

Forum:[Hack Forums](#)

Thread: [Web App Bug Hunting Tip - Using JsParser To Find Hidden Endpoints](#)

?Criminal - April 6, 2018, 10:38 am

<https://github.com/nahamsec/JsParser>

This tool JsParser is an extremely useful tool for a bug bounty hunters arsenal. A major step in bug bounty hunting is the content discovery stage, you crawl the main domain and tend to realize hmm this web application seems small but in actuality theres tons of hidden endpoints and directories that may contain outdated files with vulnerabilities that can be exploited by you, one way to go about this is going on archive.org and looking for old .JS files with hidden deprecated endpoints hidden in them or crawling the current live domain of the web app you're targeting and look for fresh .JS files because they may contain endpoints that you wouldn't find in the web application normally as some endpoints aren't even implemented into production properly but simply exist as a forgotten API left on the web server that ends up having useful functionality that you can exploit in your favor. When bug bounty hunting most people forget this vital step and by doing this you will be able to audit seemingly hidden parts of a web application you would not come across other wise. I hope you guys enjoyed this small little tip and I wish you all happy bug hunting! One thing I forgot to mention is JsParser helps automate the process of finding the URL's and displaying them clearly, you just supply a JS file as input.

ernestmiller - April 6, 2018, 11:05 am

(Apr 6, 2018 10:38 AM)?Criminal Wrote: [\[CITE\]](#) <https://github.com/nahamsec/JsParser>

This tool JsParser is an extremely useful tool for a bug bounty hunters arsenal. A major step in bug bounty hunting is the content discovery stage, you crawl the main domain and tend to realize hmm this web application seems small but in actuality theres tons of hidden endpoints and directories that may contain outdated files with vulnerabilities that can be exploited by you, one way to go about this is going on archive.org and looking for old .JS files with hidden deprecated endpoints hidden in them or crawling the current live domain of the web app you're targeting and look for fresh .JS files because they may contain endpoints that you wouldn't find in the web application normally as some endpoints aren't even implemented into production properly but simply exist as a forgotten API left on the web server that ends up having useful functionality that you can exploit in your favor. When bug bounty hunting most people forget this vital step and by doing this you will be able to audit seemingly hidden parts of a web application you would not come across other wise. I hope you guys enjoyed this small little tip and I wish you all happy bug hunting! One thing I forgot to mention is JsParser helps automate the process of finding the URL's and displaying them clearly, you just supply a JS file as input.

Praise be to the lord!!! Finally a good post!!! very informative thanks. I had almost given up on this forum for learning.

Gee4rce - April 15, 2018, 1:30 pm

I may give this a shot, thanks for sharing! Cheers

Rootomi - April 16, 2018, 7:58 am

thank you for sharing something special..me and maybe many people searching for that info.. keep it up mate