



Java Script Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



JAVA SCRIPT – Intro

- Almost all applications use it
- Very useful source to map out an app
- Often secrets are being leaked in JS
- APIs can be discovered in JS
- Hidden endpoints can be discovered
- And much more...



JAVA SCRIPT – Dorking

- Dork on Google
- Dork on GitHub
- Dork on the actual Application
- Typical searches:
apiKey, apiSecret, x-api-key, apidocs,
/api/, /internal/api



JAVA SCRIPT – How to?

- Use either Burp or view-source
- Look for custom .js files like main.js, login.js, app.js etc.
- Don't waste time on standard one like jquery.js



JAVA SCRIPT – What to look for?

- Look for Developer comments
(for example `//` this is a dev comment
or `/*` this is a multi line dev comment `*/`)
- Look for new endpoints
- Look for keys and secrets
- Look for new parameters
- Look for hidden features



JAVA SCRIPT – Keywords

Search .js files for:

```
api
api/
internal
url:
var =
//
/*
*/
http://
https://
company.com
location.search
parameter
pathname
POST
GET
```



JAVA SCRIPT – Keywords

Search .js files for:

```
setRequestHeader  
send(  
  .headers  
onreadystatechange  
var  
getParameter()  
  .theirdomain.com  
apiKey  
postMessage  
messageListenger  
  .innerHTML  
document.write(  
document.cookie  
location.href  
redirectUrl  
window.hash
```




JAVA SCRIPT – make it readable

Beautify JS code (make it easily readable)

<https://beautifier.io>

De-obfuscate JS code (make it easily readable)

<https://lelinhtinh.github.io/de4js/>



JAVA SCRIPT – Automate search

Automate

<https://github.com/003random/getJS>

<https://github.com/jobertabma/relative-url-extractor>

<https://github.com/0xsha/GoLinkFinder>



Thank You!

Become a Successful
Bug Bounty Hunter