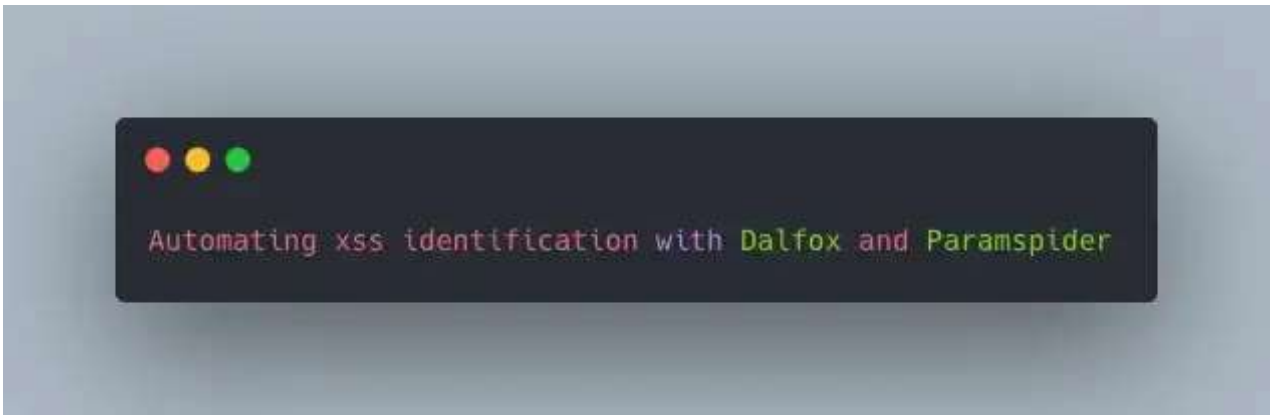
Published in InfoSec Write-ups

Paras Arora Follow
Oct 27, 2020 · 2 min read · Listen

Automating xss identification with Dalfox & Paramspider



Cross Site Scripting allows an attacker to inject malicious javascript code in the web application through some parameters and can be escalated further to perform attacks such as cookie stealing , session hijacking etc.

Types of XSS:

- Reflected XSS
- Stored XSS
- DOM Based XSS

How it all started?

I recently got an invite for a private program on BugCrowd and I immediately went through the details and found that all the subdomains are in scope.

So, I went further and started enumerating the subdomains using various tools

amass , sublist3r , subfinder , findomain-linux , crt.sh , assetfinder and saving result from every tool in txt files.

```
amass enum -d target.com -o /filepath/subdomains.txt
```

Then after getting a huge collection of subdomains sorted them uniquely and resolved them with httprobe.

```
sort -u subdomains.txt | httprobe > /filepath/uniq.txt
```

Now it became very difficult for me to check for 50+ subdomains manually by opening them in browser.

Decided to use eyewitness to screenshot every subdomain response.

```
eyewitness --web -f uniq.txt -d /path_to_save_screenshots
```

It took few minutes and after that I just wrote a simple script to embed those png screenshots with html so that I can view them directly in my browser.

```
for I in $(ls); do
        echo "$I" >> index.html;
        echo "<img src=$I><br>" >> index.html;
done
```

After all of this I found one subdomain from which I decided to proceed with my testing.

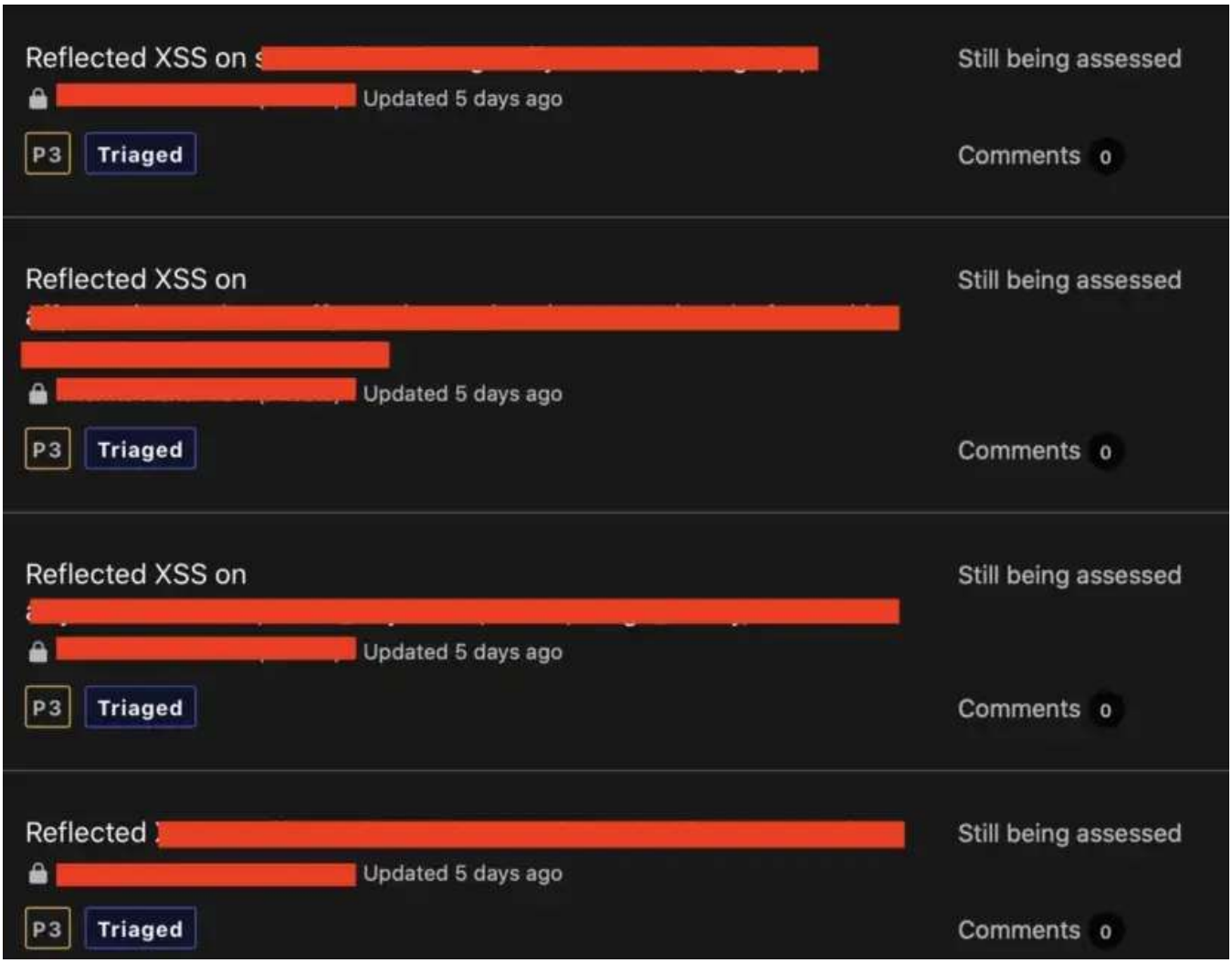
I used paramspider to extract the parameters of that subdomain

```
paramspider -d target.com > /filepath/param.txt
```

After saving the parameters in the file, automating it with dalfox

```
dalfox -b hahwul.xss.ht file param.txt
```

and after few minutes of patience I got 10 xss executed.



Twitter: http://twitter.com/parasarora06

Linkedin: http://linkedin.com/in/parasarora06

Cybersecurity Hacking Bounty Program Tech Technology