Renato Dante

Follow 43 Followers About

Bug Bounty tip Automating SSRF

Renato Dante Dec 15, 2020 · 2 min read

First of all, I want to clarify that I am not fluent in English, so mistakes will happen during the reading :) If tou have some question call me in instagram

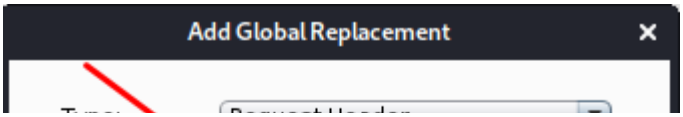
Hey, what's up?
In this article i will share a little tip about how we can automate SSRF scan for bounties. Ok Let's go.

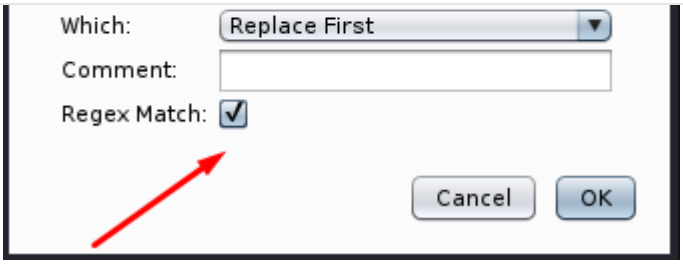
In BurpSuite we have a a great extension called "Auto-Repeter". How does it's work? Basically you can define some patterns (regex), that if found the auto-repeater will create a new request replacing for what you want.

I don't know if it's clear, let's explain with images.

In this window in Auto-Repeater we can set some regex to find urls. In this case i will use this regex.

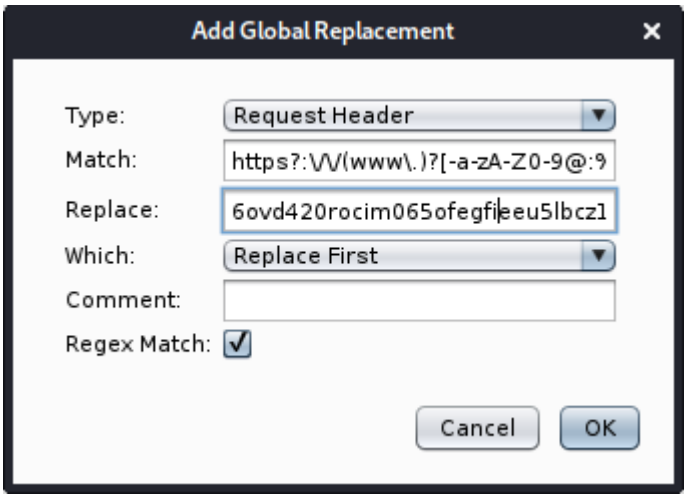
> *https?:\/\/(www\.)?[-a-zA-Z0–9@:%._\+~#=]{1,256}\.[a-zA-Z0–9()]{1,6}\b([-a-zA-Z0–9()@:%_\+.~#?&//=]*)*



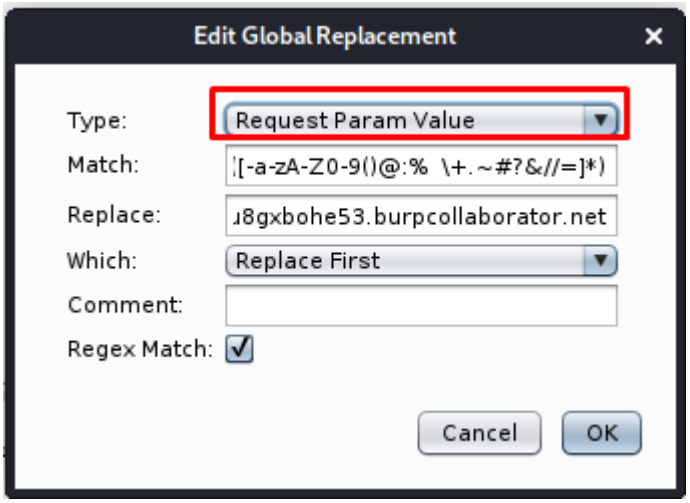


This regex only match if in url has “https”. You can do your regex to be better :)

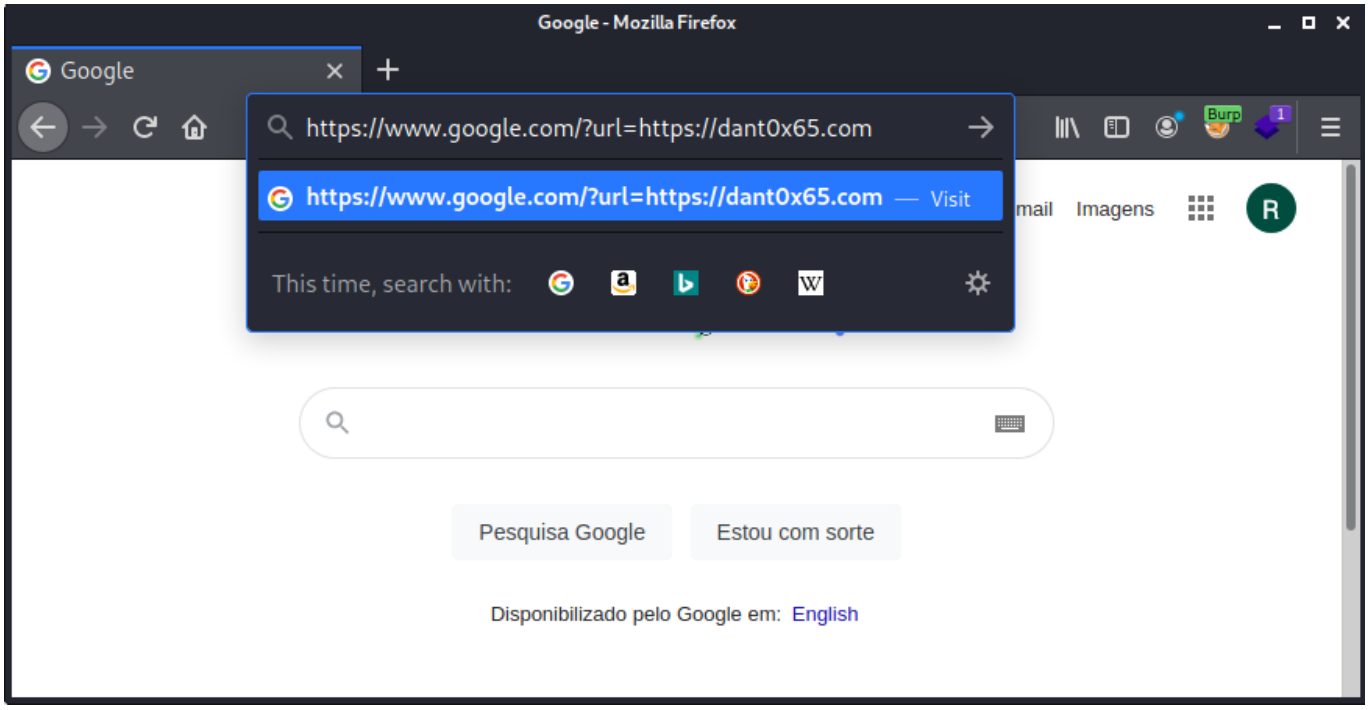
In replace field you can put your domain or burp collaborator’s url. Like this



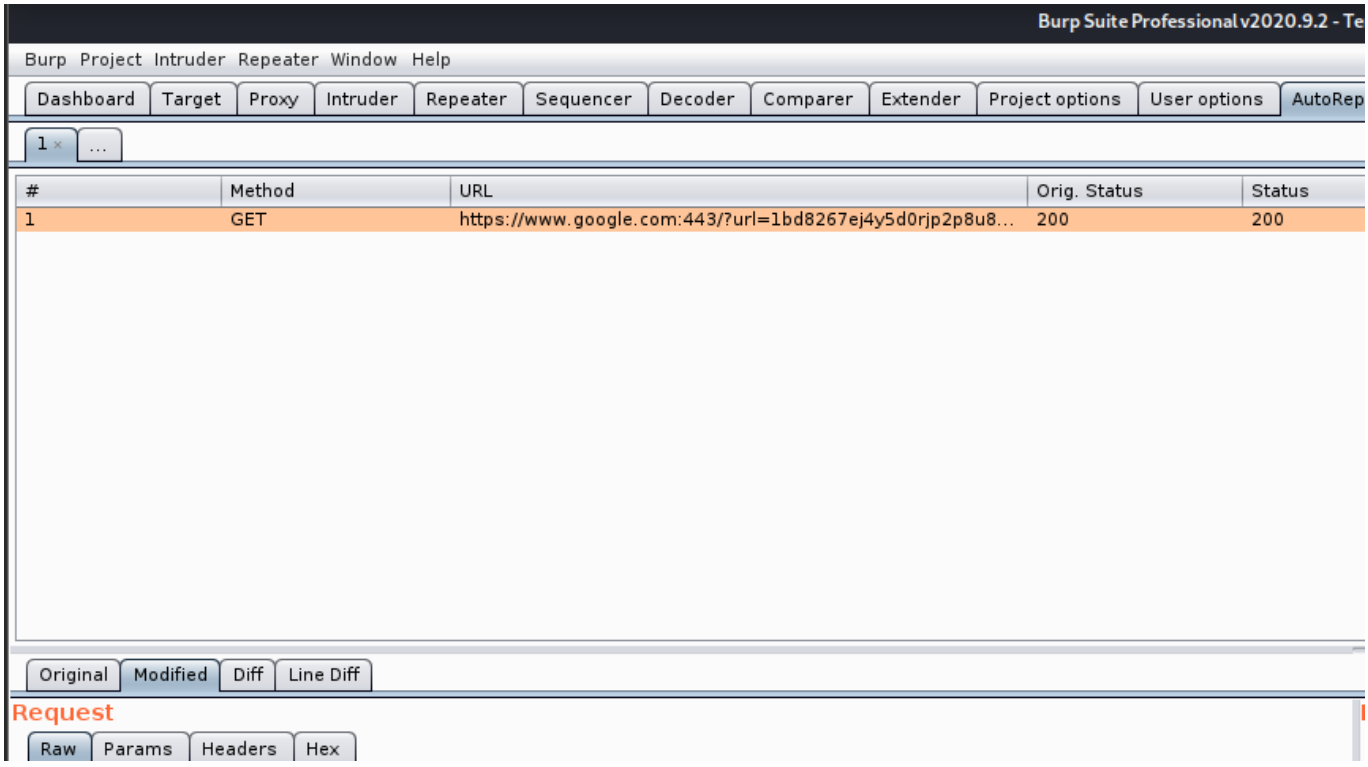
In type field you can set what you prefer, in this case i will use “Request param value”



When i'm do a GET request with url in parameter value the Auto-repeater will create a new requests replacing the url param value



Here is the url changed automatically.



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

Conclusion

You can put this setting and navigate through the site, during navigation monitor all the requests that your domain has received

Bug Bounty Hackerone Bug Bounty Tips Pentesting Pentest