

Bug Bounty — Tips / Tricks / JS (JavaScript Files)



Prateek Tiwari

Follow

Feb 21, 2018 · 4 min read



It all started in month of August when I reached out to [Gerben Javado](#) regarding a question, yes it was a basic question but a quick chat with him that day gave me some confidence to hunt for Bugs when he pointed towards his blog post [The race to the top of a bug bounty program](#), and asked me to look for Bugs in that particular program.

The game began, I never knew that I was about to turn the tables and be at the top of that program pretty soon. Within a span of 6 Months I learned a hell lot of techniques / tricks and how to read JS (that was most important for me).

Sharing is Caring :) Straight to the Point now.

Recon?



Recon Recon Recon

Everyone knows about Recon and how to do it, the most important is what more you can add in your recon techniques to find some more bugs:

Number 1 — Do you search for endpoints on Twitter, Facebook, LinkedIn, etc.? No, don't ask me how, here it is > If you know of an endpoint which returns 403 since it's an admin endpoint but have you ever imagined knowing the correct directories and parameters sometimes can turn 403 into 200 (because of misconfigurations) and then into a SQLi? ;)



Endpoint Discovered on a Social Media Platform





Result of that ^^ particular endpoint

Number 2 — CSP Headers? Anyone? It had one subdomain, I scanned for the IP ranges and found an interesting one which gave me full admin access [that report is already public ;)]. Whoaaa!

Number 3 — Google, please give me all the results which has “www.domain.com/{directory}/{directory}” > No, I’m not using site:domain.com inurl:, I’m just using DOUBLE QUOTES and as mentioned “www.domain.com/{directory}/{directory}”, this can be most of the times PITA but if you want more bugs then let’s do it. You can just modify your search based on the endpoints which you notice is being used on constant basis by the company. If you’re lucky then you can find something which can help you get ::





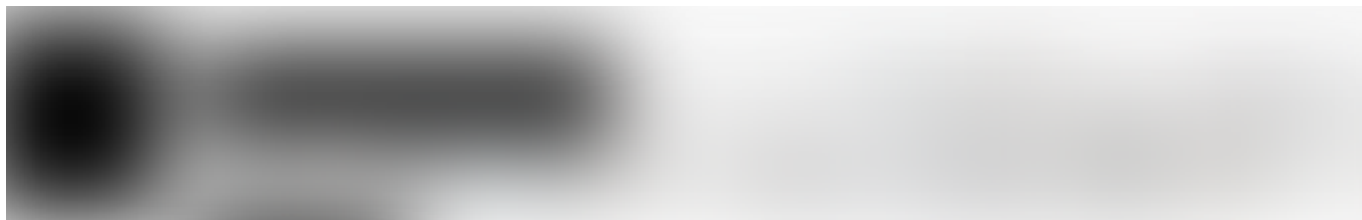
She was a nice lady who had that companies endpoint in her blog which when clicked was redirecting to her own business site. She might be having some extra privileges within her profile which allowed her to do this.

Number 4 — Don't look for Number 4, be creative ;)

Oh My JS FILES ;) I'm Loving you more and more!

There are great tools out there to look for the endpoints in JS files like JS Parser (from [Ben](#) and [Brett](#)), Linkfinder (from [Gerben Javado](#)), those are great tools but nothing can be as great as manual searches, yes those are again PITA but if you want more bugs you have to ;)

Few Examples from Manual Search:



I Love You JS :)

Yes, you read that ^^ right.



I Love you even more now ;)

JS will most of the time allow you to find something for sure, recently I was able to find an internal host of a company upon visiting it, it was only to be found that it was not accessible from outside their network. Oh really? No, let's fire Nmap and see if we can find any Open Ports. Super, later it was discovered it had Open Jenkins Instance running on port 8080 wowwww

cool it was time to execute some cmds, aaannnnnddddd using Groovy Scripts I was able to execute a cmd on the server. Woohoo!

There are couple of my reports (about JS) already published on my [H1 Profile](#) too, hackerone.com/prateek_0490.

I'd like to thank [HackerOne](#) and [BugCrowd](#) and all other companies who run a BBP and provide us with an opportunity to make this happen.

Yes, I've and I'm doing my bit in making internet a safer place :)

Questions? Hit me up on [Twitter](#) > https://twitter.com/prateek_0490

Bug Bounty

Infosec

Information Security

Security

Hackerone



1.2K claps



WRITTEN BY

Prateek Tiwari

Follow



Security Nerd | Someone who adores Information Security!



InfoSec Write-ups

Follow

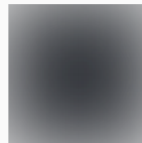
A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. Maintained by Hackrew

See responses (4)

More From Medium

Array and Object De-structuring in Javascript

Samuel Guo in JavaScript In Plain English



Dockerize Angular application

Yoshevski



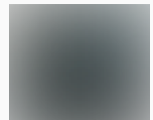
React Native: User Authentication Flow Explained

Ross Bulat



NiM Much More than UX Sugar

667



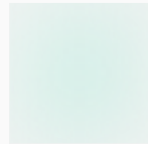
Practical data fetching with React Suspense that you can use today

Andrei Duca



The Art of JavaScript Event Delegation

Alexandra Radevich in The Startup



How to Maximize Reusability for Your React Components

jsmanifest in Better Programming



How to go from idea to URL quickly with React.js and Heroku

Tom Schweers in freeCodeCamp.org



Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. [Watch](#)

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. [Explore](#)

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just \$5/month. [Upgrade](#)

Medium

About

Help

Legal