**Vulnerability Report**

# \*\*\*Vulnerability: Hidden Secrets Within JavaScript Files

\*\*Description:

Leaked Algolia API Keys Exposed Data of an application and Millions of Users. Malicious users can use this API keys to gain sensitive information from the api server which may contain confidential data.

# \*\*Instance:

https://d2zxo3dbbqu73w.cloudfront.net/fwasset-live/39f7eef1/js/jquery-1.11.2.min.js

**\*\*Steps to reproduce:**

1. Subdomain enumeration Using tool “subfinder” and save the output in a file.

Cmd – Subfinder -d freshersworld.com | tee subDomains.txt

1. Then I will use “waybackurls” tool to get related urls of all subdomains.

Cmd –. SubDomain.txt | waybackurls > frshwayb.txt

1. Then save it on a file.
2. Filter the live hosts from the output of waybackurls tool using HTTPX tool.

Cmd – httpx -l frshwayb.txt | tee Live\_Hosts.txt

1. Get all JavaScript files from the live hosts list using “Katana” tool. And save the output on a file.

Cmd – katana -u Live\_Hosts.txt | grep “.js$” | tee Js\_urls.txt

1. Searching for any secrets in JavaScript URLs using “secretfinder” tool.

Cmd-- cat’/home/kali/Desktop/Js\_urls.txt’ | while read url; do python3 Secret Fi nder.py-I $url -o cli >>> frsecret.txt;

1. Save the output of secretfinder in a file.
2. Then you will see that it list the

HEroku API KEY -> D27CDB6E-AE6D-11cf-96B8-444553540000

Google\_captcha -> 6LYjAML3EOqw1g26eCwWPjdmecULvBH5MVPoqKYr

Authorization\_api -> apiEventListeners

Twilio\_account\_sid -> ACCeyJvcmlnaW4iOiJodHRwczovL2dvb2d

Twilio\_account\_sid -> ACNeyJvcmlnaW4iOiJodHRwczovL2RvdWJ

Twilio\_account\_sid -> ACTeyJvcmlnaW4iOiJodHRwczovL2dvb2d

**\*\*Impact:**

**Leaked Heroku**  **API Keys Exposed Data of an application. Malicious users can use this API keys to gain sensitive information from the api server which may contain confidential data.**

**\*\*Severity**:

HIGH

**\*\*Tags:**

Hidden Api Keys within javascripts files.

Affected urls –

<https://www.googletagservices.com/tag/js/gpt.js>

<https://d2zxo3dbbqu73w.cloudfront.net/fwasset-live/39f7eef1/js/jquery-1.11.2.min.js>

URL:

<https://d2zxo3dbbqu73w.cloudfront.net/fwasset-live/39f7eef1/js/jquery-1.11.2.min.js>

URL: https://d2zxo3dbbqu73w.cloudfront.net/fwasset-live/39f7eef1/js/jquery-1.11.2.min.js