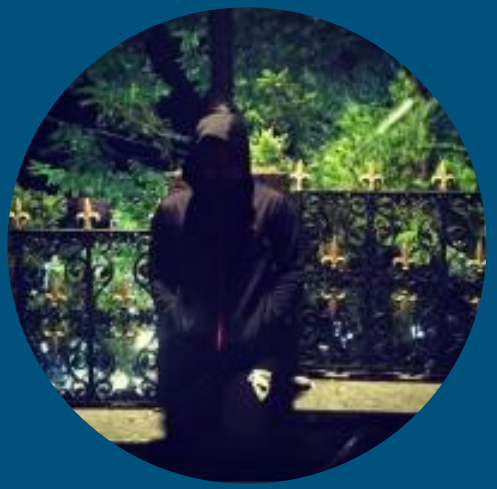
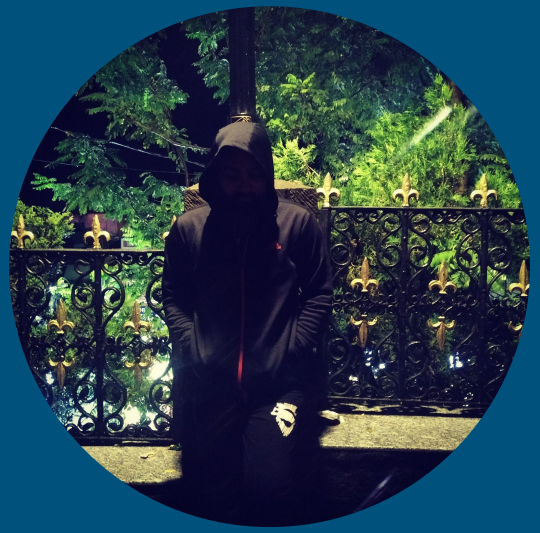
Web Application Penetration Testing Series



Finding Bugs With Afrog : Methodology

Who Am I



Sumit Jain

(Ethical Hacker & Cyber Security Expert)

Synack & Pentabug Red Team Member

Find Bugs with Afrog

- *Afrog* ： *afrog is a customizable vulnerability scanning (hole digging) tool. PoC involves CVE, CNVD, default password, information leakage, fingerprint identification, unauthorized access, arbitrary file reading, command execution, etc*

- *Installation* : *sudo go install -v github.com/zan8in/afrog/cmd/afrog@latest && sudo cp /root/go/bin/afrog /usr/bin*

Collecting Subdomains With Various Scripts

- *Subfinder : https://github.com/projectdiscovery/subfinder*
- *Assetfinder : https://github.com/tomnomnom/assetfinder*
- *Amass : https://github.com/owasp-amass/amass*

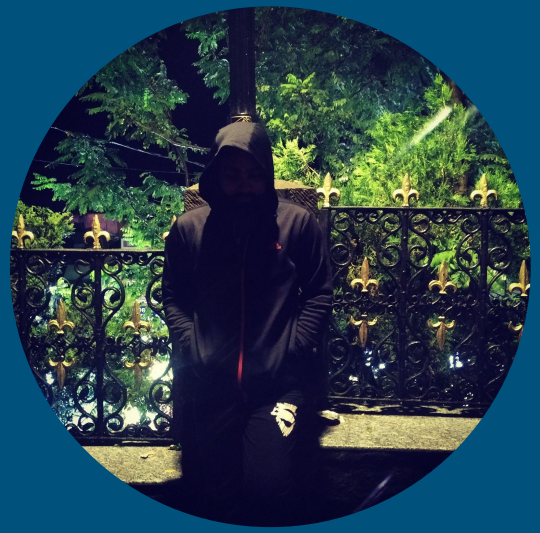
- *Alterx : https://github.com/projectdiscovery/alterx*

Collecting Urls & parameters with Scripts

- *Katana : https://github.com/projectdiscovery/katana*
- *Waybackurls : https://github.com/tomnomnom/waybackurls*
- *Gau : https://github.com/lc/gau*

Use Cases

- *afrog -t http:target.com*
- *afrog -T targetlist.txt*
- *afrog -T targeturl.txt*
- *afrog -T targetfile.txt -o result.txt*



Sumit Jain

Follow me on

Twitter : @sumit_cfe

Linkedin : @sumitthehacker

Github : @damon-sec