# Analyzing JavaScript Files To Find Bugs

Muhammad Mater · Follow
3 min read · May 23

436 5

Hi Hackers,

JavaScript plays a crucial role in web , and JavaScript files are essential components of web applications. Here are some important reasons why JavaScript files are significant in web

Interactivity: JavaScript enables developers to add interactivity and responsiveness to web pages, making them more engaging and user-friendly.

Dynamic Content: JavaScript allows for the dynamic loading and updating of content on web pages without requiring a full page reload, enhancing the user experience.

Form Validation: JavaScript enables client-side form validation, ensuring that user input meets specific criteria before submission, improving data accuracy and user experience.

JavaScript files can play a significant role in bug bounty programs, where security researchers identify and report vulnerabilities in web applications. JavaScript files can include the following:

aws access key

aws secret key

api key

passwords

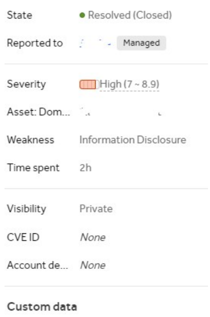
admin credential

secret token

oauth_token

oauth token secret

if you discovered sensitive information it can be reported as information disclosure and you can also benefit from this information if it contains credentials, in this case, it can be reported as broken access control and so on.

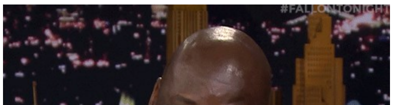


| | |
|---|---|
| State | ● Resolved (Closed) |
| Reported to | [redacted] Managed |
| Severity | High (7 ~ 8.9) |
| Asset: Dom... | [redacted] |
| Weakness | Information Disclosure |
| Time spent | 2h |
| Visibility | Private |
| CVE ID | *None* |
| Account de... | *None* |

Custom data

**Important Question: How Can I Analyze JavaScript Files ?**

it's easy just view page



Okay I'm kidding

I found valid login credentials in Java script files

Steps to do it

You'll get a list of your domains We call it domains.txt And Any Tool for Crawling URLS

Katana or Waybackurl or gau

```
cat domains.txt | katana | grep js | httpx -mc 200 | tee js.txt
```

explaining the command :

1. `cat domains.txt | katana` : This command uses the `cat` utility to display the contents of the file `domains.txt`. It assumes that `domains.txt` contains a list of domain names or URLs and pass by | to katana to crawl urls from domains
2. `grep js` : The `grep` command is used for pattern matching in text files. In this case, it is searching for lines that contain the ".js" pattern, which indicates JavaScript files. This filters the output to only include lines that mention JavaScript files.
3. `httpx -mc 200` : This command utilizes the `httpx` tool to send HTTP requests and retrieve responses from the filtered URLs. The `-mc 200` option specifies to only show URLs that return a successful HTTP status code of 200 (OK). This filters out URLs that do not exist or return errors.
4. `tee js.txt` : The `tee` command is used to display the output of a command and save it to a file simultaneously. In this case, it saves the filtered URLs that match the previous criteria into a file called `js.txt`.

Now we have java sript links

Scanning by nuclie

```
nuclei -l js.txt -t ~/nuclei-templates/exposures/ -o js_bugs.txt
```

Another Way :

Download All links in js.txt

and do search about these

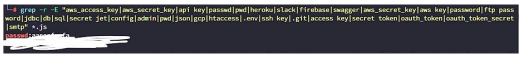
code :

```
file="js.txt"

# Loop through each line in the file
while IFS= read -r link
do
    # Download the JavaScript file using wget
    wget "$link"
done < "$file"
```

```
grep -r -E "aws_access_key|aws_secret_key|api key|passwd|pwd|heroku|slack|fireb
ase|swagger|aws_secret_key|aws key|password|ftp password|jdbc|db|sql|secret jet
|config|admin|pwd|json|gcp|htaccess|.env|ssh key|.git|access key|secret token|o
auth_token|oauth_token_secret|smtp" *.js
```

And Boom



```
└─# grep -r -E "aws_access_key|aws_secret_key|api key|passwd|pwd|heroku|slack|firebase|swagger|aws_secret_key|aws key|password|ftp pass
word|jdbc|db|sql|secret jet|config|admin|pwd|json|gcp|htaccess|.env|ssh key|.git|access key|secret token|oauth_token|oauth_token_secret
|smtp" *.js
passwd:[redacted]
```

Good Bye

My Linkedin : https://www.linkedin.com/in/micro0x00/

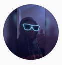
My Twitter : https://twitter.com/micro0x00

Support me :

https://www.buymeacoffee.com/Micro0x00

Bug Bounty · Bug Bounty Tips · Hacking · Bug Hunting · Recon

436 · 5



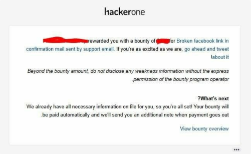
## Written by Muhammad Mater

Follow

580 Followers

Just a Boy Loves Infosec (REDTEAM, CTI, OSINT, Bug Bounty)

### More from Muhammad Mater


hackerone

[redacted] rewarded you with a bounty of [redacted] for Broken facebook link in confirmation mail sent by support email. If you're as excited as we are, go ahead and tweet !about it

*Beyond the bounty amount, do not disclose any weakness information without the express .permission of the bounty program operator*

**?What's next**

We already have all necessary information on file for you, so you're all set! Your bounty will .be paid automatically and we'll send you an additional note when payment goes out

View bounty overview

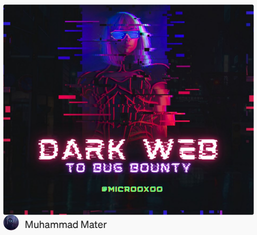
Muhammad Mater

**Easy Bugs Easy Bounty**

Hi Hackers This is a Bug For beginner hackers and Bug Hunters to get their first valid bug or...

3 min read · Sep 30

116 · 2



Muhammad Mater

**Using Dark Web in Bug Bounty**

Hi Hackers ,

5 min read · Jun 25

449 · 6

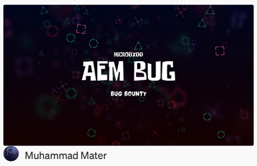
Muhammad Mater

**CVE VS CWE VS ZERO DAY WHAT THESE THINGS**

When I started cybersecurity, I was young, and I was afraid of shortcuts with 3 or 4 letters.

4 min read · Jun 5

77 · 2



Muhammad Mater

**AEM Bug in Adobe**

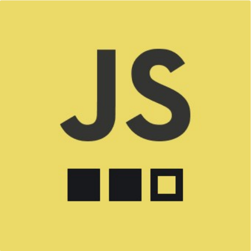
hi hackers

3 min read · May 21

99

See all from Muhammad Mater

## Recommended from Medium

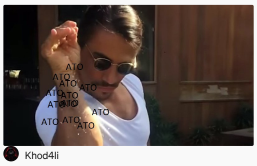


Kongsec

**How to JS for Bug Bounties : Edition 2023**

Hi everyone,

5 min read · May 18



Khod4li

**P1 XSS?**

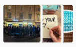
Hello to all you curious hackers. It's been two weeks since I discovered this vulnerability,...

6 min read · Oct 7

115 · 1

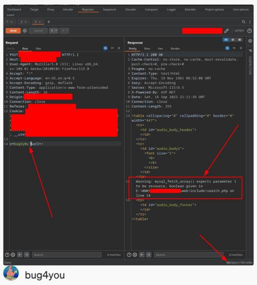
649 5

Lists



Medium Publications Accepting Story Submissions

154 stories · 822 saves



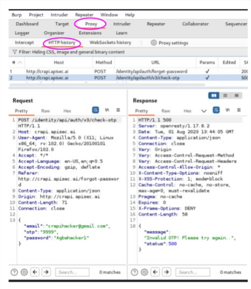
bug4you

## How I Got 4 SQLI Vulnerabilities At One Target Manually Using The...

Hi everyone, I'm Yousseff, A Junior Computer Science Student, and Cyber Security...

18 min read · Sep 19

999 13



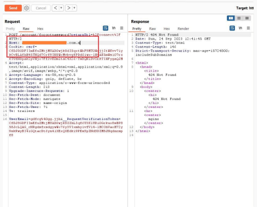
Isu Momodu Abdulrauf

## Fuzzing APIs

Fuzzing or Fuzz testing is an automated testing method where random, invalid,...

8 min read · Sep 10

129



Salman Khan

## $1,250 worth of Host Header Injection

What is Host Header Injection?

4 min read · Sep 24

711 9

Shrirang Diwakar

## Bypassing 403s like a PRO! ($2,100): Broken Access control

This article highlights my way of dealing with 403s and how I managed to get a P1 in...

3 min read · Apr 21

1.1K 8

See more recommendations