The Art of Monitoring Bug Bounty Programs

YoungVanda · Follow
Published in InfoSec Write-ups · 3 min read · Sep 26

In the name of Allah

Hi guys, I'm YoungVanda and in this write-up I wanna talk about how I monitor BBPs (Bug Bounty Programs) + Introducing you to a new made private tool.

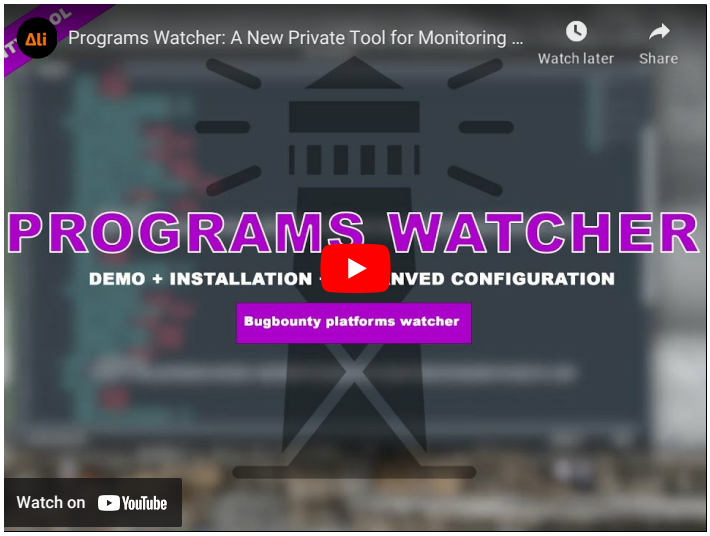
The Mindset

What would've happened if you were the first hunter working on a target? Or if you could possibly see every single changes of the programs, in all platforms(HackerOne, Bugcrowd, Intigriti, Yeswehack).
Good news baby

Introduction to Program-Watcher

This is a new tool developed by Ali Khalkhali, called Program-Watcher. This tool gets the latest changes and updates(Added Scopes, Removed Scopes, New Added Programs and much more details) of bug bounty platforms.

If you don't know how to install and work with the tool, check out the video:



What's the point

Basically by this tool, we gonna find fresh targets, they could be new scopes or new programs. It literally means, we are one of the first hunters working on these assets.

Yeap, that's a good news, finally . Yeap!?

The Points

- No more duplicates.
- Running Nuclei, in this scenario, might give you more bugs.
- Hunting XSS with Wayback + kxss is possible.
- Hunting XSS with Google Dork is possible.

I only use the last technique, for now, and I'm gonna tell you about my own approach. But you can be creative and do something crazy with the fresh targets

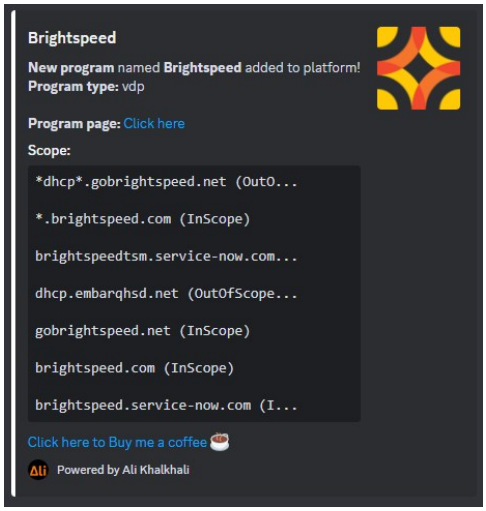
Note:

- I use this method quite often and I was quite successful in this regard. Even Ranked 1 in a Hall of Fame of a VDP Program
- Also, some of my friends use this technique for RDP targets and they've performed quite well so far.
- It's totally up to you, The way that you want to use the tool. But eventually that's a good start. Because you're the first hunter

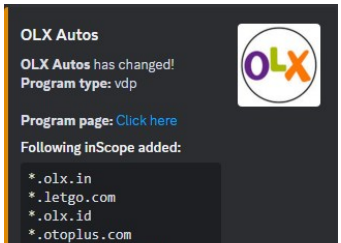
How I take advantage of program-watcher

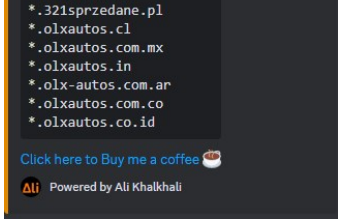
First of all, I wanna say that you can take advantage of any recent changes, please be creative. But I have my own approach for this matter.

I'm more fond of **New Programs** and **New Added Wild Scopes**. Like these messages:



I like this message: New Program named STH added to platform





I like this message: Following New inScope added (with lots of Wild scopes Yummy)

Fresh Targets + Google Dorks

I only use Google Dork technique for fresh assets. You can run Nuclei or run Wayback + kxss. The key in my methodology is that I only look for legacy applications. Just looking for easy XSS

Here are some Google Dorks I use more often than not.

```
site:*.newwild.tld ext:php
site:*.newwild.tld ext:jsp
site:*.newwild.tld ext:asp
site:*.newwild.tld ext:aspx
site:*.newwild.tld ext:htm
site:*.newwild.tld ext:html
```

I hate copy & pasting dorks, so I've made a simple dork generator.
You can check out my github to see all the dork I use:

GitHub - youngvanda/google-dork-generator: My Handy Google Dorks for Hunting/Pentesting

My Handy Google Dorks for Hunting/Pentesting. Contribute to youngvanda/google-dork-generator development by creating an...

github.com

For example, when I use this dork:

```
site:*.newwild.tld ext:php
```

I usually find endpoints like:

```
https://sub.newwild.tld/sth/sth/endpoint.php
```

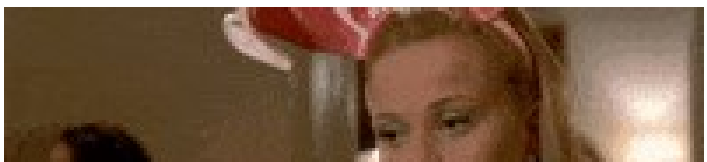
So here I do parameter discovery with x8. Also, now I know that this application is legacy, it means it is a bit old + good spot for old bug types like: XSS, SQLi, etc.
Therefore, I fuzz . I fuzz till the apocalypse, metaphorically speaking .
I fuzz for hidden endpoints, hidden parameters.
So make your own private word-list. Use raft-large and mix it with some other word-list repositories together and now you're good to go.

Here, Some fuzzing scenarios I use most of the times:

```
https://sub.newwild.tld/sth/sth/FUZZ.php
https://sub.newwild.tld/sth/sth/FUZZ
https://sub.newwild.tld/sth/FUZZ
and so on
```

Final Thing :)

Yeah man. That was all I knew. Was this write-up good enough?



Never mind . Please let me know. If you have any question, I would be more than glad to help you

Take care kings

Oh man... Wait a minute, I tweet about my recent findings and some other bug bounty tips. So check out my tweeter account . Sorry X account :)

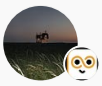
My Twitter Account: @young_vanda_

Resources:

- https://www.youtube.com/watch?v=V6d6_YVUSR8
- https://github.com/Alikhalkhali/programs-watcher
- https://github.com/youngvanda/google-dork-generator

Bug Bounty | Infosec | Cybersecurity

285



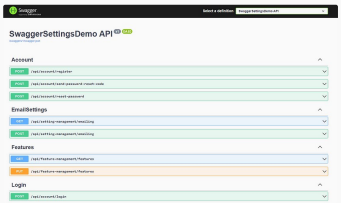
Written by YoungVanda

Follow

122 Followers · Writer for InfoSec Write-ups

bug hunter, used to be a professional chess player, now an amateur boxer

More from YoungVanda and InfoSec Write-ups



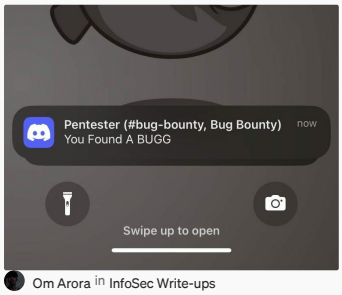
YoungVanda in InfoSec Write-ups

Swagger XSS Mass Hunting

Hi guys, in this write-up, I'm gonna explain my own approach towards Swagger XSS and why..

2 min read · Jul 29

156 4



Om Arora in InfoSec Write-ups

Find Bugs While Sleeping ? Get Phone Notifications When A Bug I...

Hello Everyone!

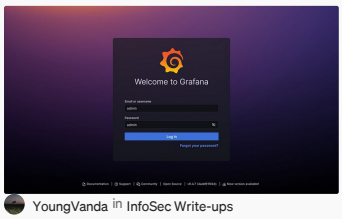
4 min read · Sep 16

302

iam_with_you11 in InfoSec Write-ups

Instagram Password Hacking

Hii Amigos in todays article we were going to learn how to hack Instagram passwords by...



YoungVanda in InfoSec Write-ups

My Second VDP Bug Went Critical: Grafana Admin Panel Bypass

Hi guys, in this write up I wanna talk about my

2 min read · Feb 23

716 16

own methodology for finding Grafana admin...

3 min read · May 18

257 6

See all from YoungVanda | See all from InfoSec Write-ups

Recommended from Medium

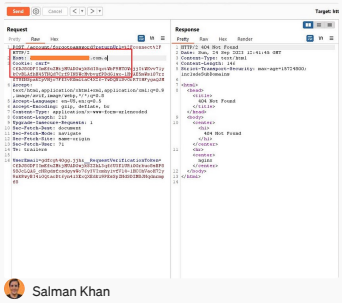
Gokulvinesh

RCE | XSS via Image Exif metadata

Hello guys,

3 min read · Sep 13

132 1



Salman Khan

$1,250 worth of Host Header Injection

What is Host Header Injection?

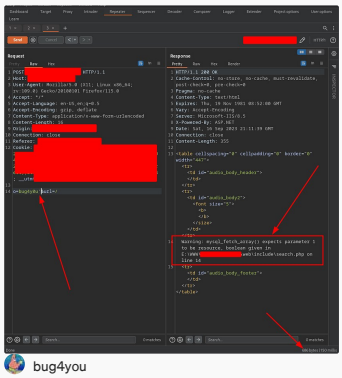
4 min read · Sep 24

713 9

Lists

Medium Publications Accepting Story Submissions

154 stories · 824 saves



bug4you

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

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

18 min read · Sep 19

1K 14

Khod4li

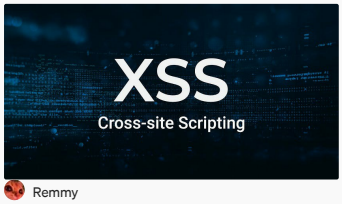
P1 XSS?

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

6 min read · Oct 7

115 1

Parkerzanta



Remmy

Earn Money with Fun! Find Vulnerability in Random Sites

This article I will tell you about how I make money from sites that do not have a Bug...

5 min read · 6 days ago

157 1

403 Forbidden? No Problem, Here's a POST XSS

Greetings to all the brilliant minds in the hacking community! I go by the name Remm...

3 min read · Oct 5

293 4

See more recommendations