Recon — my way.

Sahil Ahamad Follow
Jun 5, 2018 · 10 min read

A detailed blog post on my reconnaissance processes for web applications security testing. I always wanted to write about this subject being asked by many friends, community members, etc. but I hooked wasting a lot of hours on a Meme Channel & The Big Bang Theory TV Series.

UPDATE: I created a GitHub repository with tools from this post and personal installation guide.

ehsahil/recon-my-way

recon-my-way — This repository created for personal use and added tools from my latest blog post.

github.com

yes, I did !! 🌋

Recently, some new members of the InfoSec community asked me to share my recon process. Hence, I decided to begin writing this blog and tried to include such tools and services which helps me a lot while testing and will help the readers too, for sure.

Summary

1. **Introduction**
2. **A tool I modified.**
3. **Visual recon**
4. **More Assets—More findings—More win.**
5. **Data Storage Buckets.**
6. **Github for Recon.**
7. **Read Every JS**
8. **Archive**

9. **Continuous Recon**
10. **Extra points for recon.**

1. Introduction

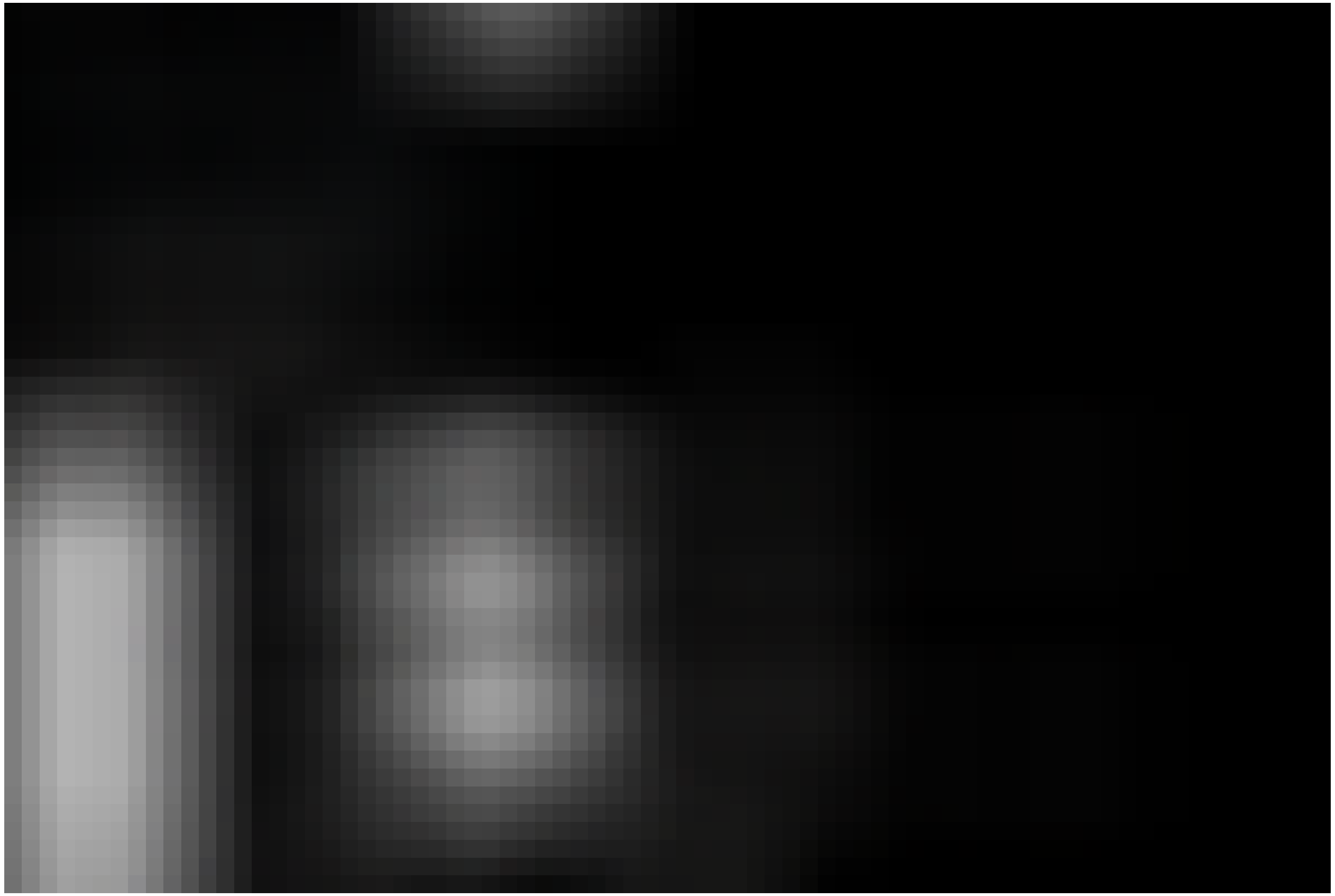
Whenever I get an invitation for a new program or I want to test a target, I start my recon process by using the **Knockpy**.

Why I use knockpy Initially? It provides me with a quick overlook of the subdomains with a response code.

Once, I found a subdomain takeover bug within 2 mins.

I ran knockpy on an old program’s in-scope asset with almost 150 bugs resolved on HackerOne. Quickly saw 404 page pointed to AWS S3 bucket and bucket were available to create. Hence, with no delay, I created the new AWS S3 bucket and uploaded a text file with the encoded filename and reported the bug and guess what? I got the bounty that too within 15 mins.

Lesson: knockpy = quick win



see 404 error in above screenshot == Quick win.

• • •

2. A Tool I Modified.

I use a customized tool for subdomain reconnaissance.

I used a resolver tool by Malvinsh and customized it.

melvinsh/subresolve

subresolve — Resolve and quickly portscan a list of (sub)domains.

github.com

Malvinsh resolver tool runs as.

Malvinsh Tools Original output.

Malvinsh tool is doing two simple processes.

- Getting the IP address of the domain/subdomain from the wordlist using **HOST.**
- Performing the Nmap scan.

Using its logic I created two scripts.

- **Subdomain.rb**
- **Recon.rb**

Caution: Do not use these scripts on programs where automatic testing is forbidden and also on the targets on which you are not allowed to.

. . .

Subdomain.rb

Subdomain.rb is a lightweight script to automate tools for subdomain finding and it’s damn flexible—more tools can be added easily.

Subfinder and sublist3r results sometime overlap. I tried to run both tools separately on a particular asset and got some distinct results—that’s why I kept both tools in this script.

The script is using the following tools to get the subdomains data.

- Subfinder

Ice3man543/subfinder

subfinder—SubFinder is a subdomain discovery tool that can enumerate massive amounts of valid subdomains for any...

github.com

- Censys subdomain finder.

christophetd/censys-subdomain-finder

censys-subdomain-finder — ⚡ Perform subdomain enumeration using the certificate transparency logs from Censys.

github.com

- Knockpy

guelfoweb/knock

knock — Knock Subdomain Scan

github.com

- Sublist3r

aboul3la/Sublist3r

Sublist3r — Fast subdomains enumeration tool for penetration testers

github.com

- Aquatone

michenriksen/aquatone

aquatone—A Tool for Domain Flyovers

github.com

subdomain.rb gist.

> *Usage: ruby subdomain.rb domain.com*

Subdomain.rb demo run.

I, usually, create a file and add all subdomains from the above outputs. Then, I use the **sort** command to delete all duplicate/overlapped subdomains from the file.

> ***sort wordlist | uniq***

I pass the final unique subdomains file to the recon.rb

. . .

Resolve.rb

Recon.rb is another lightweight script and it is also flexible hence, more tools can be added easily.Tools included in recon.rb

- **Host** : Resolve the subdomain.

- **Nmap** : Perform Port scan on subdomain

Nmap: the Network Mapper — Free Security Scanner

Nmap Free Security Scanner, Port Scanner, & Network Exploration Tool. Download open source software for Linux, Windows...

nmap.org

- **AWS CLI**—In the script AWS, CLI used test subdomains are connected to AWS bucket or not also checks for list permission. (Can be customized to test for write permission files.)

AWS Command Line Interface

The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and...

aws.amazon.com

- **Dirsearch**—Search for directories with default wordlist and all (*) extensions.

maurosoria/dirsearch

dirsearch—Web path scanner

github.com

recon.rb gist.

> *Usage: ruby recon.rb wordlist*

Recon.rb demo run.

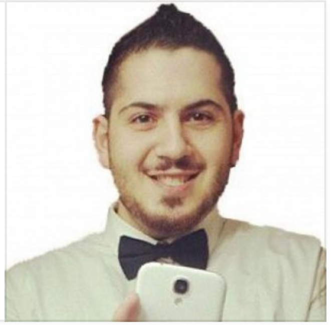
A tool with Above functionality in the organized fashion.

Lazyrecon

nahamsec/lazyrecon

lazyrecon — This script is intended to automate your reconnaissance process in an organized fashion

github.com



Interesting blog posts

[BugBounty] Decoding a $😱,000.00 htpasswd bounty

A Private Bug Bounty Program had a globally readable .htpasswd file. I cracked the DES hash, got access to development...

blog.it-securityguard.com

Scanning the Alexa Top 1M for .DS_Store files

Some readers may remember our Analysis of .git folders in the Alexa Top 1M. WIth our tools, we were able to discover and...

en.internetwache.org

. . .

3. Visual Recon

I use the previously generated wordlist from subdomian.rb for visual recon.

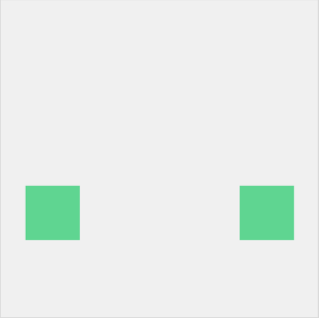
I generally use the following two tools.

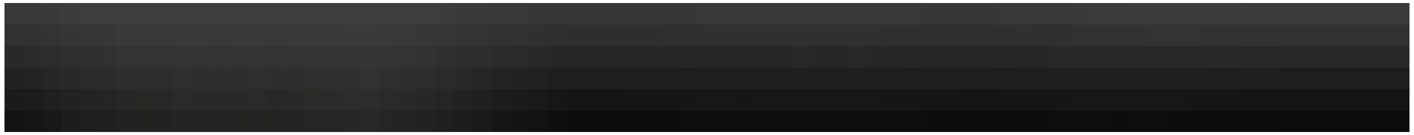
- **WebScreenshot**

maaaaz/webscreenshot

webscreenshot—A simple script to screenshot a list of websites

github.com



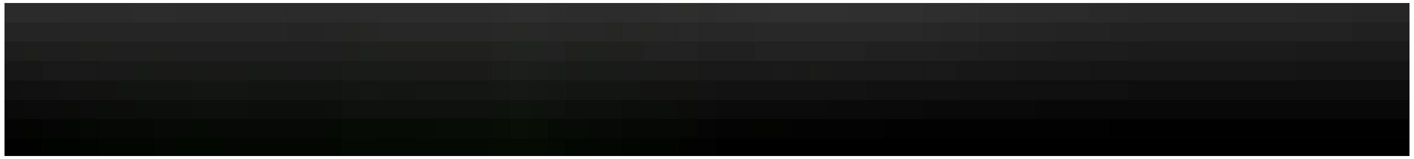


- **Lazyshot**

mdhama/lazyshot

lazyshot—The simplest way to take an automated screenshot of given URLs. Easy installation! Edit

github.com



Interesting blog posts

[Tools] Visual Recon — A beginners guide

During the process of RECON you often get thousands of domains you have to look at. A suitable way to decrease the time…

blog.it-securityguard.com

· · ·

4. More Assets — More findings — More win.

I go for this section after reporting 2–3 issues in a particular program and wait for the response, if I find program interesting then I try to collect as much information as I can about the target using the following services.

- **Censys**

Censys

Censys is a platform that helps information security practitioners discover, monitor, and analyze devices that are…

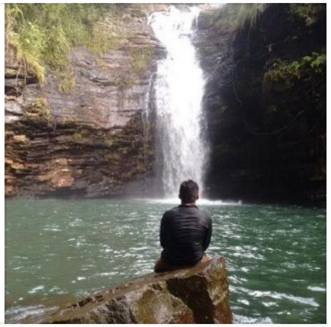
censys.io

Tool for Censys:

yamakira/censys-enumeration

censys-enumeration — A script to extract subdomains/emails for a given domain using SSL/TLS certificate dataset on…

github.com

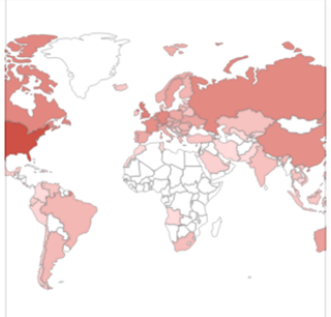


- **Shodan**

Shodan

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence…

www.shodan.io



- **ViewDNS**—Reverse Whois Lookup.

ViewDNS.info—Your one source for DNS related tools!

Reverse IP Lookup Find all sites hosted on a given server.

viewdns.info

Get the whois information of target using whois command or use an online tool.

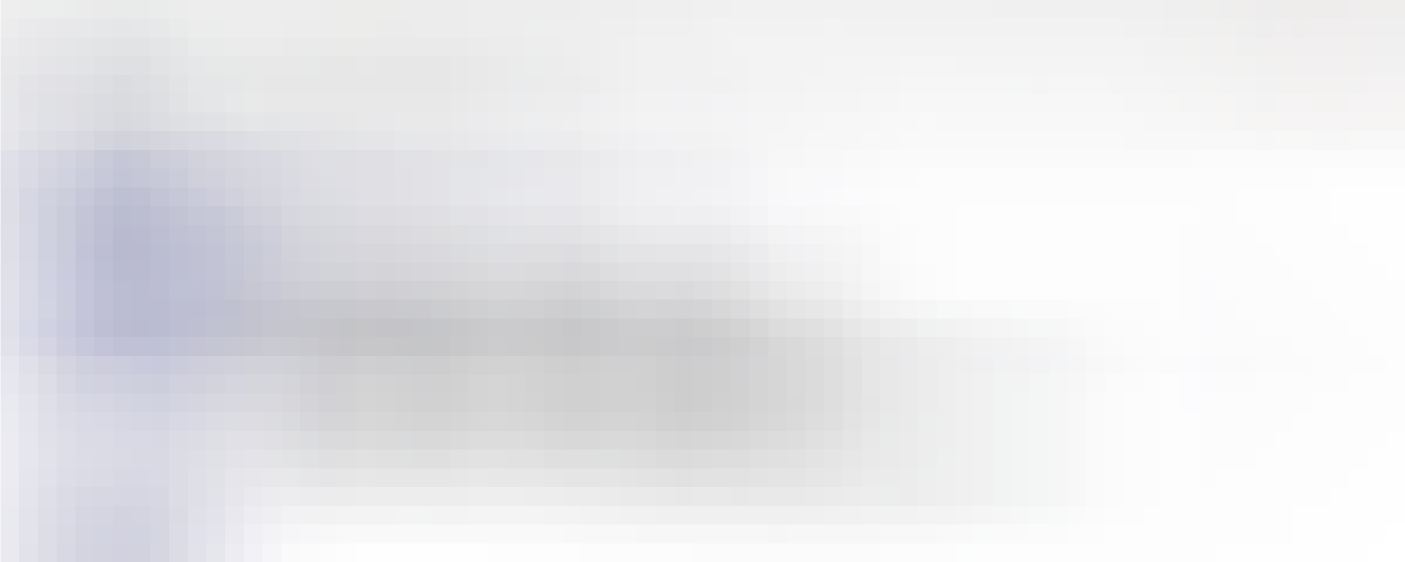
> ***whois domain.com***

If the company is not using Domain Privacy Service,

you will find the host-masters email address then use that email to find other domains registered on same email address using Reverse Whois Lookup. Targets Registered legal name also can be used.

Result for hackeone inc query

- **IP range Crawl**



IP range for hackerone.com

- **AltDNS**

infosec-au/altdns

altdns — Generates permutations, alterations and mutations of subdomains and then resolves them

github.com

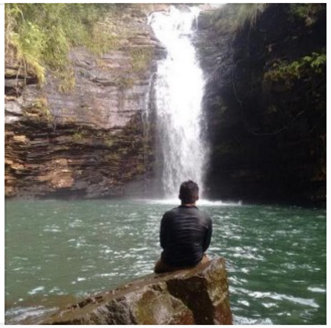
- **Nmap Subdomain finding.**
- **Content-Security-Policy (CSP)**

Tools

yamakira/domains-from-csp

domains-from-csp — A script to extract domain names from Content Security Policy(CSP) headers

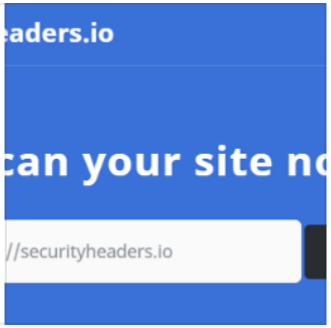
github.com



Analyse your HTTP response headers

Quickly and easily assess the security of your HTTP response headers

securityheaders.com



- **More targets with Burp Suite** by **Jason Haddix**

Jason Haddix Tweet about the method

- **Domain Analyzer**

eldraco/domain_analyzer

domain_analyzer—Analyze the security of any domain by finding all the information possible. Made in python.

github.com

- **Domain Profiler**

jpf/domain-profiler

domain-profiler—Given a domain, will tell you the decisions that the domain owner has made.

github.com

- **VHost Scan**

codingo/VHostScan

VHostScan — A virtual host scanner that performs reverse lookups, can be used with pivot tools, detect catch-all…

github.com

- ## ThreatCrowd

Threat Crowd | Threatcrowd.org Open Source Threat Intelligence

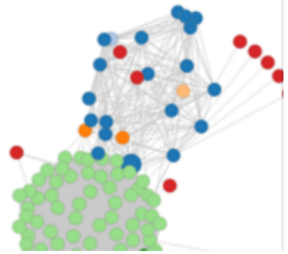
© Copyright 2017 AlienVault, Inc. | AlienVault Products | AlienVault Solutions | Open Threat Exchange | Security…

www.threatcrowd.org

- ## Visual Site Mapper

Visual Site Mapper — Create a visual map of your site

Visual Site Mapper is a free service that can quickly show an interactive visual map of your site.



www.visualsitemapper.com

- **Certificate Transparency**
- **Google Transparency Report**

Google Transparency Report

Edit description

transparencyreport.google.com

- **Certsspotter**

https://certspotter.com/api/v0/certs?domain=hackerone.com

- **CertDB**

CertDB — SSL certificates search engine

CertDB is a search engine for SSL certificates. It allows for exploration and analysis of data about organizations...

certdb.com

- **Crt.sh —**

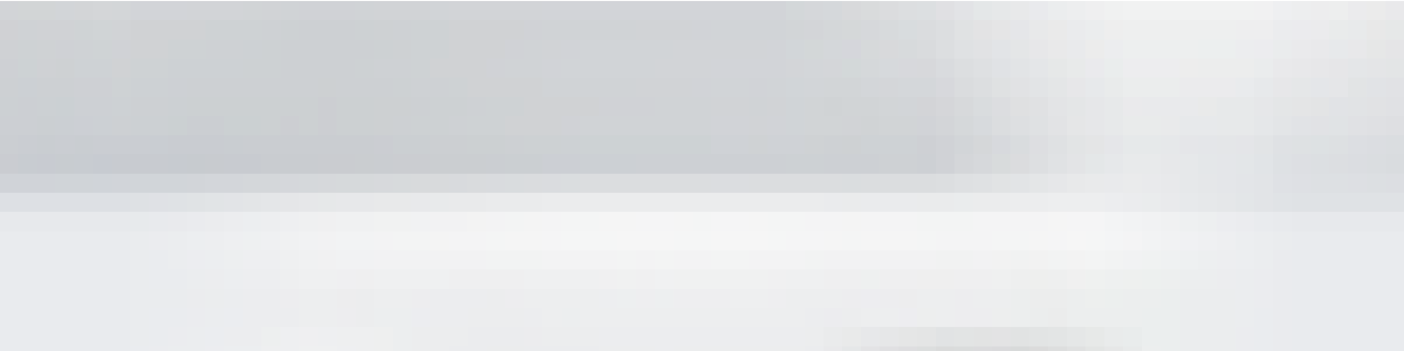
https://crt.sh/?q=%25domain.com

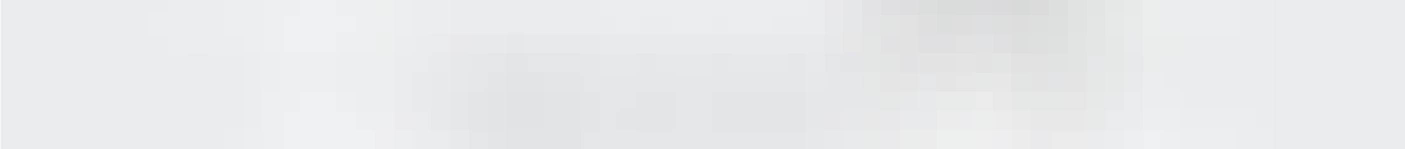
- **Facebook Certificate Transparency Monitoring Subscriptions.**

Certificate Transparency Monitoring — Facebook for Developers

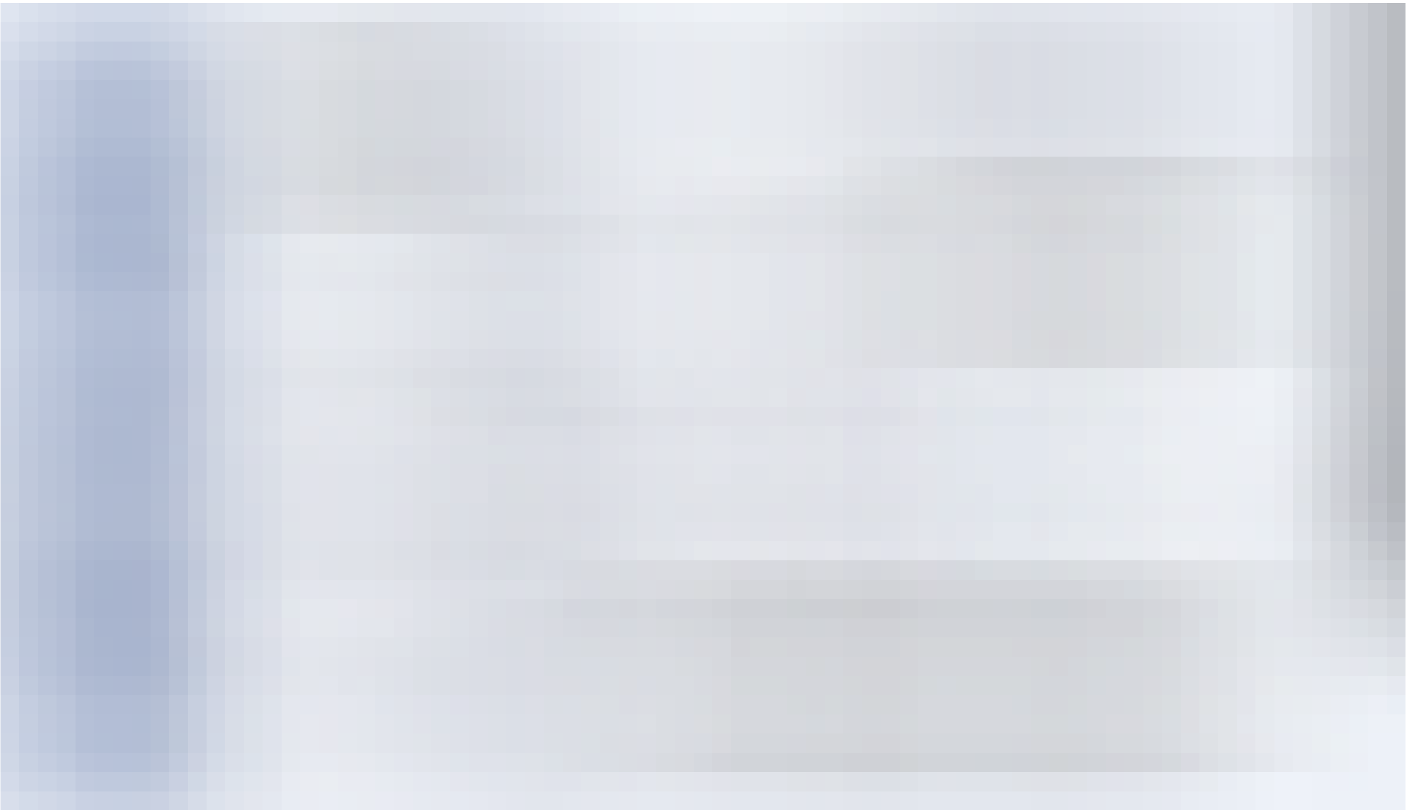
Edit description

developers.facebook.com





Facebook Crt transparency monitoring subscriptions.



Typical notification from Facebook when new asset on the same crt is available.

Interesting blog posts & tools taken from

Asset Discovery: Doing Reconnaissance the Hard Way

Last week, I wrote about Project Sonar as a great source for reconnaissance tasks. In this post, I want to generalize...

0xpatrik.com

Subdomain Takeover: Thoughts on Risks

Last year, I wrote about subdomain takeover. Although the concept is now generally understood, I noticed that people...

0xpatrik.com

Subdomain Takeover: Proof Creation for Bug Bounties

The post about subdomain takeover from last week received great feedback. I decided to follow-up and explain the...

0xpatrik.com

Project Sonar: An Underrated Source of Internet-wide Data

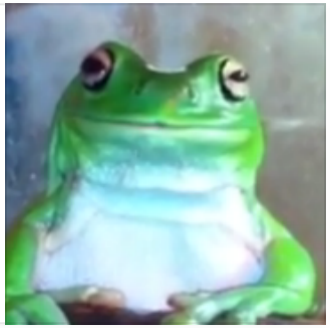
The Internet-Wide Scans Data Repository (scans.io) was created alongside Censys. The purpose of this repository is to...

0xpatrik.com

EdOverflow/can-i-take-over-xyz

can-i-take-over-xyz—"Can I take over XYZ?"—a list of services and how to claim (sub)domains with dangling DNS...

github.com



· · ·

5. Data Storage Buckets.

Common Places to find Data Storage buckets.

- Github
- Javascript files
- CSP Headers

- Archive crawl
- Pastebin

Tip: If a bucket is returning access denied. Try to search it on Google. There are good chances that the team has recently changed the permissions of the bucket and specific files have been indexed by Google (which are available with read permission).

If the application has file uploading functionality, then try to capture the file uploading request and see where the file is being uploaded. Sometimes you will find AWS or other data storage buckets, which cannot be detected by any other method.

If you find the bucket like **upload-user-content-target-prod—**try to change the prod to dev, staging, sandbox, etc.

- **AWS CLI**—AWS CLI is useful for verifying or testing the permissions of the AWS S3 buckets, Creating Buckets and Read other buckets data. AWS Account needed to use CLI.

AWS Command Line Interface

The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and…

aws.amazon.com

- **Bucket Finder—**Great Tool for finding buckets using subdomains wordlist, can be integrated into recon.rb script but I don’t always use it.

Bucket Finder—DigiNinja

An app to brute force Amazon S3 bucket names then search them for publicly available files. Even gives the option to…

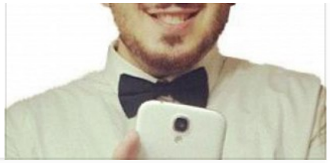
digi.ninja

- **LazyS3—**LazyS3 is an another tool which I use almost frequently to find the staging, sandboxed, dev and production buckets.

nahamsec/lazys3

Contribute to lazys3 development by creating an account on GitHub.

github.com



- **Slurp**: Slurp great tool for AWS Buckets Recon. (Deleted After Microsoft Purchased Github I guess). Weird!

https://github.com/bbb31/slurp

- **S3 Bucket Finder**—Another good tool for AWS S3 buckets.

gwen001/s3-buckets-finder

s3-buckets-finder—Find aws s3 buckets and extract datas.

github.com

Interesting blog post

A deep dive into AWS S3 access controls—taking full control over your

assets

TL;DR: Setting up access control of AWS S3 consists of multiple levels each with its own unique risk of...

labs.detectify.com

6. Github For Recon.

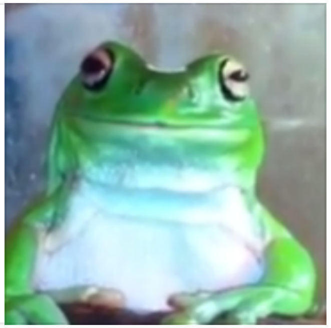
Github is extremely helpful in finding Sensitive information regarding the targets. Access-keys, password, open endings, s3 buckets, backup files, etc. can be found on public GitHub repositories.

Interesting blog post

GitHub for Bug Bounty Hunters

My tips for finding security issues in GitHub projects.

edoverflow.com



7. Read every JS.

Sometimes, Javascript files contain sensitive information including various secrets or hardcoded tokens. It’s always worth to examine JS files manually.

I have found the following things in Javascript.

- AWS or Other services Access keys
- AWS S3 buckets or other data storage buckets with read/write permissions.
- Open backup sql database endpoints
- Open endpoints of internal services.

The more Javascript files you read, the more chances will be of win.

Tools

I generally like to read the javascript code manually with the help of JSBeautifier.

Online JavaScript beautifier

Chrome, in case the built-in CSS and javascript formatting isn't enough for you: — Quick source viewer by Tomi...

jsbeautifier.org

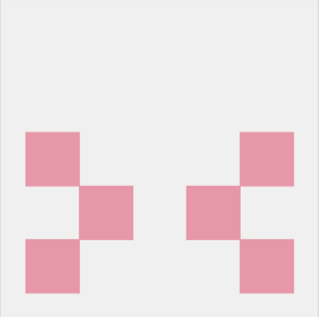
The following tools are useful:

LinkFinder

GerbenJavado/LinkFinder

LinkFinder — A python script that finds endpoints in JavaScript files

github.com

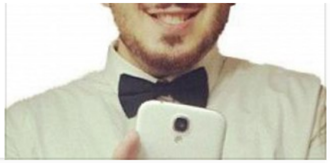


JSParser—Another great tool by Behrouz Sadeghipour

nahamsec/JSParser

Contribute to JSParser development by creating an account on GitHub.

github.com

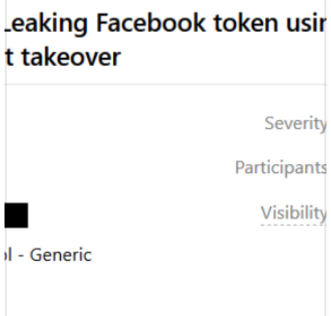


Interesting blog post

Bug Bounty — Tips / Tricks / JS (JavaScript Files)

It all started in month of August when I reached out to Gerben Javado regarding a question, yes it was a basic question…

medium.com



eaking Facebook token usir
t takeover

Severity

Participants

Visibility

l - Generic

• • •

8. Archive

Searching for the targets webpages in waybackmachine, the following things can be found.

- Old and abandoned JS files.

- Old API endpoints.
- Abandoned CDN’s Endpoints.
- Abandoned Subdomains.
- Dev & staging endpoint with juicy info in source code comments.

If you are getting 403 on a page, you can also search that 403 pages of targets in way back machine sometimes, you will find them open with helpful information.

Tool: Waybackurl

. . .

9. Continuous Recon.

- The most essential thing in continuous recon is handling of the recon data for the future uses, for this, **SecurityEscape** created a tool known as **Swiftness.** I use Swiftness to hold all of my recon data for every target.

Swiftness- My personal websec checklist.

- I use the reminder to revisiting the targets and perform recon regularly. (Every month)

. . .

10. Extra points for recon.

. . .

Note: I have provided some data in gist because I regularly update them and those updates will be automatically available here.

. . .

Best of luck for all of your future infosec things.

If you have questions and anything about the post you want to ask me, Please contact me via twitter/fb. I'll have my DM open.

Feedbacks and edits are welcome

Twitter Facebook

Until next time!

Thanks to Rishiraj Sharma and Mukesh Dhama.

Bugsbounty Infosecurity Ethical Hacking Security White Hat Hacking

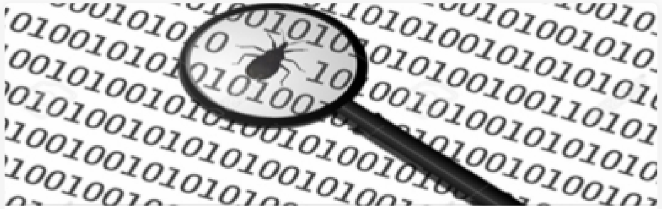
1.5K claps

7

Sahil Ahamad

Security Engineer @zomato | Bug Bounty Hunter

Follow



Related reads ★

The BatchOverflow Bug and How to Catch All Bugs

Kiran Garimella

May 11, 2018 · 12 min read

207

Related reads

h1–702 CTF — Web Challenge Write Up

Amal Murali

Jul 1, 2018 · 12 min read

904

Related reads ★

Chinese Hackers Back Beijing’s Authoritarian Pals

Foreign Policy

Jul 30, 2018 · 7 min read ★

65

Responses

Write a response…

Conversation with Sahil Ahamad.

Henrik
Jun 6, 2018

Nice writeup! Is Swiftness available to the public?

1 response

Sahil Ahamad
Jun 9, 2018

Swiftness will be available soon. I’ll post about it.

10

1 response

Show all responses