How I was able to find 100+ XSS in the United nations Bug Bounty Program

mrpentestguy · Follow
3 min read · Sep 16, 2021

194 2

Hey, Guys so this is my first blog. so I thought maybe give it try to show people how you could find bugs in an easy way

So let's get started

First After my recon for 4 days. I started to look for URLs. URLs of your choice may be from Wayback or live URLs from the website by crawling. so first I started for archive ones

For that, you could any tools of your choice. but for me, I used 2 two tools. Those are waybackurls and gau. I choose these two tools both combined like I would take URLs from both of them because of the fact. when I did my recon and send those subs to these tools. I have found out that both of these tools would give me new or different URLs and it kind of differs from the number of URLs found. Sometimes I would be getting more URLs from waybackurls tool written by tomnomnom other times i would be getting from gau. So yeah I kinda mix them and use them together.

So After i got all my urls i started for hunting XSS . My methology is different. I would look for only one type of bug for a long period of time . So I found a wooping of 1700000 urls at the end .

Now what Since I got my urls . I started using kxss this also amazing tool which was written by tomnomnom and I stored all the urls which were reflecting certain Unfiltered special characters . Now I picked those urls from it and started using dalfox .

You could use it as

```
cat urls.txt | kxss | awk '{print $4}'| sort -u >> xss_list.txt
```

or you can pipe it to dalfox directly as well which is up to you

```
cat urls.txt | kxss | awk '{print $4}'| sort -u | dalfox pipe -b <you blind xss> — custom-payload <your payload> -w 300 — multicast — mass — only-poc -o xss_vulns.txt
```

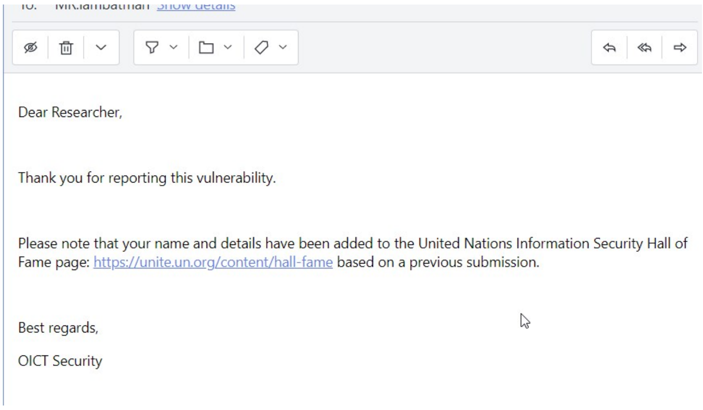
Here I found a xss with my custom payloads list i have created on my own .But one thing that striked me that the end parameter "lng" called language was found in 300+ urls from one domain lets say reacted.com and when i started to find if all the lng parameter were vulnerable or not . To me Only 179 urls were vulnerable since those urls exits . The reset of the urls didn't exist or return 404 .

The Funny thing was i able to find xss in 404 pages as well since it would not be vulnerable because there is nothing to exploit on the page .

. . .

Finally submitted to them in March -5th .

Was given hall of fame in April 22nd



To: Mr.Iambatman Show details

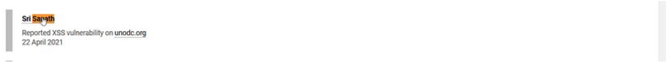
Dear Researcher,

Thank you for reporting this vulnerability.

Please note that your name and details have been added to the United Nations Information Security Hall of Fame page: https://unite.un.org/content/hall-fame based on a previous submission.

Best regards,

OICT Security



Sri Sanath
Reported XSS vulnerability on unodc.org
22 April 2021

Thank you for reading

Infosec · Information Security · Bug Bounty · Hacking · Security

194 · 2

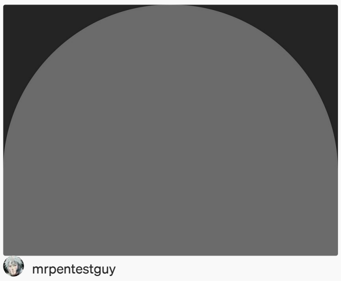
Written by mrpentestguy

Follow

156 Followers

Security Researcher | Bug Bounty hunter | Security Engineer | CTF player | OSINT

More from mrpentestguy



mrpentestguy

Blind SQL Injection

Today we will learn how we can find blind SQL injection and also at the end I will give you…

3 min read · Oct 11, 2021

137

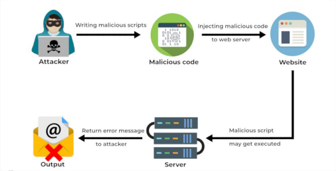
mrpentestguy

How I found a Command injection bug

Hey, guys today I want to show you how I was able to find a command injection bug through…

3 min read · Oct 19, 2021

65 · 5



Attacker
Writing malicious scripts
Malicious code
Injecting malicious code to web server
Website
Malicious script may get executed
Server
Return error message to attacker
Output

mrpentestguy in CodeX

Different types of BruteForce attacks

What is Brute force attack

4 min read · Sep 30, 2021

mrpentestguy

Remote code execution (RCE)

What is an RCE attack?

3 min read · Oct 19, 2021

6

See all from mrpentestguy

Recommended from Medium

Parkerzanta

Unauthorized Access to Admin Panel & SQL Injection

Introduction

5 min read · 6 days ago

56 3

□ ● #1[redacted]58 Account Take Over via Email Invitation October 13, 2022
[redacted] Critical

□ ● #18[redacted]06 Account Take Over via Email Invitation (Bypass report [redacted]) January 10, 2023
T[redacted] · Critical

Severity	Critical (9 ~ 10)
Asset: Dom...	www.[redacted]com
Weakness	Improper Access Control - Generic
Bounty	$1,500

lamscun

How do I change HTMLi from Low to Critical? Is your mailbox safe?

In this post, I'm just sharing how I increased the impact of regular HTMLi bugs from Low t...

6 min read · Oct 6

192

Lists

Medium Publications Accepting Story Submissions

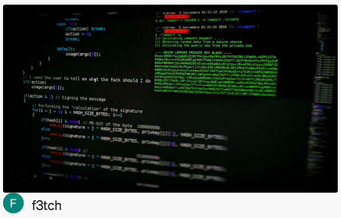
154 stories · 836 saves

Pratik Dabhi

Web Application Vulnerabilities: CRLF Injection and Beyond

4 min read · 6 days ago

72



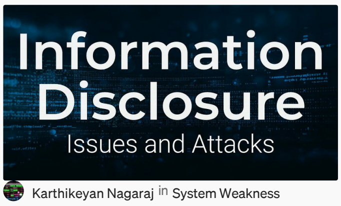
f3tch

My First Bug: A Unique $500 XSS.

whoami

4 min read · Jun 8

521 9



Karthikeyan Nagaraj in System Weakness

Information Disclosure: A Crucial Aspect in Bug Bounty Hunting |...

Unveiling the Hidden Dangers: A Guide to Tackling Information Disclosure...

3 min read · May 22

33

Boogsta

Email HTML Injection? How I did it

It's been a while and I have been very busy with bug finds so I'll be going over a few in th...

3 min read · Oct 7

13

See more recommendations