post simple POST examples, so here is the example :

<https://pastebin.com/raw/z6aSi4vx>

And now let's take that the developer only filters if `msg` contains `<` or `>`.

Exploit: Use an array to bypass the usual filter that only checks `typeof msg === "string"`.

PoC Payload :

Code <https://pastebin.com/raw/jinL6qRG>

The filter fails because the value of the key 'msg' is an open string so `< & >` is not found as an array.

Code `["text1", "text2"]` is not equal to `"<"`

It is because if the server does not check the content type of each element in the array, then JS will parse and render the HTML as XSS.

As a Result; the web displays `msg` without sanitizing each element of the array.

For example :

Code <https://pastebin.com/raw/Q36PinnF>

Fix Recommendation :

Code Javascript: <https://pastebin.com/raw/6npUSyYe>

Reminder : Try in your localhost machine.

Have a good day and don't forget to QL this post.