A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report – mergify**

**IT21831904 – K.M. Weerasinghe**

Table of Contents

[Scope of the target 3](#_Toc149248773)

[In scope and rewards 3](#_Toc149248774)

[Out of scope 3](#_Toc149248775)

[Reconnaissance 4](#_Toc149248776)

[Subdomain enumeration 4](#_Toc149248777)

[Gathering information about the target 5](#_Toc149248778)

[Virtual host discovery 6](#_Toc149248779)

[Subdomain takeover 7](#_Toc149248780)

[Scanning 8](#_Toc149248781)

[Using Nmap for scanning 8](#_Toc149248782)

[Using final recon for scanning 8](#_Toc149248783)

[Vulnerability checking 9](#_Toc149248784)

[Vulnerabilities found using NIKTO 9](#_Toc149248785)

[Vulnerabilities found using rapidscan 10](#_Toc149248786)

# Scope of the target

A white background with black text

Description automatically generated

## In scope and rewards

A screenshot of a computer

Description automatically generated

## Out of scope

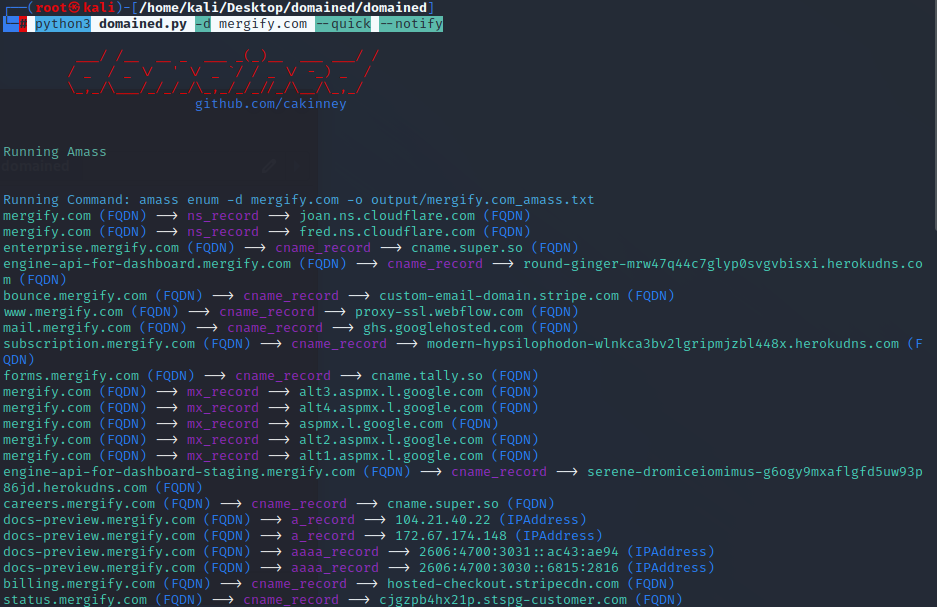
A screenshot of a computer program rules

Description automatically generated

# Reconnaissance

## Subdomain enumeration

* └─# python3 domained.py -d mergify.com --quick --notify

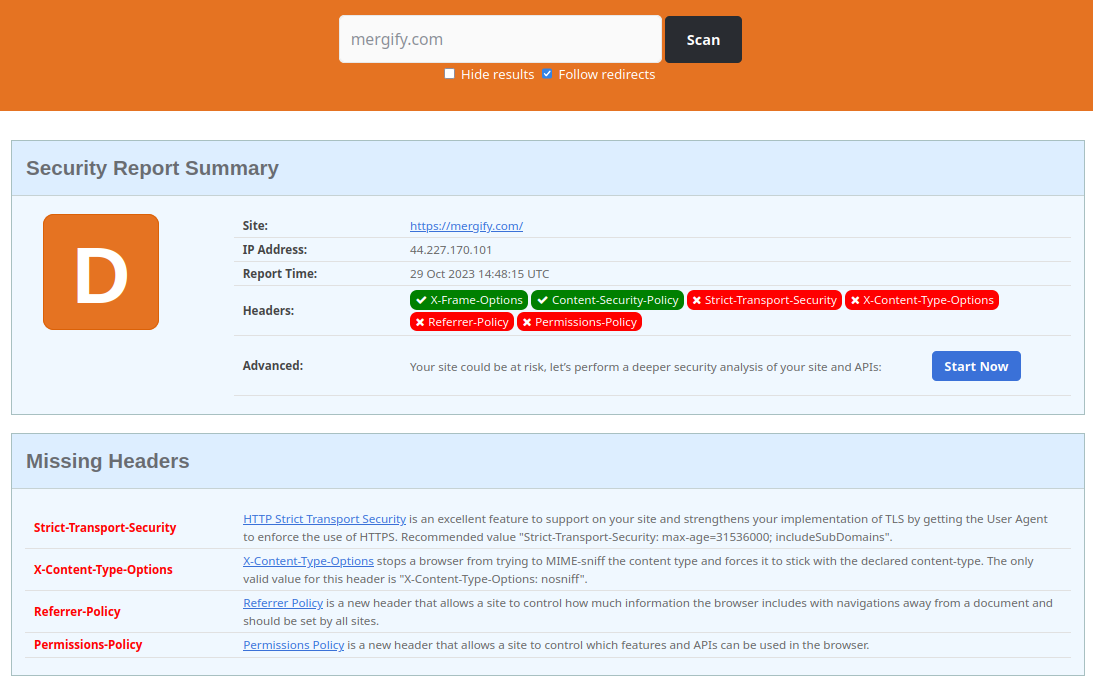


* Running Command: subfinder -d mergify.com -o output/mergify.com\_subfinder.txt A screenshot of a computer screen

  Description automatically generated
* Collected subdomains run through subjack tool to find if any of the subdomains are vulnerable

## Gathering information about the target

* Security header checking



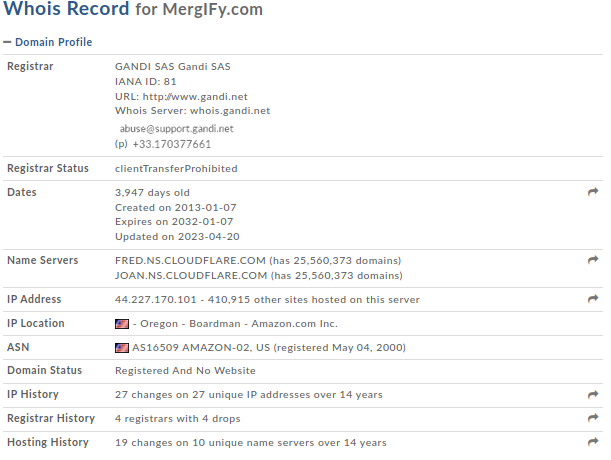
missing headers - Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.

* + Strict-Transport-Security
    - HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
  + Content-Security-Policy
    - Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
  + Referrer-Policy
    - Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
  + Permissions-Policy

Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Domain profile and whois records

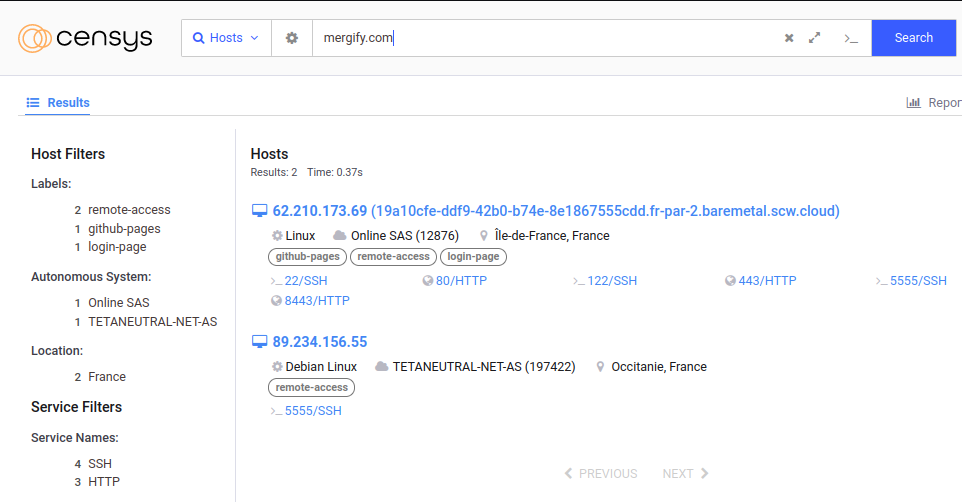
* domain profile



* A screenshot of a computer

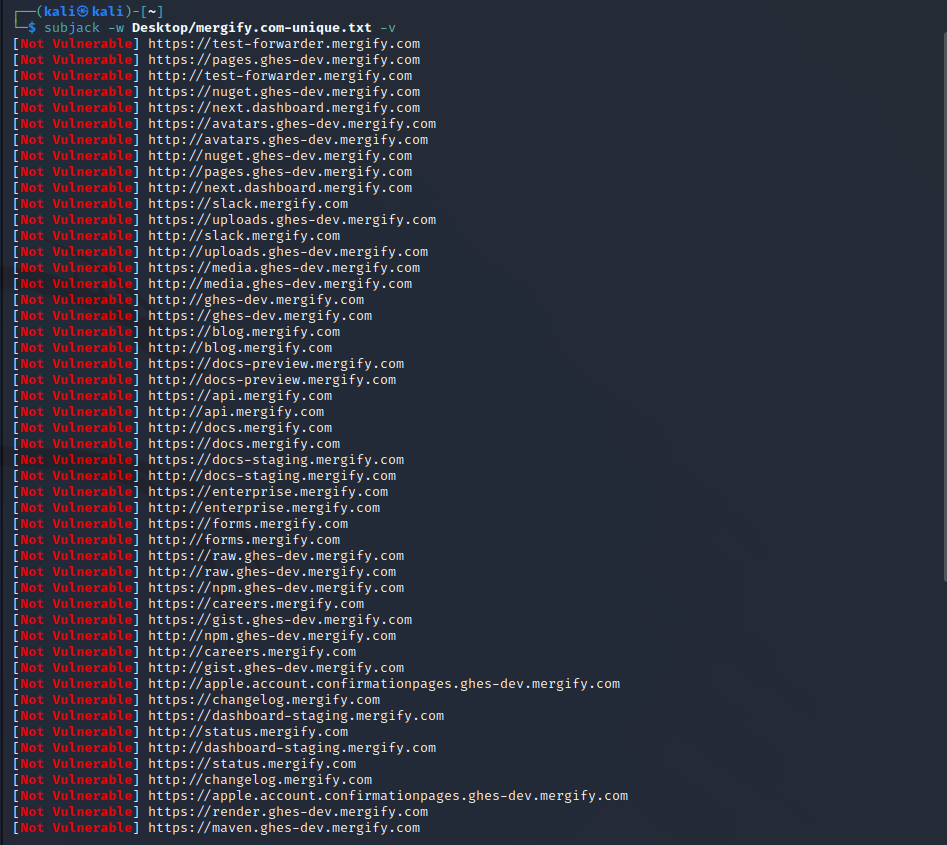
  Description automatically generatedwho is records

## Virtual host discovery

* hosts details gathered using the censys website

## Subdomain takeover

* └─$ subjack -w Desktop/mergify.com-unique.txt -v

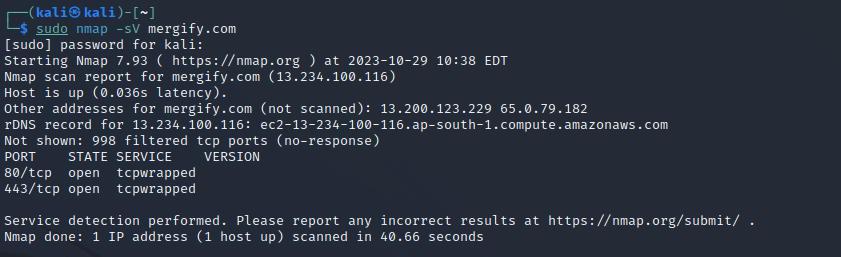


* Identifying if any of the found subdomains from the previous scans are vulnerable to takeover
* No vulnerable subdomains were found
* All subdomains appear to be secure
* No issues were identified in the subdomain analysis

# Scanning

## Using Nmap for scanning

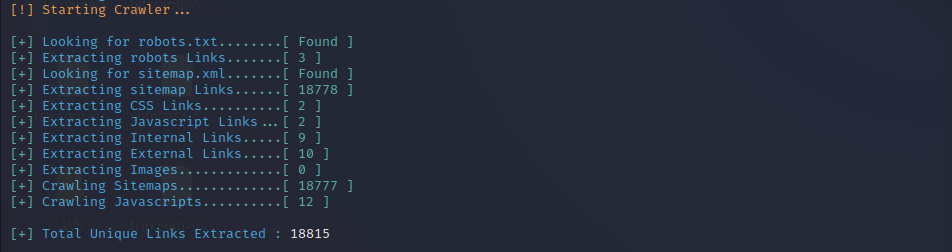
* └─$ sudo nmap -sV mergify.com



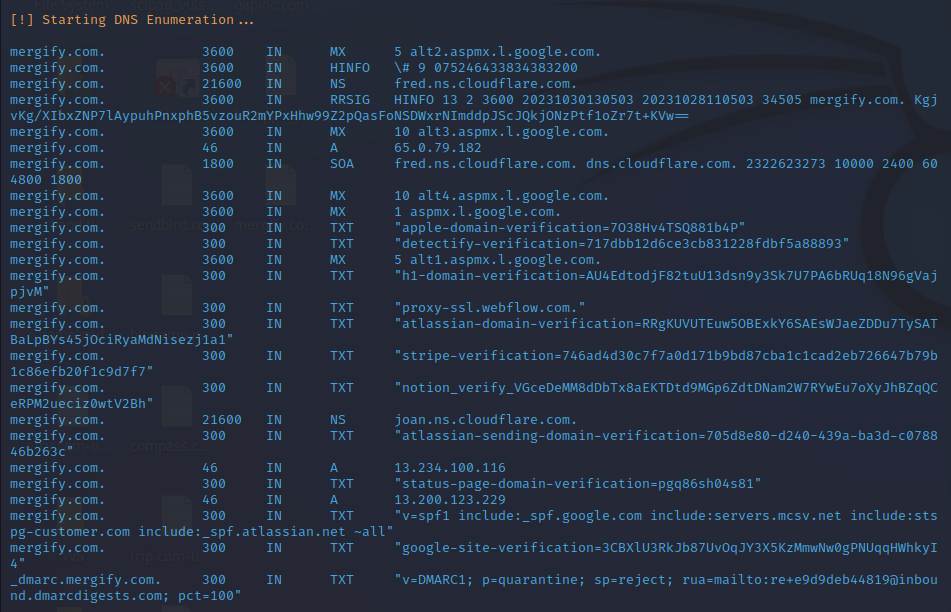
* Port 80 open
* Port 443 open

## Using final recon for scanning

Information gathered using crawlers



* Sometimes robots.txt or sitemap.xml may contain rules such that certain links that are not supposed to be accessed/indexed by crawlers and search engines. Search engines may skip those links but attackers will be able to access it directly
* A screenshot of a computer

  Description automatically generatedSitemaps and robotos.txt and robot’s links found
* DNS records gathered

# Vulnerability checking

## Vulnerabilities found using NIKTO

* └─$ nikto -h mergify.com

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 65.0.79.182

+ Target Hostname: mergify.com

+ Target Port: 80

+ Message: Multiple IP addresses found: 65.0.79.182, 13.200.123.229, 13.234.100.116

+ Start Time: 2023-10-29 08:07:08 (GMT-4)

---------------------------------------------------------------------------

+ Server: No banner retrieved

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Root page / redirects to: https://mergify.com/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Uncommon header 'x-cluster-name' found, with contents: ap-south-1-prod-hosting-red

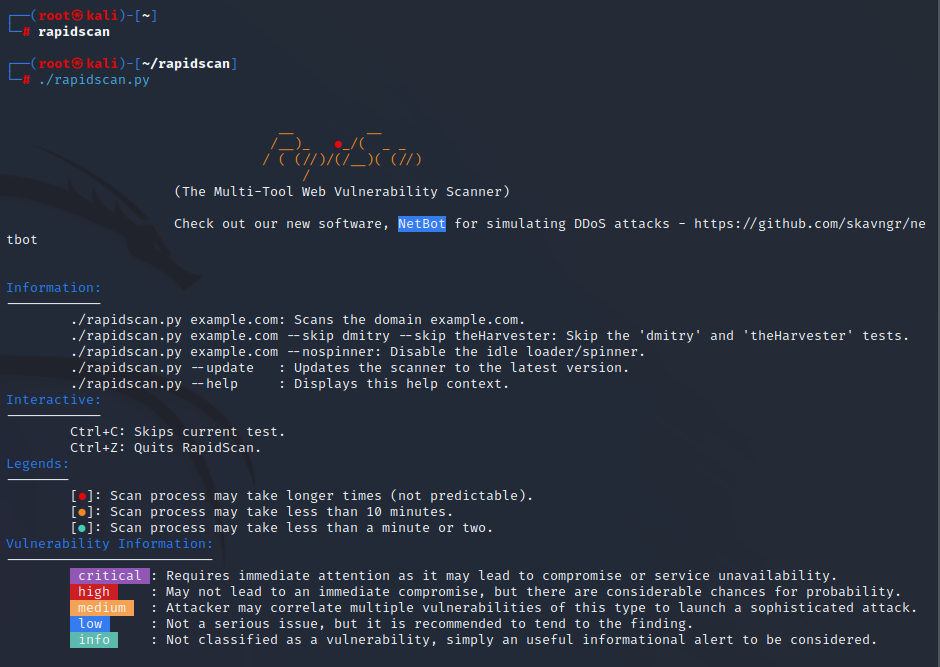
+ 7785 requests: 0 error(s) and 4 item(s) reported on remote host

+ End Time: 2023-10-29 08:37:54 (GMT-4) (1846 seconds)

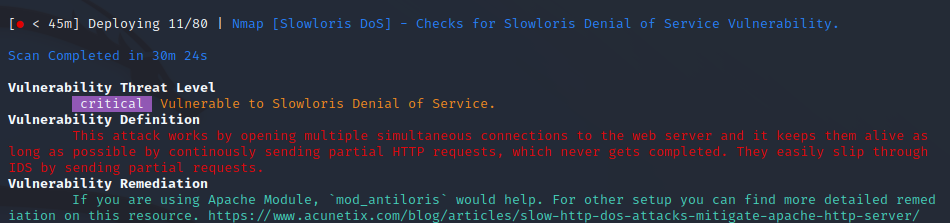
---------------------------------------------------------------------------

+ 1 host(s) tested

## Vulnerabilities found using rapidscan

* └─# ./rapidscan.py

1. Vulnerability title - vulnerable to slowloris denial of service

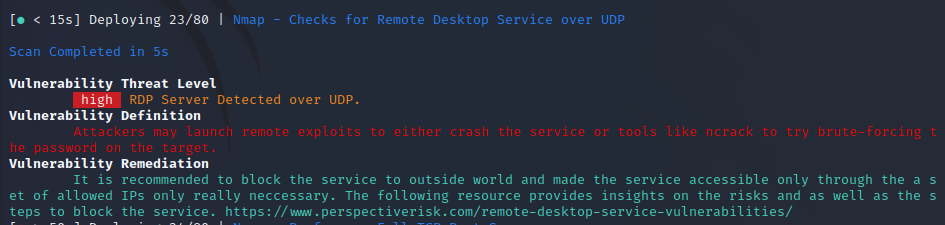


* Vulnerability threat level
  + Critical
* Vulnerability description
  + This attack works by opening multiple simultaneous connections to the web server and it keeps them alive as long as possible by continuously sending partial HTTP requests, which never get completed. They easily slip through IDS by sending partial requests.
* Affected components
  + affects web servers, could include a wide range if web server software’s
* Impact assessment
  + it can effectively deny legitimate users access to the targeted web server, disrupt services, and potentially lead to significant downtime.
* How an attack could be carried out
  + Establish multiple simultaneous connections to the target web server.
  + Keep these connections open by sending partial HTTP requests that are never completed.
  + Continuously maintain these connections to exhaust server resources.
* Proposed mitigation or fix –
  + Implementation of rate limiting to limit the number of concurrent connections from a single Ip address.
  + Implementing intrusion detection and prevention systems
  + Distribute traffic across multiple servers to reduce the impact of these type of attacks

1. A screenshot of a computer error

   Description automatically generatedVulnerability title - possible XSS, SQLi, BSQL

* vulnerability threat level
  + high
* vulnerability description
  + Hackers will be able to steal data from the backend and, they can authenticate themselves to the website and can impersonate as any user since they have total control over the backend. They can even wipe out the entire database. Attackers can also steal cookie information of an authenticated user and they can even redirect the target to any malicious address or totally deface the application.
* Affected components
  + This vulnerability impacts the application's backend and data storage components
* Impact assessment
  + The impact of this vulnerability is high, as it allows for data theft, unauthorized access, potential data loss, and various forms of user manipulation.
* Steps to reproduce
  + Identify input fields or areas in the application that lack proper validation.

1. vulnerability title – RDP server detected over UDP

* Vulnerability threat level
  + High
* Vulnerability description
  + Attacker may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password of the target.
* Impact assessment
  + The vulnerability has a high threat level, as it can lead to service disruptions or unauthorized access
* Proposed mitigation or fix
  + It is recommended that to block the service outside world and make the service accessible only through the set of allowed IPs only necessary to prevent potential exploits.

