Dalfox – Hacker Tools: XSS Scanning Made Easy □□

BY ANNA HAMMOND · SEPTEMBER 14, 2021 · LAST UPDATED ON MARCH 6, 2025

Finding XSS can sometimes be a repetitive and laborious task. Many attempts at automating the process have been made, yet very little actually come close to getting it right. Today, we're covering Dalfox, a tool that did get it right. Let's find some cross-site scripting vulnerabilities!

□□ What is Dalfox?

> **"DalFox is a fast, powerful parameter analysis and XSS scanner, based on a golang/DOM parser. supports friendly Pipeline, CI/CD and testing of different types of XSS. I talk about naming. Dal(_) is the Korean pronunciation of moon and fox was made into Fox(Find Of XSS).**
>
> **Dalfox README.MD"**

This tool can be used to find reflected parameters, identify injection points, check for bad headers and even check for basic other vulnerabilities such as SQLI, SSTI, open redirects and CRLF.

Additionally the tool can mine parameters by brute forcing them, but also through the DOM. It will look through the output to grep for SSTI, credential leaks, SQL errors and such.

It doesn't only scan for reflected XSS though! The tool can also find stored or DOM based XSS vulnerabilities. Once it has identified an injection point, it has the ability to find a fitting payload to give you that sweet, sweet alert popup. It does this by analyzing disallowed characters, encodings and such.

How well is it fit for bug bounty hunters? Well, Dalfox has a bunch of options that you may want to use, such as setting a specific user-agent or delaying requests. This way, you can adhere to the rules of the program you're hunting on!

There's way more to discover, but that's the joy of playing around with a new tool! Use it, tune it and enjoy!

□□ Setting up DalFox

Installing this Go tool is very easy. Firstly, we clone the repository. After that, we can use **go install** and **go build** to get our very own Dalfox binary!

```
git clone https://github.com/hahwul/dalfox
cd dalfox
go install
go build
```

□□ Our first scan

Check out the video below for an example of a scan!

Conclusion

Dalfox is a powerful tool to help you get more efficient at finding XSS vulnerabilities. It won't do wonders, but it's a great way to start and limit the places you need to manually look through.

If you would like to recommend a tool for us to cover next week, then be sure to let us know down below. Also be sure to check out all the previous Hacker Tools articles, such as the last one on KiteRunner.

Did you know that there is a video accompanying this article? Check out the playlist!